



United States Department of Agriculture



FNS Handbook 901

The Advance Planning Document Process:
A State Systems Guide to America's Food Programs

Version 2.5 January 2026

Guidance documents lack the force and effect of law, unless expressly authorized by statute or incorporated into a contract. USDA may not cite, use, or rely on any guidance that is not available through their guidance portal, except to establish historical facts.



P1. Navigating this Handbook

P1.1 How to Read this Handbook

This handbook has been designed to be easy to read and to be user-friendly. Throughout the handbook, you will notice several visual elements that operate as sign-posts to help you navigate the information. The handbook has been designed to be used both manually and electronically. Therefore, many of these features are hyperlinked.

The three main visual elements used are:

- Chapter Introduction pages
- Cross-references
- Call-out boxes and icons

P1.1.1 Chapter Introductions

Each chapter in Handbook 901 begins with an introduction page. This page is designed as an overview for the chapter as a whole. It consists of three parts: Key Points, Chapter Contents, and Key Acronyms. The Key Points section will introduce you to the important concepts to look for while reading the chapter. They are phrased in the form of questions.

For example, if this Preface had a section of Key Points it would look like **Figure 1**.

Key Points

The information in this section allows you to answer the following questions:

- What are the three parts of the chapter Introductions?
- What are the three different types of references used?
- What do the seven icons used with call-out boxes denote?

Figure 1: Example of Key Points

Following the Key Points section is the Chapter Contents table. It is fully navigable and can be used to jump ahead to specific sections within the chapter. When viewing electronically, just Ctrl + Click on the heading in the table of contents to travel to the section you need.

If this Preface had a Chapter Contents table, it would look like **Figure 2**.

Chapter Contents	
P1.1	How to Read this Handbook..... 1
P1.1.1	Chapter Introductions.....1
P1.1.2	References 3
P1.1.3	Call-Out Boxes and Icons 5
P1.1.4	SNAP and WIC Icons.....5
P1.2	Navigation and the Table of Contents..... 6

Figure 2: Example of Chapter Contents

Following the Table of Contents is the Chapter Acronyms table. Chapter Acronyms is simply a list of the acronyms specific to that chapter’s content. It will be helpful to be familiar with these terms before you read the chapter. Additional terms can be found in the glossary. A link to the glossary follows every Chapter Acronyms table.

Chapter Acronyms	
ADP	Advance Planning Document
EBT	Electronic Benefit Transfer
FFP	Federal Financial Participation
FNS	Food and Nutrition Service



For definitions of terms used in this handbook please see appendix **A1 Glossary**

Figure 3: Example of Chapter Acronyms Table and Cross-Reference to Glossary

P1.1.2 References

Three types of references are used in Handbook 901. These references direct you to additional information that may be helpful or shed extra light on a subject.

- **Cross-References**
- **Footnotes**
- **Endnotes**

P1.1.2.1 Cross References and Hyperlinks

Cross-references to locations within HB901 will be found either in a Cross-Reference box or in the body of the narrative and are shown in bold, italic font as represented in **Figure 4**. Simply hover and Ctrl + Click the bold links to travel to sections within the chapter or to other places in the document, as well as to Tables and Figures. Links to content outside the document will be hyperlinks, and notated in the traditional [blue underlined style](#).

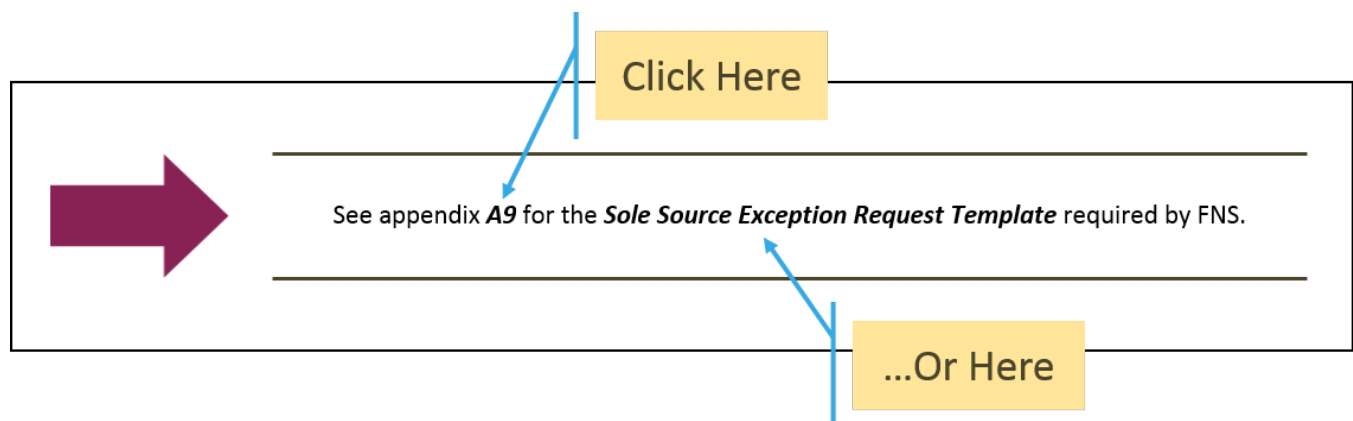


Figure 4: Example of a Cross Reference Box

P1.1.2.2 Footnotes

Footnotes contain supplemental information not vital to the main narrative but that is interesting or helpful. They are located at the bottom of pages and annotated in-line with symbols. *The traditional order of these symbols in English is *, †, ‡, and § that is how they are annotated in Handbook 901.

* The novel, *Ibid: A Life*, by Mark Dunn is written entirely [in footnotes](#).

P1.1.2.3 Endnotes

Endnotes are citations for sources and regulations. They are designed for you to navigate to the source, so each endnote includes a hyperlink to the original source material. Endnotes are found at the end of the chapter and are annotated with numbers. The superscript number that is in line with the narrative is called the Endnote Reference.¹

Endnotes in this handbook are structured to provide the most important information first. In the example shown in **Figure 5: Endnote Structure**, the title is first, followed by the Regulation number, the author of the document (which in this case is The US Government), and finally the URL hyperlinked to the original source. The structure of the endnote will remain consistent; however, the elements will change depending on the source being cited. In some cases there will be Version or Control Numbers instead of a Regulation number or a Section Name instead of a Title. Acronyms will be used instead of commonly used long phrases in order to simplify the endnote.

These are common acronyms used in the endnotes of HB901:

- **NIST: National Institute of Standards and Technology**
- **OMB: Office of Management and Budget**
- **CFR: Code of Federal Regulations**

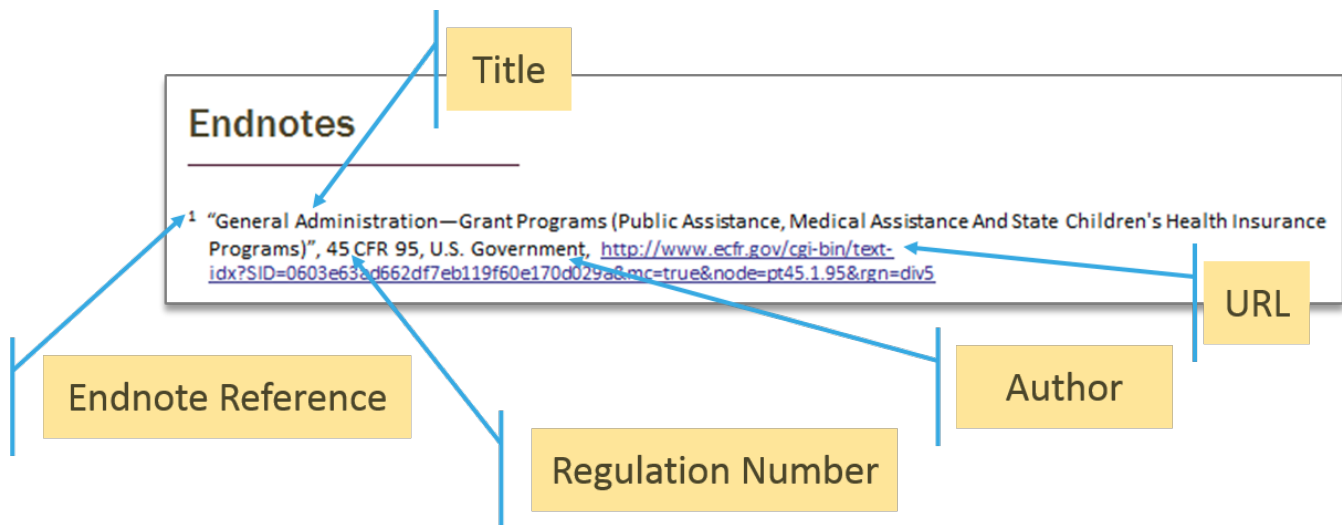


Figure 5: Endnote Structure

While these sources are readily available online, they will likely be changed or updated over time. If you find that a URL is out-of-date or no longer functioning, simply copy the title or regulation number into your preferred search engine to find its updated home on the web.

P1.1.3 Call-Out Boxes and Icons

Information that requires special attention is shown in gold call-out boxes, like this one in **Figure 6**.

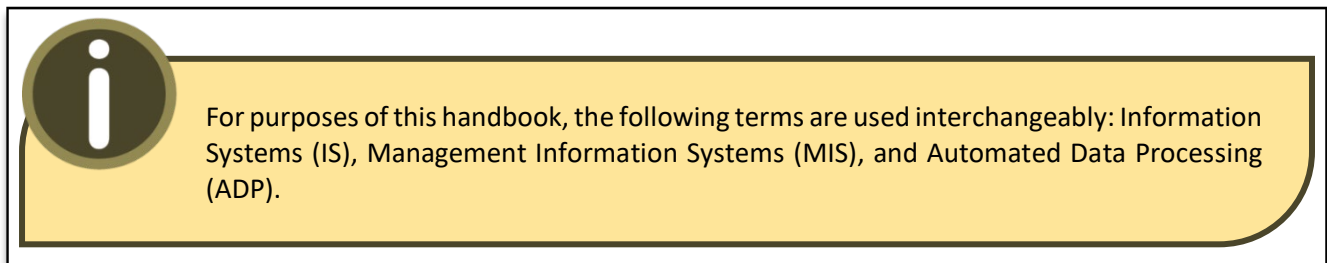


Figure 6: Example of a Call-out Box

Callout boxes will also sometimes include hyperlinks to the source of the content. In addition to the text, each call-out box uses one of seven different icons to quickly denote what kind of information is in the box.

The icons are as follows:



P1.1.4 SNAP and WIC Icons



You will notice that there are icons above denoting SNAP- and WIC-specific information. These icons are used in two different ways. When there is a larger amount of program-specific content, a SNAP or WIC icon will be used in conjunction with a SNAP or WIC heading. It will be contained within the body of the program-specific narrative, as shown in this paragraph with the WIC icon.

In cases of smaller amounts of program-specific information to showcase, the icon and content will appear in call-out boxes within the general topic narrative, as shown with the SNAP icon in **Figure 7**.

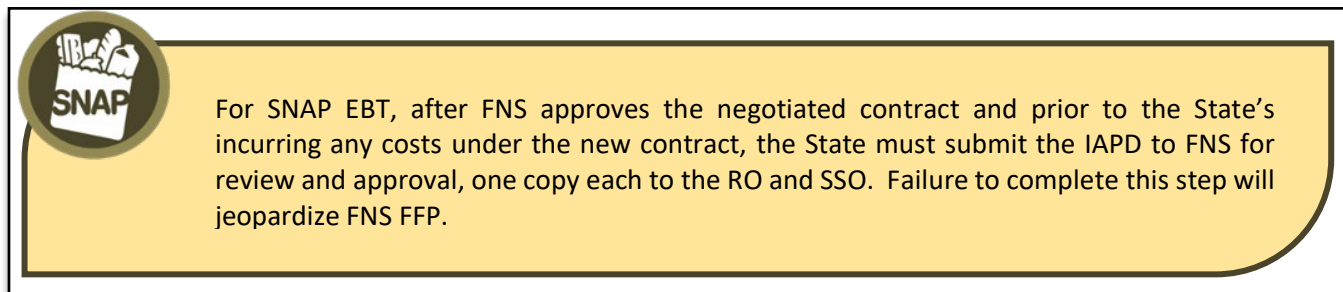


Figure 7: Example of a SNAP-Specific Call-out Box

P1.2 Navigation and the Table of Contents

The table of contents (TOC) immediately following this Preface will be vital to users' navigating this handbook. The TOC is fully navigable and contains links to all the main content via a four-level heading structure. Also included are detailed contents of the Appendices, as well as tables of tables and figures, so that you can easily find exactly the content you need. When reading chapters, you can use the Bookmarks Pane in addition to the Chapter Contents to jump forward or backward within the chapter with just a click.

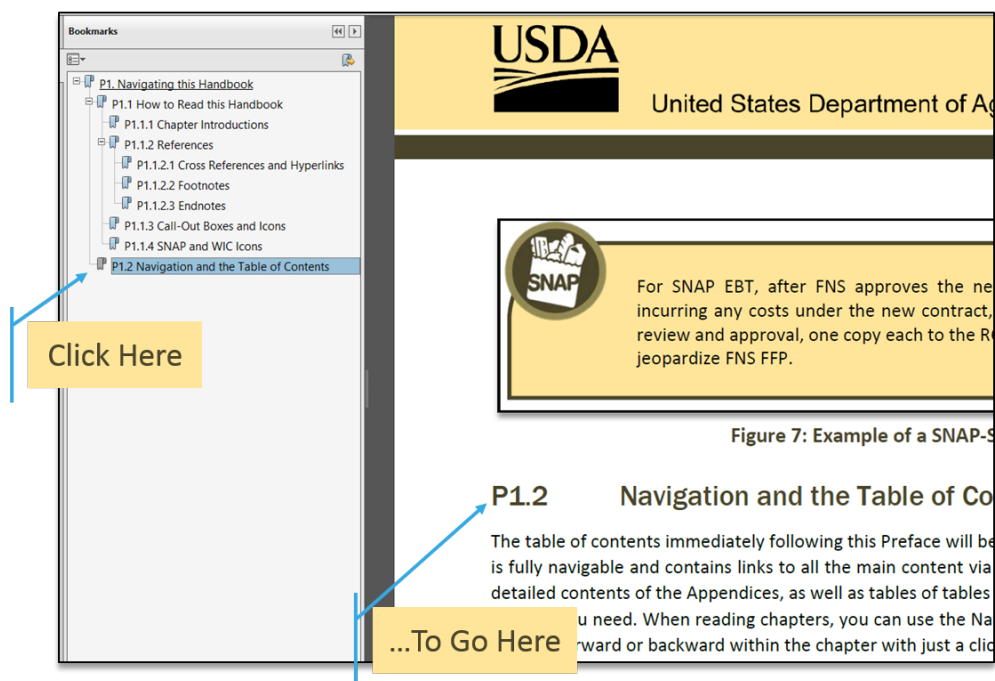


Figure 8: Using the Bookmarks Pane



Endnotes

¹ Note (typography), Wikipedia, [https://en.wikipedia.org/wiki/Note_\(typography\)](https://en.wikipedia.org/wiki/Note_(typography))



Table of Contents

P1.	Navigating this Handbook.....	1
P1.1	How to Read this Handbook	1
P1.1.1	Chapter Introductions	1
P1.1.2	References	3
P1.1.2.1	Cross References and Hyperlinks.....	3
P1.1.2.2	Footnotes.....	3
P1.1.2.3	Endnotes.....	4
P1.1.3	Call-Out Boxes and Icons	5
P1.1.4	SNAP and WIC Icons	5
P1.2	Navigation and the Table of Contents	6
1.0	Getting Started with the Advance Planning Document (APD) Process	41
1.1	Introduction	44
1.2	Introduction to FNS Programs	45
1.2.1	Supplemental Nutrition Assistance Program (SNAP).....	46
1.2.2	Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).....	46
1.3	The Electronic Benefits Transfer (EBT).....	47
1.4	Federal Funding.....	47
1.4.1	SNAP and FFP	48
1.4.2	WIC and FFP.....	48
1.5	Determining the Need for an APD.....	49
1.5.1	Thresholds	49



1.5.1.1	Planning.....	49
1.5.1.2	Implementation	50
1.5.1.3	Maintenance and Operations.....	50
1.5.2	Cost Increases	52
1.5.2.1	SNAP Cost Increases.....	52
1.5.2.2	WIC Cost Increases.....	52
1.5.3	SNAP & WIC EBT	52
1.5.4	WIC MIS Exceptions.....	53
1.6	Introduction to the Advance Planning Document.....	54
1.7	Introduction to the APD Process	55
1.7.1	Planning Phase	57
1.7.2	Implementation Phase	57
1.7.3	APD Closure	57
1.7.4	Acquisition Document Approvals.....	58
1.8	Roles and Responsibilities	58
1.8.1	FNS.....	58
1.8.2	State Agency	60
1.8.3	Project Management.....	61
1.9	Stakeholders	62
1.9.1	Core Stakeholders - The Project Team	62
1.9.2	Key Stakeholder - FNS	63
1.9.3	Key Stakeholder - State Agencies	63
1.9.4	Other Key Stakeholders.....	64
1.9.4.1	Federal Stakeholders.....	64
1.9.4.2	Financial Institutions and EBT Processors.....	64
1.9.4.3	Retail Vendors	65



1.9.4.4	Food Manufacturers and WIC.....	65
1.10	Governance - Legislation, Regulation, Policy (LRP)	65
1.10.1	SNAP LRP	65
1.10.2	WIC LRP	66
1.11	Moving forward with the Handbook 901.....	66
1.12	Getting Started Summary	67
2.0	Lifecycle Management	70
2.1	Lifecycle Management – An Overview	72
2.2	Systems Development Lifecycle Management.....	73
2.2.1	Overview of Systems Development Phases	73
2.2.1.1	The Initiation Phase	74
2.2.2	The Development Phase	75
2.2.2.1	Implementation Phase.....	75
2.2.2.2	Maintenance & Operation Phase	75
2.2.2.3	Disposal Phase.....	76
2.2.3	Management of the SDLC Phases	76
2.2.4	System Development Lifecycle Methodologies.....	77
2.2.4.1	Waterfall.....	79
2.2.4.2	Agile80	
2.3	Project Management Lifecycle	82
2.3.1	Project Initiation Phase	83
2.3.2	Project Planning Phase	84
2.3.3	Project Execution Phase.....	84
2.3.4	Project Monitoring and Controlling Phase	85
2.3.5	Project Closure Phase.....	86



2.4	Acquisition Lifecycle Management	87
2.4.1	Pre-Award Phase.....	88
2.4.2	Award Phase	89
2.4.3	Post-Award Phase.....	90
2.5	Data Lifecycle Management	91
2.5.1	Technical vs. Non-Technical Data	92
2.5.2	Data Lifecycle Management Phases	93
2.5.2.1	Acquire Phase	93
2.5.2.2	Store Phase.....	94
2.5.2.3	Use, Share, and Archive Phases	95
2.5.2.4	Destroy	95
2.6	Alignment of Lifecycles.....	97
2.6.1	Lifecycle Management (LCM) Interactions.....	97
2.6.2	Aligning SDLC and PMLC.....	98
2.6.3	Aligning ALC to SDLC	99
2.6.4	Aligning SDLC, ALC, and PMLC to DLC	99
2.6.5	Aligning SDLC and the APD Process.....	99
2.7	Lifecycle Management Summary	101
3.0	The Advance Planning Document Process	103
3.1	Overview of the Advance Planning Document	106
3.2	The APD Process.....	107
3.2.1	Introduction	107
3.2.1.1	The General APD Process	108
3.2.1.2	Relationship of APD Process to SDLC	110
3.2.2	Preparation & Submission.....	111



3.2.2.1	Preparation	111
3.2.2.2	Submission.....	112
3.2.3	Review	113
3.2.3.1	APD Reviews in General	113
3.2.3.2	APD Evaluation in General	114
3.2.3.3	FNS APD Review Timeframes	116
3.2.4	Disposition.....	118
3.2.4.1	Approval Decision	118
3.2.4.2	Disapproval Decision	119
3.2.4.3	Provisional Approval in SNAP.....	119
3.2.5	Performing APD Activities.....	120
3.2.6	Relationship Between Procurements and the APD Process	120
3.2.7	APD Closure	122
3.2.8	Post-Implementation Reviews	123
3.2.9	Regional Office Fiscal Closure.....	124
3.3	APD Information Specific to Program or Project Type	124
3.3.1	Planning APD.....	125
3.3.1.1	Purpose of PAPD.....	125
3.3.1.2	Related SDLC Activities for PAPD	125
3.3.1.3	PAPD Documentation Requirements.....	126
3.3.1.4	Preparing the PAPD	127
3.3.1.5	Submitting the PAPD	128
3.3.1.6	Performing Planning Activities	129
3.3.2	Implementation APD.....	130
3.3.2.1	Purpose of the IAPD.....	130
3.3.2.2	Related SDLC Activities for IAPD.....	130



3.3.2.3	IAPD Documentation Requirements	131
3.3.2.4	SNAP EBT Required IAPD Documentation	133
3.3.2.5	WIC EBT Required IAPD Documentation	134
3.3.2.6	Preparing the IAPD	134
3.3.2.7	Submitting the IAPD	135
3.3.2.8	Performing Implementation Activities	135
3.3.3	APD Update	136
3.3.3.1	Purpose of the APDU.....	136
3.3.3.2	Related SDLC Activities for APDU	137
3.3.3.3	APDU Documentation Requirements.....	137
3.3.3.4	Preparing the APDU	137
3.3.3.5	Submitting the APDU	138
3.3.3.6	Performing On-Going APD Activities.....	139
3.3.4	APDU As-Needed.....	139
3.3.4.1	Purpose of the APDU As-Needed.....	139
3.3.4.2	Related SDLC Activities for APDU As-Needed	140
3.3.4.3	APDU As-Needed Documentation Requirements	140
3.3.4.4	Preparing the APDU As-Needed.....	142
3.3.4.5	Submitting the APDU As-Needed	142
3.3.4.6	Performing As-Needed Activities.....	143
3.3.5	Emergency Acquisition Request	143
3.3.5.1	Purpose of the EAR	143
3.3.5.2	Related SDLC Activities for EARs	144
3.3.5.3	EAR Required Documentation	144
3.3.5.4	Preparing the EAR	144
3.3.5.5	Submitting the EAR.....	145



3.3.5.6	Performing EAR Activities.....	146
3.4	Post-Implementation APDs.....	146
3.5	APD Components	147
3.5.1	Actual Expenditures to Date	147
3.5.2	Annual APD Update Revised Documents	147
3.5.2.1	Revised Budget	147
3.5.2.2	Revised Cost Allocation Plan.....	147
3.5.2.3	Revised Functional Requirements	148
3.5.2.4	Revised Project Management Plan and Resource Requirements	148
3.5.2.5	Revised Schedule of Activities, Milestones, and Deliverables	148
3.5.2.6	Revised Technical Approach	148
3.5.3	Alternatives Analysis	148
3.5.4	Capacity Plan or Study	149
3.5.5	Changes to the Approved APD	149
3.5.6	Contractor Performance	149
3.5.7	Conversion or Transition Plan.....	149
3.5.8	Cost Allocation Plan	149
3.5.9	Cost Benefit Analysis.....	150
3.5.10	Detailed Design Document	150
3.5.11	Disaster Recovery Plan.....	150
3.5.12	EBT Disaster Recovery Plan.....	151
3.5.13	Executive Summary – General Guidelines	151
3.5.14	Feasibility Study	153
3.5.15	Functional Requirements Document.....	153
3.5.16	General System Design	154
3.5.17	Project Management Plan	154



3.5.18	Project Status	154
3.5.19	Proposed Budget.....	154
3.5.20	Request for Waiver of Depreciation.....	155
3.5.21	Resource Requirements.....	155
3.5.22	Schedule of Activities, Milestones, and Deliverables	156
3.5.23	Security Plan	156
3.5.24	Test Plan	157
3.5.25	Training Plan	157
3.5.26	Transmittal Letter	158
3.6	APD Process Summary.....	158
4.0	Procurement.....	162
4.1	Purpose and Goals	165
4.2	Procurement Process Summary	166
4.2.1	Primary Procurement Documents.....	167
4.2.2	Pre-Award Phase.....	167
4.2.2.1	Procurement Planning.....	167
4.2.2.2	RFP Preparation.....	168
4.2.2.3	RFP Review and Approval.....	169
4.2.3	Award Phase	169
4.2.3.1	Evaluating Proposals.....	170
4.2.3.2	Source Selection	170
4.2.4	Post-Award Phase.....	172
4.2.4.1	Contract Approval	172
4.2.4.2	Managing Contracts	172
4.2.4.3	Contract Amendments	174



4.2.4.4	Contract Closeout	175
4.2.4.5	Disposition of Government Property.....	175
4.3	Procurement Reviews.....	176
4.3.1	Determining the Need for Review	176
4.3.2	Overview of the FNS Review Process.....	179
4.4	Regulations and Policies	182
4.5	Roles and Responsibilities	183
4.5.1	FNS.....	183
4.5.2	State Agency	183
4.6	Technical Procurement Planning	184
4.6.1	Performance Requirements	184
4.6.2	System Transfer Considerations.....	185
4.6.2.1	WIC State Agency Model (SAM) Exception	186
4.6.2.2	WIC Exception – (non-SAM).....	186
4.6.3	EBT Conversion or Transition Planning.....	187
4.6.4	SNAP EBT Conversion or Transition Planning	188
4.7	RFP and Contract Planning.....	191
4.7.1	Preparing Criteria for Evaluating Proposals	192
4.7.1.1	Technical Evaluation Criteria.....	193
4.7.1.2	Proposed Cost Considerations	193
4.7.1.3	Previous Program Experience	194
4.7.2	Terms and Conditions	195
4.7.3	Incentives and Remedies.....	197
4.7.4	Quality Assurance Surveillance Plan (QASP)	198
4.7.5	Required Federal Assurances.....	199
4.7.6	Travel and Per Diem in Fixed Price Contracts.....	201



4.7.7	FNS Procurement Standards for State Agencies	201
4.7.7.1	Code of Conduct.....	201
4.7.7.2	Contracting with Small and Minority Firms, Women's Business Enterprises, and Labor Surplus Firms.....	202
4.7.7.3	Full and Open Competition	202
4.7.7.4	Geographic Preference Prohibition.....	202
4.7.7.5	State Agency Procurement Records and Information Systems	202
4.7.7.6	Ownership and Licensing	203
4.7.7.7	Intellectual Property Rights & Transferability.....	203
4.7.8	FNS Specific Procurement Requirements	204
4.7.9	Order of Precedence.....	204
4.7.10	Disputes	205
4.7.10.1	Alternative Dispute Resolution	205
4.7.11	Debarment and Suspensions	206
4.8	Procurement Methods	206
4.8.1	Competitive Procurements	207
4.8.1.1	Firm Fixed-Price Contracts.....	207
4.8.1.2	Time and Materials Provisions in Contracts.....	208
4.8.1.3	Service Agreements	209
4.8.2	Non-Competitive Procurements.....	211
4.8.3	Cooperative Purchasing.....	212
4.8.3.1	U.S. General Services Administration (GSA).....	213
4.8.3.2	National Association of State Procurement Officials (NASPO) ValuePoint	214
4.8.4	Contract Periods.....	215
4.8.5	Contractor Types and Roles.....	216
4.8.5.1	The Planning Contractor.....	217



4.8.5.2	Project Management Contractor	218
4.8.5.3	Planning and PM Contractor Considerations	219
4.8.5.4	Development and Implementation Support Contractor	220
4.8.5.5	Maintenance, Operations, and Enhancements Contractor Support	221
4.8.6	Conflicts of Interest	222
4.9	Procurement Documents	225
4.9.1	Request for Proposals.....	225
4.9.2	Contracts.....	226
4.9.3	RFP and Contract Components.....	227
4.9.3.1	RFP and Contract Format	227
4.9.3.2	Guidance for RFP and Contract Descriptions	228
4.10	Procurement Summary	231
5.0	System Planning.....	235
5.1	State Planning for Information Systems.....	237
5.1.1	System Planning and the APD Process.....	237
5.1.2	Recognizing the Need or Opportunity	237
5.1.3	Acting on the Need or Opportunity	238
5.2	Needs Assessment.....	239
5.2.1	Business Analysis.....	240
5.2.2	Business Needs Assessment.....	241
5.2.3	Business Capability Definition.....	245
5.2.4	SNAP Program Waivers	247
5.2.5	The Business Case	247
5.2.6	From Business Case to APD	248
5.3	Feasibility Study.....	248



5.3.1	Requirements Analysis	253
5.3.1.1	Business Analysis	254
5.3.1.2	Business Needs Assessment.....	254
5.3.1.3	Systems Analysis	255
5.3.1.4	System Integrity Review Tool Analysis for SNAP	255
5.3.1.5	WIC Functional Requirements Document (FReD)	256
5.3.1.6	System Integrity Review Tool Analysis for WIC	256
5.3.1.7	Functional Requirements Document.....	256
5.3.2	Alternative Analysis	257
5.3.2.1	Minimum Alternatives	257
5.3.2.2	Other Alternative Considerations	259
5.3.2.3	WIC State Agency Model Systems (SAM) Alternatives	261
5.3.2.4	Performing Alternatives Analysis	263
5.3.3	Cost Benefit Analysis.....	264
5.4	Technical Planning	268
5.4.1	Data Conversion & Migration	268
5.4.2	Capacity Planning Study.....	270
5.4.3	Technical Approach	272
5.5	Considerations	273
5.5.1	FNS Priority for Transferability and/or Reusability	273
5.5.1.1	Technological Transferability and/or Reusability Considerations.....	274
5.5.1.2	Other Transfer Considerations	275
5.5.2	Technology and System Capabilities	278
5.5.2.1	Open Systems Architecture	278
5.5.2.2	System Adaptability	279
5.5.3	Interconnectivity and Legacy Systems	280



5.5.4	Implementing New Systems.....	281
5.5.4.1	Considerations for Build vs. Buy	281
5.5.4.2	Solution Options.....	282
5.5.4.3	Technology Choices.....	282
5.6	System Planning Summary.....	284
6.0	Test Planning.....	287
6.1	Introduction	290
6.1.1	Test Plan - A General Description	290
6.1.2	FNS Requirements for Testing	291
6.1.3	Required Testing Activities	293
6.1.4	The Complete and Final Test Plan.....	295
6.2	Software Test Lifecycle	298
6.3	Requirements Analysis Phase	299
6.3.1	Planning Requirements Testing.....	300
6.3.2	Requirements Testability	301
6.3.3	Use Cases	302
6.3.4	Data Conversion and Migration	303
6.4	Test Planning Phase.....	303
6.4.1	Testing Approach	304
6.4.1.1	Entry / Exit Criteria	305
6.4.1.2	Pass / Fail Criteria.....	306
6.4.1.3	Test Suspension / Resumption Criteria	307
6.4.2	Issue and Defect Tracking.....	307
6.4.3	Resource Determination	308
6.4.3.1	Support Software	308



6.4.3.2	Test Environment / Staffing / Training Needs.....	309
6.4.4	Test Schedule Planning and Milestones	311
6.4.5	Test Risks/Issues.....	313
6.4.6	Test Constraints.....	314
6.4.7	Go/No-Go Decision Process.....	315
6.5	Test Case Development Phase.....	317
6.5.1	Items to be Tested	317
6.5.2	Test Cases	318
6.5.3	Test Scenarios / Test Conditions	319
6.5.4	Test Scripts.....	320
6.5.5	Test Data.....	320
6.5.6	Test Criteria	323
6.5.7	Expected Results.....	323
6.5.8	Error Handling.....	324
6.5.9	Test Procedures and Progression.....	324
6.6	Environment Setup Phase.....	324
6.7	Test Execution Phase	325
6.7.1	The Systems Test	326
6.7.2	User Acceptance Test.....	327
6.7.3	Pilot.....	328
6.8	Test Cycle Closure Phase.....	329
6.9	Test Lifecycle Support.....	330
6.9.1	Roll Back Contingency Plan.....	330
6.9.2	Quality Assurance	330
6.9.3	Independent Verification & Validation.....	331
6.10	Beyond Rollout.....	333



6.11	Test Planning Summary	333
7.0	Project Management	337
7.1	Project Management	339
7.1.1	Managing IT Projects.....	339
7.1.2	Role of the Project Manager.....	341
7.2	Project Management Knowledge.....	343
7.3	Roles & Responsibilities.....	345
7.4	Project Management Plan	347
7.4.1	Requirements Management Plan	348
7.4.2	Communications Management Plan	349
7.4.3	Risk Management Plan	351
7.4.3.1	General APD Project Risks	352
7.4.3.2	Recurring APD Process Risks.....	352
7.4.3.3	Common IS Project Risks	353
7.4.3.4	Risk Management and the SDLC	354
7.5	Monitoring and Control	355
7.5.1	State Agency Project Monitoring & Control.....	355
7.5.2	FNS Project Monitoring.....	357
7.6	Project Closure.....	358
7.7	Other Resources	360
7.8	Project Management Summary	361
8.0	Financial Management.....	363
8.1	APD Financial Preparations	366
8.1.1	General APD Funding Requests.....	366



8.1.2	Regulatory Guidance	367
8.1.3	Administrative Requirements	369
8.2	Allocable Costs.....	369
8.2.1	Necessary and Reasonable Costs	369
8.2.2	Direct and Indirect Costs	370
8.2.3	Allowable Costs	370
8.2.4	Unallowable Costs.....	371
8.2.5	Processing Cost Disallowances.....	372
8.2.6	Developmental Versus Operational Costs	374
8.3	Common Cost Items for IT Systems Projects	374
8.3.1	Compensation for Personnel Services (Staff Costs)	374
8.3.2	Outside Contractor Professional Services.....	375
8.3.3	Internal/State IT Professional Services.....	375
8.3.4	Documentation/Materials.....	376
8.3.5	Telecommunications.....	376
8.3.6	Equipment and Other Capital Expenditures	376
8.4	Waivers of Depreciation	377
8.4.1	Software Costs.....	378
8.4.2	Hardware Costs	378
8.4.3	Site Preparation Costs	378
8.4.4	Interest.....	378
8.5	Cost Allocation	379
8.5.1	Division of Cost Allocation Services (CAS)	380
8.5.2	Cost Allocation Stakeholders	381
8.5.3	Cost Allocation Plan	382
8.5.4	Cost Allocation Methodologies.....	382



8.5.5	Indirect Cost Proposals.....	384
8.6	Cost Reviews and Audits	385
8.6.1	Office of Management and Budget (OMB) Responsibilities.....	385
8.6.2	Food and Nutrition Service (FNS) Review	386
8.6.3	General Budget Estimates	387
8.6.4	Operational Budget Estimating.....	389
8.6.5	Completing the Planning Advanced Planning Document Budget	389
8.6.6	Completing the Implementation Advance Planning Document Budget	390
8.6.7	Completing an APDU Budget.....	391
8.7	Expenditure Reporting	391
8.7.1	Revised Project Cost Estimate	391
8.7.2	Actual Costs to Date	392
8.7.3	Program and Budget Summary for SNAP APDs.....	392
8.7.4	WIC Developmental Costs.....	393
8.7.5	WIC- State Agency Management Information System Annual Cost Survey	393
8.7.6	Annual APDU Expenditure Reporting.....	393
8.7.7	Regional Office Expenditure Review	394
8.8	Other Resources	394
8.9	Financial Management Summary.....	395
9.0	Systems Security	400
9.1	Introduction	403
9.1.1	Security Guidance	404
9.1.2	Systems Security Controls	406
9.1.3	IT Security Controls.....	407
9.2	Management Controls	408



9.2.1	IS Security Policy.....	409
9.2.2	Risk Management	410
9.2.2.1	Risk Assessment	410
9.2.2.2	Risk Analysis.....	411
9.2.2.3	Risk Mitigation	411
9.2.2.4	Cost Considerations	412
9.3	Operational Controls	412
9.3.1	Media Protection.....	412
9.3.2	Personnel Security.....	413
9.3.2.1	Separation of Duties	414
9.3.2.2	Security Awareness, Training, and Education.....	416
9.3.3	Physical Security.....	417
9.3.4	Contingency Plans	418
9.3.4.1	Business Continuity Plan.....	421
9.3.4.2	Disaster Recovery Plan.....	421
9.3.4.3	Occupant Emergency Plan.....	422
9.3.4.4	Security Incident Response Plan.....	422
9.3.4.5	Recovery Teams.....	423
9.3.5	Configuration Management.....	424
9.4	Technical Controls	424
9.4.1	Identification and Authentication.....	424
9.4.1.1	Identification.....	425
9.4.1.2	Authentication	425
9.4.2	Logical Access Control	425
9.4.2.1	Logical Access Control Software	426
9.4.2.2	Operating System Security	426



9.4.3	Network Security.....	427
9.4.4	Firewalls.....	427
9.4.5	Routers and Switches	428
9.4.6	Virus Protection Controls.....	429
9.4.7	Penetration Testing	429
9.4.8	Audit	430
9.4.9	Internet and Web Security	430
9.4.9.1	Basic Internet Security Issues.....	431
9.4.9.2	Web Server Security	435
9.4.9.3	Web Browser Security.....	436
9.4.9.4	Mobile Device Security	436
9.5	Privacy Controls	437
9.5.1	Authority and Purpose	437
9.5.2	Accountability, Audit, and Risk Management.....	438
9.5.3	Data Minimization and Retention	438
9.5.4	Individual Participation and Redress.....	439
9.5.5	Transparency.....	440
9.5.6	Use Limitation.....	440
9.6	EBT - Specific Controls	441
9.6.1	EBT Cards.....	441
9.6.2	Encryption.....	441
9.6.3	POS Terminal and ATM Security	442
9.6.4	EBT Security Standards	442
9.7	Security Reviews and Reporting.....	443
9.7.1	Security Plans	443
9.7.2	FNS Security Plan Reviews	445



9.8	Security Summary	446
A1.	Acronyms and Glossary of Terms	450
A1.1	Acronyms	450
A1.2	Glossary of Terms	454
A2.	Regulations.....	468
A3.	Regional Office Information	475
A4.	System Type and Acquisition Selection Tool	479
A4.1	Introduction	479
A4.2	Using this Tool.....	479
A4.3	References.....	479
A4.4	System Type Selection.....	482
A4.4.1	Taking Stock	482
A4.4.2	System Ownership	483
A4.4.3	Resources	483
A4.4.4	Customization	484
A4.4.5	Risk	485
A4.4.6	Data	485
A4.4.7	Standards	486
A4.4.8	Decision Matrix.....	487
A4.4.9	Types of Systems	489
A4.5	Becoming a Cloud Provider	491
A4.5.1	Cloud Broker	492
A4.6	Cloud Deployment Selection.....	493



A4.6.1	Public Cloud	494
A4.6.2	Private Cloud.....	494
A4.6.3	Hybrid Cloud	495
A4.6.4	Community Cloud	495
A4.6.5	Bridging Resource Gaps with Cloud	496
A4.6.6	Cloud Security Control Level	497
A4.6.7	Purchasing SaaS.....	498
A4.6.8	Purchasing PaaS.....	499
A4.6.9	Purchasing IaaS	500
A4.7	Purchasing COTS	501
A4.8	Upgrade Current System	502
A4.9	Transfer an Existing System.....	503
A4.10	Custom Built System.....	504
A5.	Feasibility Study Worksheet	505
A6.	Cost Benefit Analysis Worksheet.....	507
A6.1	Costs.....	507
A6.2	Benefits.....	511
A7.	Sample Transmittal Letter	514
A7.1	Transmittal Letter Template	514
A7.2	Sample Transmittal Letter	516
A8.	Sample Budgets	518
A8.1	Sample PAPD Budget	518
A8.2	Sample IAPD/U Budget	519



A8.2.1	Year One	519
A8.2.2	Year Two	521
A8.2.3	Year Three	523
A8.2.4	Year Four.....	525
A8.2.5	Total Summary Budget	527
A8.3	Total Summary Budget	530
A8.4	WIC EBT/MIS Funding Sources Table	532
A9.	State Sole Source Exception Request.....	533
A10.	Request for Proposal Template	535
A10.1	Introduction	537
A10.1.1	How to Use this Template	537
A10.1.2	RFP and Contract Organization.....	538
A10.2	Template Contents	539
A10.2.1	Part I—The Schedule.....	540
A10.2.1.1	Section A – Solicitation/contract form	540
A10.2.1.2	Section B – Supplies or services and prices/costs.....	544
A10.2.1.3	Section C – Description/specifications/SOW	546
A10.2.1.4	Section D – Packaging and marking.....	554
A10.2.1.5	Section E – Inspection and acceptance	554
A10.2.1.6	Section F – Deliveries or performance	555
A10.2.1.7	Section G – Contract administration data.....	557
A10.2.1.8	Section H – Special contract requirements	557
A10.2.2	Part II—Contract Clauses	561
A10.2.2.1	Section I – Contract clauses.....	561
A10.2.3	Part III—List of Documents, Exhibits, and Other Attachments	565



A10.2.3.1	Section J – List of attachments	565
A10.2.4	Part IV—Representations and Instructions	566
A10.2.4.1	Section K – Representations, certifications, and other statements of offerors or respondents	566
A10.2.4.2	Section L – Instructions, conditions, and notices to offerors or respondents.....	566
A10.2.4.3	Section M – Evaluation factors for award.....	572
A10.3	Alternative RFP and Contract Formats.....	577
A10.3.1	RFP and Contract Format Alternative - Example One	578
A10.3.2	RFP and Contract Format Alternative - Example Two	580
A11.	Federal Procurement Clauses.....	583
A11.1	Equal Employment Opportunity.....	583
A11.2	Clean Air and Federal Water Pollution Control Act.....	583
A11.3	Anti-Lobbying Act.....	583
A11.4	Americans with Disabilities Act.....	584
A11.5	Drug-Free Workplace Statement.....	584
A11.6	Royalty Free Rights to Use Software or Documentation Developed...	585
A11.7	Debarment and Suspension	586
A12.	RFP and Contract Review Checklist.....	587
A12.1	General Review Items.....	587
A12.2	Part 1 - The Schedule	587
A12.2.1	Section A - Solicitation/Contract Form.....	587
A12.2.2	Section B - Supplies or Services and Prices/Costs	589
A12.2.3	Section C - Description/Specifications/Work Statement.....	589
A12.2.4	Section D - Packaging and Marking.....	594



A12.2.5	Section E - Review and Acceptance	595
A12.2.6	Section F - Deliveries or Performance	596
A12.2.7	Section G - Contract Administration Data.....	596
A12.2.8	Section H - Special Contract Requirements	597
A12.3	Part 2 - Contract Clauses.....	600
A12.3.1	Section I - Contract Clauses	600
A12.4	Part 3 - List of Documents, Exhibits, and Other Attachments.....	603
A12.4.1	Section J - List of Attachments.....	603
A12.5	Part 4 - Representations and Instructions	603
A12.5.1	Section K - Representations	603
A12.5.2	Section L - Instructions, Conditions, and Notices to Offerors or Respondents..	604
A12.5.3	Section M - Evaluation Factors for Award	606
A13.	Sample Status Report	608
A13.1	Status Report Checklist	608
A13.2	Cover Page.....	609
A13.3	Document Information	610
A13.4	Executive Summary.....	610
A13.5	Status Overview	611
A13.6	Work Accomplished	611
A13.6.1	Work Completed for Last Reporting Period	611
A13.7	Deliverables in Progress	612
A13.8	Planned Activities.....	612
A13.8.1	Work Planned for Next Reporting Period.....	612
A13.9	What is Going Well?	613



A13.10	Key Issues with Resolution Strategy.....	613
A13.11	Project Deliverable Status.....	613
A13.12	Open Risks.....	615
A13.13	Problem Areas/Risk Mitigation.....	616
A13.14	Project Budget and Actual Expenditures.....	617
A13.15	Contractor Performance Update	618
A13.16	Updated Project Schedule of Milestones and Deliverables.....	618
A14.	Security Plan Checklist.....	619
A14.1	Security Plan Checklist Overview	619
A14.2	System Identification	620
A14.3	Sensitivity of Information Handled.....	621
A14.4	Management Controls	622
A14.5	Operational Controls	623
A14.6	Technical Controls	632
A14.7	Privacy Controls	640
A14.8	EBT Controls	645
A15.	Final Test Plan Template.....	646
A15.1	Introduction	646
A15.1.1	Summary of Final Test Plan Contents.....	646
A15.1.2	How to Use This Template.....	647
A15.2	Template for Test Plan Contents.....	648
A15.2.1	Scope and Purpose.....	648
A15.2.2	Timeline/Milestones	648



A15.2.3	Test Schedule	649
A15.2.4	Testing Resources.....	650
A15.2.4.1	Staffing with Roles and Responsibilities	650
A15.2.4.2	Test Environment.....	652
A15.2.4.3	Support Software	652
A15.2.5	Test Approach	653
A15.2.5.1	Entry / Exit Criteria	654
A15.2.5.2	Pass / Fail Criteria.....	655
A15.2.5.3	Test Suspension / Resumption Criteria	655
A15.2.5.4	Test Criteria.....	655
A15.2.6	Test Cases	656
A15.2.7	Test Scenarios / Test Conditions	657
A15.2.8	Items to be Tested	657
A15.2.8.1	Data Conversion.....	658
A15.2.8.2	System Security	659
A15.2.8.3	Stress/Load Testing	659
A15.2.9	Issue/Defect Tracking and Prioritization	660
A15.2.9.1	Defect Resolution Process.....	660
A15.2.9.2	Regression Testing Process.....	662
A15.2.9.3	Evaluation of Test Progression.....	662
A15.2.10	Risk Management	663
A15.3	Additional Final Test Plan Contents.....	663
A15.3.1	UAT Test Deliverables.....	663
A15.3.2	Go/No-Go Determination Process.....	663
A15.3.3	Roll Back Contingency Plan.....	664
A16.	Ownership Rights.....	665



A16.1	Policy Requirements	665
A16.2	Understanding the Policy.....	665
A16.2.1	Purpose	665
A16.2.2	Supporting the Policy in Acquisitions	666
A16.2.3	Software Ownership	666
A16.2.4	Licensing Principles.....	666
A16.2.5	“Rights in Data” and “Works-Made-for-Hire”	667
A16.2.6	Assistance Provided by State Employee	668
A16.2.7	Public Domain Status	669
A16.2.8	Transferring Software.....	669
A16.3	Applying the Policy - Contractual Provisions.....	670
A16.3.1	Ownership and Licensing	670
A16.3.2	Example Contract Clauses	671
A16.4	Example Clauses for Supporting Transferability	672
A16.4.1	Modular Open Systems Approach (MOSA)	673
A16.5	Inappropriate Intellectual Property Clauses	678
A16.5.1	Limiting State Ownership.....	678
A16.5.2	Use of the Software or resulting work	678
A16.6	Best Practices	678
A16.6.1	Maintaining authority to hold copyright	678
A16.6.2	States Capitalizing on Intellectual Property	679
A16.6.3	Vendor Profiting from Deliverables.....	679
A16.7	Use of Privately Developed Software	679
A16.8	Acceptance of Free Software.....	680
A16.9	Protecting State Agency Ownership.....	680



Table of Tables

Table 1: PAPD Document Submission Thresholds	49
Table 2: IAPD Document Submission Thresholds.....	50
Table 3: Maintenance and Operations Decision Table Examples	51
Table 4: Project Costs and Required Documentation in WIC.....	53
Table 5: APD Types and Purpose	54
Table 6: Examples of Data for DMLC	94
Table 7: APD Federal Review Sample Timetable	117
Table 8: Closure Documentation Requirements	122
Table 9: PAPD Documentation Requirements	127
Table 10: IAPD Documentation Requirements	131
Table 11: Annual APDU Documentation Requirements	137
Table 12: APDU Documentation Submission Thresholds	138
Table 13: APDU As-Needed Documentation Requirements.....	141
Table 14: EAR Required Documentation	144
Table 15: Executive Summary Guidelines.....	152
Table 16: COMPETITIVE – RFP and Contract Document Submission Thresholds.....	177
Table 17: NON-COMPETITIVE - Procurement Contract Document Submission Thresholds.....	178
Table 18: State Agency Roles and Responsibilities	184
Table 19: Sample SNAP EBT Time Frame	189
Table 20: Basic Contract Provisions and Federal Assurances	199
Table 21: Pros and Cons of Contractor Options	220
Table 22: Conflict of Interest Examples	224
Table 23: Feasibility Study Guidelines	250
Table 24: Minimum Alternatives.....	258
Table 25: Alternative Platforms/Capacity Enhancement	260
Table 26: Labor Alternatives	260
Table 27: Alternatives for Acquiring Services	261
Table 28: Gap Analysis.....	264
Table 29: CBA Guidelines	265



Table 30: Use Case Methodology Inputs	302
Table 31: Example Defect Severity Codes.....	308
Table 32: Example of Test Staffing and Training Table.....	310
Table 33: Example of a Test Case Table Listing	317
Table 34: Example Test Scenario and Test Conditions Table.....	320
Table 35: Gold Copy Database Characteristics.....	321
Table 36: Gold Copy Database Capabilities	321
Table 37: QA Interface with the Test Lifecycle.....	331
Table 38: IV&V Typical Task Models.....	332
Table 39: Risk Management in Support of SDLC Phases	354
Table 40: Internet Project Management Resources.....	360
Table 41: Literary Project Management Resources	361
Table 42: Regulations and Policy Governing Financial Management	368
Table 43: SNAP and WIC Timeline for Appeals	373
Table 44: Additional APD Resources	394
Table 45: Security Related Policies and Guidance.....	404
Table 46: IT Security Controls by Category	407
Table 47: Policy Levels and Descriptions	409
Table 48: Risk Mitigation Options	411
Table 49: Separation of Duties.....	415
Table 50: Five Common Cyber Threats	432
Table 51: Internet Security Issues Checklist.....	434
Table 52: Contents of the Systems Security Plan.....	444
Table 53: Regulations	468
Table 54: Key Terms and References.....	479
Table 55: System Type Selection Based on Security to Responsibility.....	485
Table 56: Decision Matrix	487
Table 57: Uniform Contract Format	539
Table 58: Example of Test Schedule	649
Table 59: Example of Test Staffing and Training Table.....	650
Table 60: Example of Support Software Description	653
Table 61: Example of Systems Test /UAT Sample and Tolerance Data.....	656



Table 62: Example of Test Cases and Objectives..... 656

Table 63: Example of Test Scenarios and Test Conditions..... 657

Table 64: Example of Items to be Tested for UAT 658

Table 65: Example of Data Conversion Elements..... 659

Table 66: Example of Defect Identification and Analysis 660

Table 67: Example of Defect Tracking Form Field Definition..... 660

Table 68: Example of Defect Status Description 661

Table 70: Example of Test Progression 662



Table of Figures

Figure 1: Example of Key Points	1
Figure 2: Example of Chapter Contents	2
Figure 3: Example of Chapter Acronyms Table and Cross-Reference to Glossary	2
Figure 4: Example of a Cross Reference Box	3
Figure 5: Endnote Structure	4
Figure 6: Example of a Call-out Box.....	5
Figure 7: Example of a SNAP-Specific Call-out Box	6
Figure 8: Using the Bookmarks Pane.....	6
Figure 9: Advance Planning Document Preparation Activities	56
Figure 10: State Expertise	60
Figure 11: Handbook 901 Mind Map	66
Figure 12: SDLC Phases	73
Figure 13: Management Areas of Focus of the SDLC	76
Figure 14: Common SDLC Activities.....	77
Figure 15: Methodology Decision Factors	79
Figure 16: Waterfall SDLC	80
Figure 17: Agile SDLC	81
Figure 18: PMLC Phases	82
Figure 19: Acquisition Lifecycle Model	87
Figure 20: Contract Management Overview.....	90
Figure 21: Types of System Data	91
Figure 22: Technical vs. Non-Technical Data	92
Figure 23: Data Management Lifecycle	93
Figure 24: Common Lifecycle Phase Types	97
Figure 25: PMLC, ALC, SDLC, and DMLC Alignment.....	98
Figure 26: SDLC, PMLC, and APD Integration.....	101
Figure 27: Overview of PAPD and IAPD Processes.....	109
Figure 28: Major SDLC Activities Related to the APD Process	110
Figure 29: General FNS Review Process.....	114



Figure 30: APD Review Clock.....	116
Figure 31: RFP and Contract Process Review	121
Figure 32: PAPD Process Map	129
Figure 33: IAPD Process Map	135
Figure 34: APDU Process Map.....	139
Figure 35: Emergency Acquisition Request Process Map.....	145
Figure 36: Inappropriate Restriction of Competition	165
Figure 37: Procurement Process Overview	166
Figure 38: FNS Review Process for RFPs and Contracts.....	181
Figure 39: EXAMPLE Order of Precedence	204
Figure 40: Conflicts of Interest	223
Figure 41: Planning Activities for Preparing APDs.....	237
Figure 42: Overview of Initial System Planning	239
Figure 43: Business Capability Definition and the Needs Assessment.....	246
Figure 44: Conceptual SNAP or WIC SOA.....	280
Figure 45: “Complete and Final Test Plan” Milestones	292
Figure 46: Typical Test Lifecycle	299
Figure 47: Testing Milestones	312
Figure 48: Test Cases as a Test Case Suite	319
Figure 49: Testing Process.....	326
Figure 50: The Triple Constraint	339
Figure 51: PM Responsibilities	342
Figure 52: PMI Project Processes	343
Figure 53: Example of a RACI Matrix	346
Figure 54: Example of a Requirements Traceability Matrix.....	349
Figure 55: Lines of Communication	350
Figure 56: Risk Analysis Process	351
Figure 57: The CAM-TOOL for Cost Allocation Methodologies.....	383
Figure 58: Security Level Definitions	411
Figure 59: Staffing and Logical Controls	415
Figure 60: Map of Regions	475
Figure 61: Taking Stock of Current Applications	482



Figure 62: Application Ownership	483
Figure 63: Resources.....	483
Figure 64: Application Customization	484
Figure 65: Risk	485
Figure 66: Types of Systems.....	489
Figure 67: Cloud Service Selection	490
Figure 68: Becoming a Cloud Provider.....	491
Figure 69: Cloud Broker	492
Figure 70: Cloud Deployment Selection	493
Figure 71: Public Cloud	494
Figure 72: Private Cloud.....	494
Figure 73: Hybrid Cloud	495
Figure 74: Community Cloud.....	495
Figure 75: Bridging Resource Gaps with Cloud	496
Figure 76: Cloud Security Control Level	497
Figure 77: Purchase SaaS	498
Figure 78: Purchase PaaS	499
Figure 79: Purchase IaaS	500
Figure 80: Purchase COTS	501
Figure 81: Upgrade Current System	502
Figure 82: Transfer Existing System.....	503
Figure 83: Custom Built System	504



1.0 Getting Started with the Advance Planning Document (APD) Process

Key Points

The information in this section should allow you to understand the following:

- What programs are covered by the Food and Nutrition Service Advance Planning Document (APD) process?
- What is the APD?
- What is the APD process?
- Why is the APD necessary?
- What are the major components of the APD?
- How do the APD and the APD process relate to the Systems Development Lifecycle?
- Who are the major stakeholders in the APD process?
- What legislation, policies, and regulations govern the APD and APD process?

Chapter Contents

1.1	Introduction.....	44
1.2	Introduction to FNS Programs.....	45
1.2.1	Supplemental Nutrition Assistance Program (SNAP)	46
1.2.2	Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)	46
1.3	The Electronic Benefits Transfer (EBT)	47
1.4	Federal Funding	47
1.5	Determining the Need for an APD.....	49
1.5.1	Thresholds	49
1.5.2	Cost Increases.....	52
1.5.3	SNAP EBT Exceptions	52
1.5.4	WIC Exceptions	53



1.6	Introduction to the Advance Planning Document	54
1.7	Introduction to the APD Process	55
1.7.1	Planning Phase	57
1.7.2	Implementation Phase	57
1.7.3	APD Closure	57
1.7.4	Acquisition Document Approvals	58
1.8	Roles and Responsibilities	58
1.8.1	FNS	58
1.8.2	State Agency	60
1.8.3	Project Management	61
1.9	Stakeholders	62
1.9.1	Core Stakeholders - The Project Team	62
1.9.2	Key Stakeholder - FNS	63
1.9.3	Key Stakeholder - State Agencies	63
1.9.4	Other Key Stakeholders	64
1.10	Governance - Legislation, Regulation, Policy (LRP)	65
1.10.1	SNAP LRP	65
1.10.2	WIC LRP	66
1.11	Moving forward with the Handbook 901	66
1.12	Summary	67



Chapter Acronyms

APD	Advance Planning Document
APDU	Advance Planning Document Updates
CFR	Code of Federal Regulations
EAR	Emergency Acquisition Request
EBT	Electronic Benefit Transfer
FM	Financial Management
FFP	Federal financial participation
FNS	Food and Nutrition Service
IAPD	Implementation Advance Planning Document
IS	Information System or Systems – This acronym is used in singular and plural forms.
IT	Information Technology
M&O	Maintenance and Operations
MIS	Management Information Systems
NSA	Nutrition Services and Administration
OA	Operational Adjustment Funds
PAPD	Planning Advance Planning Document
RFP	Request for Proposal
RO	Regional Office
SAM	State Agency Model
SDLC	System Development Life Cycle
SNAP	Supplemental Nutrition Assistance Program
SSO	State Systems Office
TANF	Temporary Assistance for Needy Families
WIC	Special Supplemental Nutrition Program for Women, Infants, and Children



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.



1.1 Introduction

No American should have to go hungry. The Food and Nutrition Service (FNS) works to reduce hunger and obesity through the administration of 15 federal nutrition assistance programs of the United States Department of Agriculture (USDA). These include the Supplemental Nutrition Assistance Program (SNAP), the Special Supplemental Nutrition Program for Women, Infants and Children (WIC). SNAP is the largest of the domestic food and nutrition assistance programs administered by FNS. WIC provides supplemental, nutritious foods, nutrition education, and counseling at WIC clinics. See section **1.2 Introduction to FNS Programs** for more information on these programs. Both programs are administered nationally by FNS and are operated locally by State and local health or human services agencies. FNS' primary focus in its oversight of State systems is to ensure the stewardship of federal funds used to carry out the mission of increasing food security through its domestic nutrition assistance programs. These funds may come from a variety of sources, depending on the program. Different sources of funding may carry different requirements on how the funds may be used and are tracked. State agencies may receive federal funding to develop, acquire, and/or implement Information Systems (IS) that support the operation of FNS programs. State agencies are required to submit an Advance Planning Document (APD) to FNS in order to obtain prior approval to receive or utilize federal funding for IS supporting these programs.

The APD explains the State agency's intended activities and projected expenditures for planning and implementing an IS in *advance* of carrying them out and incurring costs. The "APD Process" is the process in which those documents are submitted to FNS for review and approval, beginning a period of communication and cooperative oversight that will last until the project is complete. Documents will be submitted throughout the project, including planning, procurement and status documents. FNS will review them in accordance with regulations, and may require revisions or clarifications before approving. State agencies may not execute contracts or obligate funds without this approval.



The FNS HB901 provides guidance for USDA APD processes ONLY. It does not provide guidance for APD requirements for other federal agencies that may also be providing Federal financial participation.

The APD process is a series of successive steps through which a State agency can meet federal oversight requirements. These requirements must be met to receive federal written prior approval and Federal financial participation (FFP) for Information Technology (IT) projects. The APD process steps include the preparation, filing, review, approval, and use of the APD and related documents. Such documents will be essential for project



planning, management, and control purposes. The APD process was established by the SNAP Regulation [7 CFR 277.18](#) and adopted by WIC through [7 CFR 246.3\(b\)](#).

The APD process has an impact on a variety of stakeholders. Different roles and responsibilities will be assigned to stakeholders based on their interest and influence on the system in development. These relationships to the APD process and the project will be explored in section **1.6 Introduction to the Advance Planning Document** and section **1.7 Introduction to the APD Process** of this chapter.

FNS Handbook 901 (hereafter referred to as “FNS HB901” or simply “HB901”) is intended to serve as guidance for those State agencies and FNS staff who prepare, review, and/or approve APDs. The HB901 is the primary reference for the FNS APD process.



For purposes of this handbook, the following terms are used interchangeably: Information Systems (IS), Management Information Systems (MIS), and Automated Data Processing (ADP).

For the HB901 and the APD, the “system” is an Information System (IS) intended to support certification, eligibility and their related EBT systems. It may include both hardware and software. Often, systems used to determine eligibility for SNAP and WIC are implemented in conjunction with other health or social services systems. These might include systems to support U. S. Department of Health and Human Services (DHHS) programs such as Medicaid, the Children’s Health Insurance Program (CHIP), Temporary Assistance for Needy Families (TANF), or Maternal and Child Health.² The DHHS also has an APD process. Consequently, in joint projects, State agencies must submit APDs to all federal agencies from which they are requesting FFP and/or grant funding for an IS project.

1.2 Introduction to FNS Programs

The FNS HB901 is a reference and guide for State agencies that administer SNAP and WIC programs. The mission of SNAP and WIC programs is to increase food security and reduce hunger by providing children and low-income people access to food, a healthful diet, and nutrition education in a way that supports American agriculture and inspires public confidence. FNS is committed to the sound stewardship of taxpayer dollars through aggressive efforts to reduce and prevent fraud, and increase efficiency. SNAP and WIC programs have become increasingly complex over the last decade, and they are increasingly reliant on advanced technology solutions to manage program operations. Information systems are essential to State and local agency program administration and operations to ensure continued response to the needs of low-income families while negotiating changing economic conditions and ensuring SNAP and WIC remain vigilant stewards of taxpayer dollars.



1.2.1 Supplemental Nutrition Assistance Program (SNAP)



The Supplemental Nutrition Assistance Program is the cornerstone of federal food assistance programs and serves as the first line of defense against hunger. SNAP offers nutrition assistance to millions of eligible, low-income individuals and families, and provides economic benefits to communities. It began in its modern form in 1961, with origins in the 1930 Food Stamp Plan to help the needy. USDA establishes the Program regulations under the Food Stamp Act of 1977, as amended. As of October 1, 2008, SNAP is the new name of the Food Stamp Program and reflects changes made to meet the needs of clients. It puts healthy food within reach, increases benefit amounts, and makes program benefits more accessible.

SNAP enables low-income families to buy nutritious food with Electronic Benefits Transfer (EBT) cards in authorized retail food stores. SNAP provides crucial support to needy households and to those making the transition from welfare to work. FNS administers SNAP nationally, and State and local human services agencies operate the program locally.



Federal, State, and local governments share the costs of administering SNAP. Congress authorizes the program and appropriates necessary funds. The Federal government fully funds the client benefits of SNAP.

1.2.2 Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)



The WIC program was established by Congress under Section 17 of the Child Nutrition Act of 1966. WIC's objective is to safeguard the health of low-income women, infants, and children who are at nutritional risk. WIC provides supplemental, nutritious foods, nutrition education and counseling at WIC clinics; and screening and referrals to other health, welfare, and social services for members of the following populations:

- Pregnant women (through pregnancy and up to 6 weeks or after pregnancy ends)
- Breastfeeding women (up to infant's 1st birthday)
- Non-breastfeeding postpartum women (up to 6 months after the birth of an infant or after pregnancy ends)
- Infants (up to 1st birthday)
- Children up to their 5th birthday



WIC is a Federally-funded grant program administered by State and local agencies for which Congress authorizes specific amounts of funds each year.

1.3 The Electronic Benefits Transfer (EBT)

Electronic Benefits Transfer is an electronic system used by SNAP and WIC that allows recipients to more easily and efficiently use their benefits. EBT systems operate much like debit card systems by authorizing transfer of government benefits from a federal account to a retailer account to pay for products received.

EBT replaced paper coupons for SNAP in the 1990's, and is rapidly replacing paper checks or vouchers for WIC today. In some States, transition to EBT is still ongoing. EBT has increased security for recipients using their benefits and increased efficiencies for retailers redeeming benefits. In addition, the availability of EBT data has greatly enhanced government oversight of benefits. For more information, see "[General Electronic Benefit Transfer \(EBT\) Information](#)" on the FNS website.[†]



Issuance of SNAP benefits, including EBT, is covered by [7 CFR 274.2](#).



Issuance of WIC benefits, including EBT, is covered by [7 CFR 246.12](#).

1.4 Federal Funding

The purpose of APDs is to request federal funding which may be spent on allowable costs specifically related to implementing, upgrading, operating, and maintaining IS needs for certification, eligibility, and their related EBT

[†] (<http://www.fns.usda.gov/ebt/general-electronic-benefit-transfer-ebt-information>)

systems. It does not include direct appropriations, subsidies, or loans. SNAP and WIC are each funded by different mechanisms.



Full details on managing funds from multiple sources and allowable and non-allowable costs are described in chapter **8.0 Financial Management**.

1.4.1 SNAP and FFP



SNAP is an “appropriated entitlement” program. The federal government is committed to fund all SNAP food benefits and 50% of all allowable administrative costs for regular operating expenses.³ Additional federal funding for an IS project is also available for 50% of costs. A SNAP IS project does not require a special grant award, but does require separate approval. SNAP EBT is funded the same way as a SNAP IS⁴, and requires approval for a State agency to get FFP.⁵

1.4.2 WIC and FFP



WIC is a grant program that is 100% federally funded. Decisions related to the type of funding used will depend on Congressional mandates, availability, application timelines, life of the funds, and FNS priorities. WIC funding is provided to State agencies through three general mechanisms: Nutrition Services and Administration (NSA) funds, Operational Adjustment (OA) funds, and national technology and infrastructure funds. A WIC IS project requires approval of a separate grant or grants.

Nutrition Services and Administration funds are allocated to each WIC State agency through a pre-determined funding formula. These funds are used to pay the operating expenses at the State and local level, including operation of the MIS and food delivery system. Many states also use NSA to pay for at least a portion of technology projects such as program staff time contributed to the IS project.

Operational Adjustment funds are a small percentage of NSA funds allocated by the FNS Regional Offices (RO), to help balance funding priorities across states. Regional offices often award these funds on a competitive basis. For IS projects approved in an APD, State agencies may apply for OA funds through their RO, for a portion or all of the project cost.

National and Infrastructure grants are available for EBT and MIS projects. Annual amounts vary depending on appropriations. State agencies must apply for the funds, and if awarded, must comply with the terms of the grant or cooperative agreement. Terms for technology grants usually include complying with the APD process and with quarterly project and financial reporting requirements.



WIC EBT funding sources are the same as for WIC IS projects. The funding prioritization at the time of application will be applied to WIC EBT and IS projects. This includes NSA, OA, national technology or infrastructure grant funding, and occasionally, State funding resources.⁶ Contact the FNS Regional Office for additional information on funding and FNS priorities. A State agency may submit a grant request for a national technology grant at any time.

1.5 Determining the Need for an APD

State agencies should always contact FNS to confirm if they need to go through the APD process. Determining requirements will differ depending on the program requesting the funds and the project they are planning. However, there are three main factors State agencies can consider to determine if they need to proceed using the APD: Thresholds, Maintenance and Operations, and Cost Increases. The following sections briefly describe how and when these apply, and to whom.

1.5.1 Thresholds

1.5.1.1 Planning

When the State agency wishes to utilize federal funding for planning costs, Planning Advance Planning Documents (PAPDs) are required whenever the anticipated cost of the project exceeds the specified threshold for certification, eligibility or EBT systems. For all project types, even if the total project cost is not expected to exceed the threshold, the State agency is advised to notify FNS by communicating its plans so that FNS is aware of IT efforts and can confirm if approval is needed. **Table 1: PAPD Document Submission Thresholds** indicates the funding thresholds for each program. Except in unusual circumstances, significant hardware or software development costs will be ineligible for funding during project planning, although incidental hardware and software that supports the planning process may be approved.

Table 1: PAPD Document Submission Thresholds

Stakeholder		Program/Funding Source			
State Agency	FNS	SNAP	SNAP EBT	WIC	WIC EBT
Prepares and submits PAPD at least 60 days before project initiation	Reviews within 60 days	For all projects ≥\$6 million total project costs	For all projects requesting FFP for new technology	For all projects ≥\$1,000,000 utilizing federal funding*	For all projects requesting FFP for new technology
*See Table 4 for requirements at lower thresholds					



Although State agencies cannot know the total anticipated project cost before conducting the planning phase, it is reasonable to assume that a complete system replacement, transfer, or major upgrade will exceed the threshold. State agencies must make a good faith effort to anticipate the scope of their intended project, and submit the appropriate documents for approval. If in doubt, a PAPD should be submitted to assure that planning costs are approved. State agencies should assume that incremental efforts which may be under approval thresholds individually, but which support a unified outcome, will be regarded by FNS as a single project, and that a cumulative threshold will apply.

1.5.1.2 Implementation

After the planning phase is complete, should the State agency decide to proceed with project execution, an Implementation Advance Planning Document (IAPD) may be required. An IAPD must be submitted for all IS projects requesting or utilizing FFP, regardless of whether a PAPD was submitted or approved, in accordance with the established dollar thresholds for the program. **Table 2: IAPD Document Submission Thresholds** indicates the funding thresholds for each program. Failure to submit an IAPD may result in the disallowance of costs that might otherwise have been covered by federal funds.

Table 2: IAPD Document Submission Thresholds

Stakeholder		Program/Funding Source			
State Agency	FNS	SNAP	SNAP EBT	WIC	WIC EBT
Prepares and submits IAPD at least 60 days before project initiation	Reviews within 60 days	For all projects $\geq$ \$6 million total project costs	For all projects requesting FFP	For all projects $\geq$ \$1,000,000 utilizing federal funding*	For all projects requesting FFP
*See Table 4 for requirements at lower thresholds					

1.5.1.3 Maintenance and Operations

The State agency moves into the Maintenance and Operations (M&O) phase of the System Development Lifecycle (SDLC) when the implementation phase is complete. FNS does not require annual APD Updates to approve the funding of maintenance and operations activities. This includes work that supports the continued operation of an existing IS without adding significant new functionality, such as routine hardware and software replacements or routine upgrades. However, prior approval of an APD is required for M&O when significant platform changes or software enhancements are made to the system. **Table 3: Maintenance and Operations Decision Table Examples** provides examples to help determine the need for APDs and associated procurements.



Enhancements are modifications that will change the functions of software and hardware beyond their original purposes. Enhancements are not meant to correct errors or deficiencies which may have been present in the software, or hardware, or to improve operational performance of the software or hardware. Specific examples include adding new software components, transitioning to web-based systems, and implementing enterprise architecture or systems.

Table 3: Maintenance and Operations Decision Table Examples

IAPD Required		IAPD Not Required
Software	Software enhancement adds new functionality to the existing certification/eligibility or issuance system	Routine software maintenance, including fixes, patches, and upgrades that do not introduce additional functional capabilities to the system
	Implementation of Enterprise Architecture	Routine software license renewals
		Routine support activities that normally include corrective, adaptive, and perfective changes, <u>without introducing additional functional capabilities</u>
Services	Consultant services are used to develop and implement software upgrades to an existing system that adds new functionality to the system	Contract for routine M&O services is due to expire; SOW does not include enhancements or upgrades to software that will add functionality to the system [‡]

Even if the planned changes do not meet these criteria, the State agency should keep FNS informed during the M&O phase. This may be satisfied by submission of the procurement documents along with a transmittal letter signed by the State official who has authority to commit State resources. Once it appears that a software enhancement will substantially increase risk, cost, or functionality, it may trigger an IAPD or APD Update As-Needed.

[‡] Even purchases which do not require approval in an APD must be procured through free and open competition. Request for Proposals (RFPs) and contracts are subject to FNS approval.

1.5.2 Cost Increases

1.5.2.1 SNAP Cost Increases



In the event that a SNAP project originally estimated to cost less than \$6M encounters changes in scope or price that increase total costs to exceed that threshold, the State agency must submit an APD to FNS for approval of the entire project, not just that portion over the \$6M threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements are addressed when submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and also avoid or shorten any project slowdown during the approval process.

1.5.2.2 WIC Cost Increases



In the event a WIC project originally estimated to cost less than the \$1,000,000 threshold encounters changes in price or scope that increase the cost to exceed the threshold, the State agency must submit an APD to FNS for approval of the entire project, not just that portion over the \$1,000,000 threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements are addressed when submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and also avoid or shorten any project slowdown during the approval process.

1.5.3 SNAP & WIC EBT



The APD process for SNAP and WIC EBT differs from the process for eligibility and certification systems. For example, PAPDs, Planning RFPs, and full IAPDs are not required when simply transitioning from one EBT processing contract to another (even with the same vendor). Please note that a PAPD is required for EBT systems if the State is exploring new technology or expects to incur excessive planning costs. Therefore, it is important to consult with FNS before initiating any planning activities. When the State is moving EBT to new technology, or incorporating enhancements or upgrades that significantly change the architecture and interface requirements or functionality of issuing benefits electronically, these changes must be submitted in an IAPD for approval. Otherwise, when simply transitioning from one contract to the next for ongoing EBT operations in SNAP, the IAPD is submitted after the contract is signed. Consult with the FNS Regional Office (RO) or State Systems Office to help make this determination.

1.5.4

WIC MIS



Because WIC is a grant program with limited funding, IS projects which fall below the threshold of \$1,000,000 for a full IAPD still require notice to, or approval by, the FNS RO at various cost levels. However, a less comprehensive set of documents or information is required at lower costs. See **Table 4** for applicable thresholds.

Table 4: Project Costs and Required Documentation in WIC

Project Cost	Documents Required from State Agency
<\$5,000	No federal review needed for IS
\$5,000 to \$99,999	Written notification to the RO within 60 days of the expenditure or the contract execution
>\$100,000 Non-Competitive Acquisition	Sole source justification submitted to FNS for approval prior to acquisition
\$100,000 to \$999,999	Specific documentation required for FNS prior approval Description of needs Explanation of purchases Budget Cost allocation proposal [§] Procurement documents (e.g., RFPs and contracts)
≥\$1,000,000	State agency must submit a complete PAPD and IAPD

Non-competitive acquisitions below \$250,000 for WIC projects are allowable without prior approval as long as they meet the State agency's procurement requirements. FNS will require justification for any sole source procurements that exceed this amount. The State agency will be responsible for any non-competitive costs incurred without prior approval from FNS, and these costs will be subject to disallowance.



See appendix **A9** for the **State Sole Source Exception Request** required by FNS.

[§] If any systems acquisition is to be used for non-WIC functions, a cost allocation proposal must be submitted.

1.6 Introduction to the Advance Planning Document

The Advance Planning Document (APD) is made up of several documents such as a budget, schedule and management plan, produced by a State agency. Many of these documents are generated as the State agency proceeds through the activities of planning, implementing, and operating an IS in support of certification, eligibility, and EBT systems. Systems development or acquisition, whether in the public or private sector, goes through a detailed process of planning, analysis, preparation, budgeting, and negotiation. These processes, which are part of the APD process, closely correspond to the SDLC. However, the SDLC is not the same as the APD process.



The APD process itself, while dependent on the SDLC, encompasses the submission, review, approval, and continued updating of the APD until the completion of the planning and/or implementation of the SNAP, WIC, and/or EBT system.

In the broadest terms, the SDLC is the overall process of developing a system through multiple phases, from investigation of initial requirements through analysis, design, implementation, upgrades, modifications, maintenance, and disposal. The planning and implementation of a system can take years. The useful life of the system will span many years. Maintenance, upgrades, and modifications to keep system capabilities current with technology advancements may require multiple projects. SNAP, WIC, and EBT policy changes will also drive the need for system upgrades and modifications. Any of these may trigger the need for an APD and its type as it relates to where in the system's life cycle the needed activities are occurring. See section **1.5.1 Thresholds** for more information on triggers for APDs.



For a detailed look at the SDLC and how it aligns with the APD, see chapter **2.0 Lifecycle Management**.

The two types of APDs, PAPD and IAPD, address all of the SDLC activities and requirements. As outlined in **Table 5**, each type of APD is devoted to a specific purpose and activities performed under each of the SDLC phases directly feed information into the related APD. There are also two types of APD Updates (APDUs): APDU Annual and APDU As-Needed. The APD process also includes an Emergency Acquisition Request (EAR) to use in times of emergency or disaster situations.

Table 5: APD Types and Purpose

Type of APD	SDLC Phase	Purpose

1.6 Introduction to the Advance Planning Document

1.0 Getting Started with the Advance Planning Document (APD) Process

54

Table 5: APD Types and Purpose

Planning APD (PAPD)	Initiating (Planning)	A PAPD specifies the nature of the planning effort, including plans to investigate the feasibility, system alternatives, requirements, and resources needed to move forward with system development.
Implementation APD (IAPD)	Development and Implementation	An IAPD addresses the outcome of the feasibility study, and plans for design, development, integration, testing, and deployment activities; completes the planning phase; requests funding to conduct implementation activities.
Annual APD Update (APDU)	Planning or Implementation	An APDU is an update to an ongoing project and is required annually when planning or implementation activities occur for more than 1 year.
APDU As-Needed	Planning or Implementation	An APDU As-Needed is an update for unexpected project changes that significantly affect project costs, schedule or scope, for which the State agency is seeking approval prior to the next annual update.
Emergency Acquisition Request (EAR)	Development and Implementation	An EAR requests immediate funding for hardware, software, and/or services in emergency situations in which program operations would be interrupted or extremely hindered. An IAPD must follow within 45 days. A PAPD is not required.

1.7 Introduction to the APD Process

Several requirements must be met in preparing an APD for a program's system needs. These requirements originate from the relationship to dollar thresholds established in law and regulations, types of action/approval sought, program funding source, or amount of funding sought.

To identify which steps of the APD process to follow, a State agency must determine the SDLC phase, the type of acquisition or services being sought, and the particular program requirements (e.g., thresholds, documentation) that apply. The State agency must also determine whether the estimated total cost exceeds the program thresholds, including the cost of equipment and service resources acquired from State, commercial, and other sources. State agencies are encouraged to consult with FNS as frequently as needed. FNS views the APD process as a Federal-State partnership and strives to implement a team effort in carrying out the requirements of the process.



This section is an introduction to the APD process. Full details on the APD process, required documentation, and the FNS review process are described in chapter **3.0 The Advance Planning Document Process**.

Figure 9 shows the top-level activities necessary to prepare both the PAPD and the IAPD. There are many details that go into preparing the APDs and going through the APD process. What follows is a simple introduction to the overall process. Chapters 2 through 4 provide details for the overview described below.

It is important to note that before any APD activity occurs, when a State agency first identifies a need or opportunity, a needs assessment must be conducted to determine the extent and urgency of the need and whether the time is right to address it. The needs assessment occurs prior to the Planning Phase. The needs assessment is intended to assist decision makers in developing the case to move forward with planning activities that are essential to defining the scope of the project, acknowledges future funding and staffing priorities, as well as acquiring the desired resources. A needs assessment will help the State agency determine whether or not the project is necessary. If the State decides the project is necessary, they must determine the need for an APD and what type of APD is required. Regardless of the outcome of the needs assessment, the State agency should consult with FNS in making a final determination on how to proceed. The approved PAPD approves funding to conduct the planning activities.

Once all the planning activities in the approved PAPD are completed, the IAPD is submitted and the PAPD is closed. It is possible that the planning resulted in a decision not to proceed with a project. However, more commonly, the decision is to implement. Implementation activities begin once the IAPD is approved. The approved IAPD is also the approval of funding for the implementation activities in SNAP. Additional grant approval may be required in WIC.

Because planning and implementation often take more than one year, APDUs are an important part of the APD process. They are the basis for continued federal funding and provide a means to make adjustments to the approved APD based on project realities such as actual expenses and schedule adjustments.

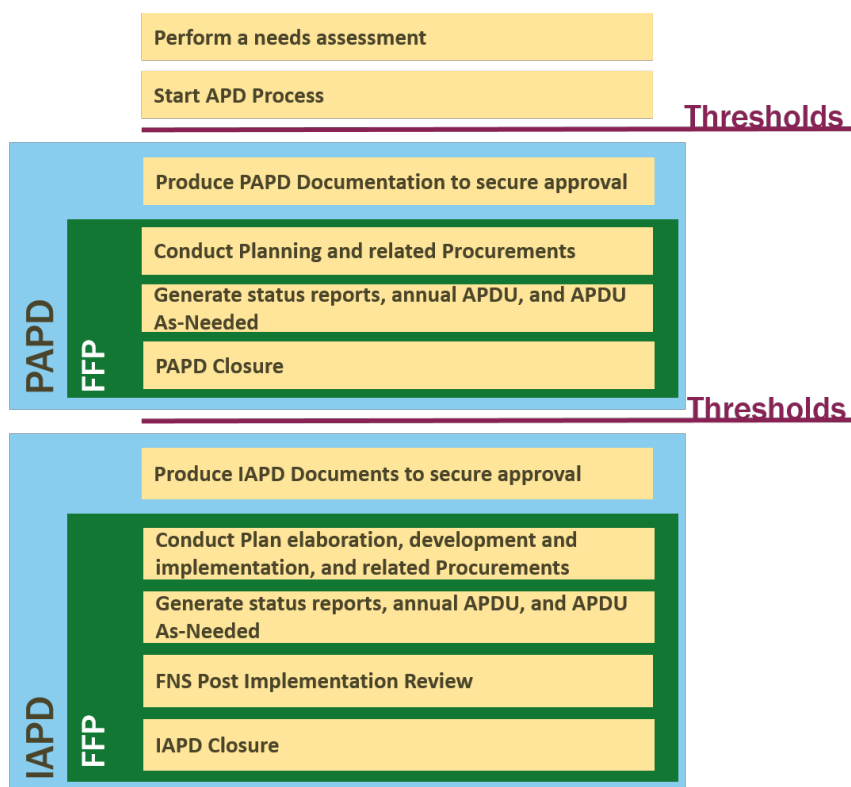


Figure 9: Advance Planning Document Preparation Activities



1.7.1 Planning Phase

After completing the needs assessment, if the State agency decides to proceed with a planning process after consulting with FNS, it creates the PAPD. The PAPD is electronically submitted to the appropriate FNS RO with a courtesy copy to the FNS State Systems Office (SSO). FNS will begin its review, and may request additional information or clarification from the State agency. After reviewing all of the information, FNS will make a decision and provide it to the State agency in writing. Once an approval letter is received, the State agency may proceed with the planning activities. If the planning activities will take more than one year, the State agency must update FNS annually with an APD Update (APDU). The planning phase activities include the SDLC planning activities. Project planning, resource determination, cost estimating, and budgeting are also part of the planning process. Each of these SDLC planning activities will produce documents describing the results of planning efforts. These documents become the basis for compiling the Implementation APD for submission.

1.7.2 Implementation Phase

After completing the planning phase in accordance with the approved PAPD, the State agency and FNS will determine whether to proceed with a project. Assuming that planning activities support implementation, the State agency begins preparing the IAPD. The IAPD, as a “document of documents,” is compiled using the results of the planning phase. The process for the IAPD is similar to the PAPD, except that the required components are more extensive. The State agency creates the IAPD and submits it electronically to the appropriate FNS RO with a courtesy copy to the SSO. FNS will begin its review, and may request additional information or clarification from the State agency. After reviewing all of the information, FNS will make a decision and provide it to the State agency in writing. Approval is required before the State agency proceeds with any of the implementation activities described in the IAPD. The implementation phase activities include the SDLC activities for development, testing and implementing the system, to include user acceptance testing, pilot testing the system, and accomplishing full roll-out. All of these SDLC activities are monitored for how closely they follow the activities described in the approved IAPD. If the implementation activities will take more than one year, the State agency must update FNS annually with an APD Update (APDU).

1.7.3 APD Closure

Both the planning phase and the implementation phase will eventually end. When planning or implementation activities are completed, the State agency must submit a final APDU. USDA will confirm all activities are complete as described in the approved APD (PAPD or IAPD), to include any approved APDUs. Once confirmed, FNS and the State agency may close the APD. This step is necessary to officially end all approved activities, document actual costs incurred, and terminate federal funding activities.



1.7.4 Acquisition Document Approvals

The State agency may decide to use contractor support to perform parts of the planning or implementation activities. This requires the use of requests for proposals (RFPs) and contracts. Based on expected contract costs, the State agency may be required to submit the RFPs and contracts to FNS for review and approval based on the thresholds for the contracts. This is part of the APD process. RFPs and contracts go through a similar submit, review, and approval process as APDs. The State agency is required to obtain prior approval before releasing RFPs and signing contracts resulting from the source selection process.



Full details on procurement thresholds and the FNS review process for procurements are described in chapter **4.0 Procurement**.

1.8 Roles and Responsibilities

The State agency and FNS have the primary responsibilities in the APD process. The State agency administers FNS programs, depending heavily on IS. The FNS SSO is responsible for coordinating the review and approval process for APDs. The SSO is a State agency's initial point of contact regarding the APD process or State systems issues. The SSO collaborates with the program (WIC or SNAP) and Financial Management (FM) entities in the FNS ROs and headquarters. The SSO also works to provide consistency and collaboration within FNS and between federal agencies.

1.8.1 FNS

FNS expertise parallels and supports State expertise in program management, project management, FM, and IT. All these disciplines work as a team, providing general management and decision-making skills.

In addition, FNS RO and headquarters staff are available to answer questions and provide technical assistance to any State agency that requests additional help, such as the following:

- Providing guidance in developing APD documents
- Overseeing the APD process for State agencies; coordinating all phases of the process on behalf of FNS with the State agency and monitoring progress under approved APDs
- Reviewing and rendering decisions on all APDs and required documentation submitted in accordance with established guidelines and time frames
- Assisting with analysis process to determine “best fit” hardware/software
- Providing most up-to-date policy, procedures, and requirements



- Knowing what systems, hardware, and software other States are using/developing
- Reviewing hardware/software requests with focus on costs and support of existing system
- Clarifying technical terms found in documents
- Interfaces with other federal agencies
- Providing information on conferences and/or training opportunities
- Conducting or participating in project meetings, conference calls, or both to discuss items of concern to one or more States, as necessary
- Approving specific program waivers (SNAP only)
- Coordinating and conferring with other federal partners during approval process to ensure consistency
- Arranging visits to State agencies during the project life cycle, especially during testing, pilot, and roll out, as appropriate
- Arranging dates and preliminary agenda for post-implementation reviews and preparing final reports, including any corrective action requirements, as necessary
- Providing technical assistance (e.g., training, acceptance testing, budgeting, and cost allocation)
- Responding to official requests regarding the APD process or APDs (e.g., Freedom of Information Act (FOIA), General Accounting Office (GAO))
- Officially closing APDs

1.8.2 State Agency

The responsibility for administering FNS programs and ensuring compliance with federal rules and regulations resides with State agency partners, including Indian tribal organizations. These agencies often use IS as a key mechanism to carry out their responsibility to provide efficient and effective program administration, such as accurately determining eligibility and benefit levels, generating reports to monitor and assess program activities, trends, and expenses, and combating fraud.

State expertise (see **Figure 10**) typically should include program management, project management, FM, and IT staff. All these disciplines work as a team, providing general management and decision-making skills as well as subject matter areas of expertise.

State agency responsibilities include the following:

- Administering FNS programs
- Identifying program needs or requirements best addressed through IT
- Assessing the planning and implementation steps to successfully meet these needs
- Preparing and submitting necessary documentation to appropriate federal agencies to secure approval of IS projects and federal funding
- Implementing IT plans
- Conducting the overall project and the integration of system solutions
- Managing all aspects of the systems project throughout its life cycle, including reporting, project management, financial management, and risk management
- Demonstrating through thorough testing that the system meets all program functional and performance requirements



Figure 10: State Expertise



- Ensuring active involvement and communication with the State's oversight/executive committee at all stages of the SDLC
- Tracking and reporting on project funds
- Responding to FNS requests and updating APD documentation when needed
- Ensuring fair and open competition in the procurement process and in managing contractors
- Enforcing contract provisions; including boilerplate requirements, key personnel clauses, program-specific requirements, and performance guarantees
- Adhering to federal requirements for status reports, State plans, funding process requirements, and policy implementation

1.8.3 Project Management

It is important to have a defined formal structure for the project and for the project staff. This provides each individual with a clear understanding of the authority given and responsibility necessary for the successful accomplishment of project activities. Project team members need to be accountable for the effective performance of their assignments and achievement of the project goals and objectives.

The roles and responsibilities of project participants will vary, but a successful project team requires:

- Implementing effective project management, with an emphasis on strong leadership and a structured project environment
- Chartering the project at the outset, stating the objective and business benefits and timescales for delivery
- Ensuring supportive sponsorship throughout the project, at a high enough level within the organization to overcome obstacles both within and outside the organization
- Providing authority to complete a project
- Promoting participation (at some level) in the planning process
- Cultivating ownership of and buy-in to the project management plan
- Assigning responsibility and accountability for completion of the project
- Ensuring strong, committed executive management support
- Connecting the business goals to IT
- Communicating objectives frequently
- Establishing clearly defined principles so that no one is unsure about how to proceed
- Reviewing projects often to determine whether they are yielding the expected benefits
- Recognizing different perspectives to reflect the concerns and interests of the various stakeholders
- Being proactive

- Giving IT and program subject matter experts a seat at the business table
- Recognizing that everyone shares success; just as stakeholders have specific interests, they also all contribute to the success of the projects

The requirements placed on participants will be determined and defined during the project management planning process. However, a good “rule of thumb” is that the project manager should be full-time and have no other significant responsibilities except to manage the project. On a large project, individual role assignments may require full-time attention to the function. For smaller projects, role assignments may be performed part-time, with staff sharing in the execution of multiple functions.

1.9 Stakeholders

Stakeholders are individuals and organizations who have a vested interest in the success of the project. The identification and input of stakeholders helps to define, clarify, drive, change, and contribute to the scope, cost, timing, quality, and ultimate success of the project. To ensure project success, the project management team needs to identify stakeholders early in the project, determine their needs and expectations, and manage and influence those expectations over the course of the project. Ensuring accountability, efficiency, and effectiveness in program operations requires a commitment to quality service from all key stakeholders.

By using FNS HB901 to implement the APD process properly, and working in partnership with FNS, each stakeholder plays its part in implementing effective and efficient IS to administer the SNAP and WIC programs.



Refer to appendix **A3 Regional Office Information** for a list of FNS Regional Offices.
Please consult the FNS website for the most current information.
(<http://www.fns.usda.gov/apd/>)

1.9.1 Core Stakeholders - The Project Team

The project team is comprised of the core stakeholders with whom other key stakeholders interact and participate. Being primarily responsible for the success of the project, the project team has the most immediate stake in the outcome of the project, making them core stakeholders. They are the focus of all activity and are the people held directly responsible for the project. Coordinating the activities of other key stakeholders, and working to achieve the goals of the key stakeholders, further emphasizes the importance of the project team as the core stakeholder.

A project team includes a diverse combination of people who share the responsibility for accomplishing project goals and managing the performance of the project work activities and typically includes the following members:



Project Sponsor—Defines and initiates projects and hires or assigns project managers to manage cost, schedule, and performance of component projects, while working to ensure its ultimate success and acceptance. The project sponsor maintains continuous alignment of program scope with strategic business objectives and makes recommendations to modify the program to enhance effectiveness toward the business result or strategic intent. The project sponsor is responsible for determining and coordinating the sharing of resources among his/her constituent projects to the overall benefit of the program.

Project Director—Responsible for strategic planning and decision making, as well as fiscal responsibilities for the project. This provides a separation of duties from the daily project management provided by the project manager. A project sponsor may serve as a project director but not as a project manager.

Project Manager—Responsible for leading the team through the SDLC activities and has ultimate responsibility for project success. The project manager is also responsible for reviewing deliverables for accuracy, approving deliverables, and providing status reports to management.

Project Team—Team members (State program, FM and IT staff; and their contractors) are responsible for accomplishing assigned tasks as directed by the project manager or per Federal and State regulations.

A project team may work in the same location or may be separated by distance and function as a virtual team (i.e., fulfills its project obligations with little or no time spent face-to-face). In order to ensure that all team members have clear expectations of proper behavior, it is important that ground rules for roles, responsibilities, and expectations, be established at the beginning of a project and addressed in the project management plan.

1.9.2 Key Stakeholder - FNS

FNS establishes overall program policy and provides guidance and technical assistance to State agencies. FNS accesses data and State IS and uses reports generated by State IS to meet federal reporting requirements. These reports assist FNS in allocating funds, developing national statistics for program evaluation, and ensuring that its programs meet intended objectives. FNS provides advice and consent to State agencies on the APD process, approval requirements, and lessons learned in other state projects.

1.9.3 Key Stakeholder - State Agencies

State agencies represent the interests of the millions of needy households receiving benefits from SNAP and WIC. In providing benefits to eligible people, the State agencies have a vested interest in the success of projects which support program operations. They provide the project teams, support staff, and other State resources needed to ensure success. The State agency's success in completing the APDs and the APD process directly impacts the outcomes for the effective and efficient delivery of SNAP and WIC benefits using IS to administer these programs.



1.9.4 Other Key Stakeholders

FNS works closely with many federal agencies outside of the USDA that provide services to low-income families; have responsibility for health, nutrition, or education policy; and have a stake in State IS. Among these are a variety of agencies within the DHHS. DHHS agencies include the Administration on Children and Families (ACF), Centers for Medicare and Medicaid Services (CMS), and the Maternal and Child Health Bureau. Other federal partners include the Social Security Administration (SSA), and the Department of Education (DoED).

In addition, FNS works with a wide range of professional and academic organizations, private sector firms, and private non-profit organizations at the local, State, and national levels. Organizations representing program partners and cooperators, businesses such as the retail food and banking industries and various agriculture producer groups, and public interest advocates, all play a critical role in sustaining the effectiveness of these programs.

1.9.4.1 Federal Stakeholders

DHHS funds and oversees several programs that are complementary and important to FNS, following the same general rules and guidelines for federal funding provided in FNS HB901. These programs may be integrated within the same systems as SNAP at the State level, and in many cases are combined into a single eligibility process at the local/customer level. A single worker may take in a huge amount of eligibility data and then process the application to determine eligibility for many programs. These joint systems are often completely integrated, and the process of oversight has to be coordinated between FNS and DHHS. Each federal agency is responsible for review and approval of its own costs and federal funding participation in State IS projects.

1.9.4.2 Financial Institutions and EBT Processors

Financial institutions or processors play an important role in the redemption and reconciliation of FNS-issued benefits. The EBT Processor transmits redemption data to FNS, performs settlement to State or federal accounts, generates electronic funds transfer payments to retailer financial institutions, and transmits redemption information to the State agency. Additionally, the EBT Processor maintains account information, posts benefits, processes benefit transactions to the household account, or processes WIC claims submitted by WIC vendors, and provides transaction reports to the State agency. In many states, WIC uses paper checks. The redeemed checks (a.k.a. food instruments) or reports of redeemed food instruments are provided to the IS by banks or other financial service organizations, which are in turn used to generate food benefit reconciliation reports. Banks play an important role in screening the redeemed checks to support retailer compliance for a number of required fields. Examples include ensuring the food instrument was filled in correctly, signed, dated, and redeemed within the allowable time period.



1.9.4.3 Retail Vendors

Retailers** are key to program access and integrity; by providing allowable foods, abiding by program policy and, in some cases, pricing guidelines. In an EBT environment, vendors are relieved of much of the in-lane food purchase screening, and payment submissions are streamlined. For WIC, foods are scanned and matched to a State agency Authorized Product List prior to purchases. IS and EBT implementations must coordinate with retailer vendors to ensure benefits are not disrupted during processor or IS provider transitions.

1.9.4.4 Food Manufacturers and WIC



For WIC, infant formula manufacturers are the main source of rebates to the State agencies. In some States, cereal and juice manufacturers provide rebates as well. The WIC IS or EBT system produces reports that are provided to manufacturers to support rebate billings. With EBT, WIC IS receives more timely and accurate redemption data, which provides rebate data for food manufacturers and more efficiently handles the rebate process.

1.10 Governance - Legislation, Regulation, Policy (LRP)

State agencies must familiarize themselves with applicable Legislation, Regulations, and Policies (LRP) prior to beginning the APD process. In conjunction with this handbook, it is important to be familiar with the LRP pertaining to each FNS program. FNS HB901 provides only a brief overview of the relevant LRP for each program. The purpose of this handbook is to ensure compliance with federal regulations, preserve the oversight of federal funds, and enable State agencies to determine their IS needs and manage these costly projects effectively and efficiently.

1.10.1 SNAP LRP



SNAP rules (regulations) are published by the Federal Register in the Code of Federal Regulations (CFR), Title 7 CFR Parts 271 through 283.

** In WIC Retailers are known as Vendors

1.10.2 WIC LRP



WIC rules (regulations) are published by the Federal Register in the CFR, Title [7 CFR Part 246](#). Additional policies for WIC are included in 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.⁷



See appendix **A2 Regulations** for full descriptions of applicable governance for SNAP and WIC.

1.11 Moving forward with the Handbook 901

As described in this chapter, the FNS HB901 is a reference tool and guide for State agencies embarking on the APD Process. FNS provides technical assistance and performs oversight of State agencies to ensure their modernization efforts and other initiatives deliver program benefits effectively and efficiently by way of the Advance Planning Document. The objective of the APD is to ensure these projects are implemented in a successful manner that maintains or improves program operations while meeting the requirements for FFP. The submission, review, and disposition is a series of successive steps known as the “APD process.”

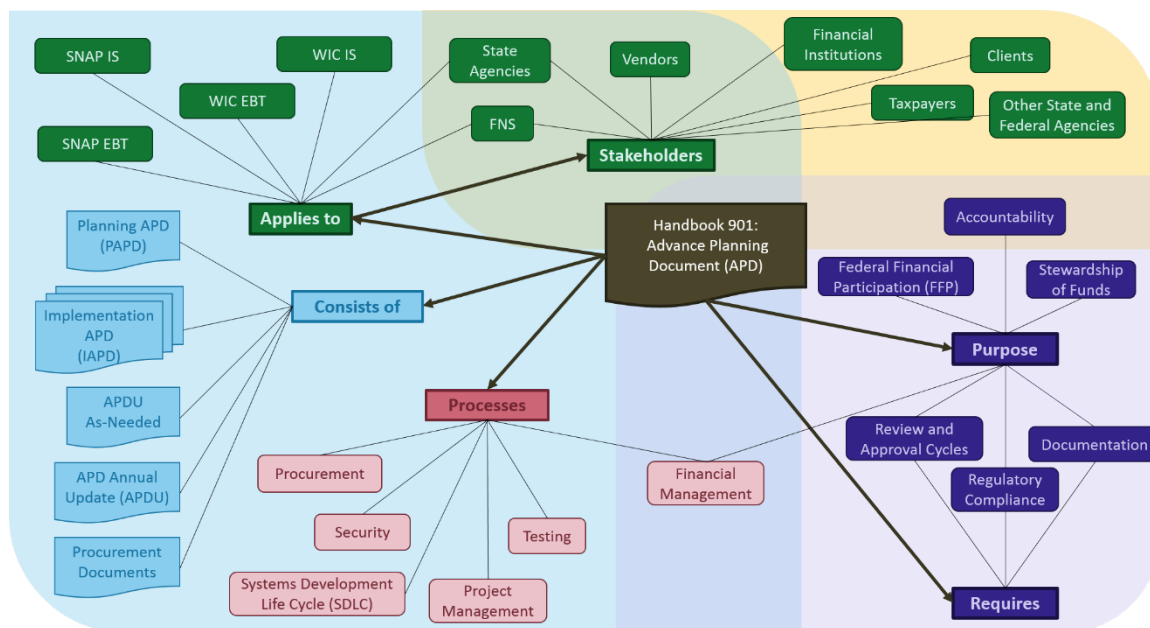


Figure 11: Handbook 901 Mind Map



This getting started chapter has provided an overview of the Purpose, Processes and Parts of the APD, as well as the people and organizations involved. These interactions are mapped out in Figure 11.

The following three chapters outline in detail how State Agencies interact with and apply the APD Process:

- **Lifecycle Management** (chapter **2.0**) - A discussion on scheduling, timelines, methodologies, and the activities required to adequately plan a project
- **The Advance Planning Document Process** (chapter **3.0**) - A detailed exploration of the specific APD Documents and the Submittal, Review, and Approval needed in order to obtain FFP
- **Procurement** (chapter **4.0**) - Guidance for conducting procurements in conjunction with the APD process

FNS also provides technical support to strengthen project management, financial management, and other technical aspects in order to reduce the risk of project failure and improve project outcomes. FNS encourages States to consider ways to improve program administration and operations.

Chapters 5 through 9 of this handbook address these important supplementary practices:

- **System Planning** (chapter **5.0**) - An examination of what to consider when preparing to implement a system, in order to create a successful solution to meet certification and eligibility program needs
- **Test Planning** (chapter **6.0**) - Guidance for test planning and development of the FNS-required test plan
- **Project Management** (chapter **7.0**) - Overview of project planning and project management principles
- **Financial Management** (chapter **8.0**) - Guidance for budgeting, cost allocation, and financial reporting
- **Systems Security** (chapter **9.0**) - General guidelines for system and data security

Following the chapters is a comprehensive appendix section. The appendices offer ancillary information and guidance, as well as functional content such as the glossary, sample forms, budgets, templates, checklists, and supplemental information.

1.12 Getting Started Summary

- SNAP and WIC are two FNS nutrition assistance programs eligible for Federal financial participation for IS
- State agencies may receive federal funding to develop, acquire, and/or implement information systems that support the operation of FNS programs
- The APD produced by a State agency is made up of several documents generated as the State agency proceeds through the activities of planning, implementing, and operating an IS in support of certification, eligibility, and EBT systems



- The APD documents include a budget, schedule, and management plan for planning and implementation activities
- The “APD Process” is the process in which those documents are submitted to FNS for review and approval, beginning a period of communication and cooperative oversight that will last until the project is complete
- The APD explains the State agency’s intended planning and implementation activities and projected expenditures for an IS in *advance* of carrying them out and incurring costs
- APDs are required whenever the anticipated cost of the project exceeds the specified threshold for certification, eligibility, or EBT systems
 - State agencies are required to submit an APD to FNS to obtain prior approval to receive or utilize federal funding for IS supporting these programs
 - FNS works closely with many federal agencies outside of USDA that have a stake in State IS who have separate APD processes
- The APD processes closely correspond to, but are not exactly the same as the SDLC
- State agencies must familiarize themselves with applicable legislation, regulations, and policies prior to beginning the APD process
- FNS Handbook 901 is intended to serve as guidance for those State agencies and FNS staff who prepare, review, and/or approve APDs
 - ***The Advance Planning Document Process*** (Chapter **3.0**) provides detailed exploration of the specific APD Documents and the Submittal, Review, and Approval needed in order to obtain FFP
 - ***Procurement*** (Chapter **4.0**) provides guidance for conducting procurements in conjunction with the APD process



Endnotes

-
- ² "General Administration—Grant Programs (Public Assistance, Medical Assistance And State Children's Health Insurance Programs)", 45 CFR 95, U.S. Government, <http://www.ecfr.gov/cgi-bin/text-idx?SID=0603e63ad662df7eb119f60e170d029a&mc=true&node=pt45.1.95&rgn=div5>
- ³ "Federal reimbursement rate", 7 CFR 277.4(b), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=0603e63ad662df7eb119f60e170d029a&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_14#se7.4.277_14
- ⁴ "Administrative costs principles", 7 CFR 277.9(c)(1) through (2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_19#se7.4.277_19
- ⁵ "Advance planning documentation", 7 CFR 274.1(f), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.274&rgn=div5%23se7.4.274_11#se7.4.274_11
- ⁶ "EBT management and reporting", 7 CFR 246.12(y), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=596d3cf56e7ebc393daa90f09f54852c&mc=true&node=se7.4.246_112&rgn=div8
- ⁷ "Appendix II to Part 200—Contract Provisions for Non-Federal Entity Contracts Under Federal Awards," [https://www.ecfr.gov/current/title-2/part-200/appendix-Appendix II to Part 200](https://www.ecfr.gov/current/title-2/part-200/appendix-Appendix%20II%20to%20Part%20200)



2.0 Lifecycle Management

Key Points

The information in this section should allow you to understand the following:

- What is Systems Development Lifecycle Management?
- What is the Project Management Lifecycle?
- What is Acquisition Lifecycle Management?
- What is Data Lifecycle Management?
- How are the different Lifecycle Management (LCM) related?
- What is the relationship of each LCM to the APD process?

Chapter Contents

2.1	Lifecycle Management – An Overview	72
2.2	Systems Development Lifecycle Management.....	73
2.2.1	Overview of Systems Development Phases.....	73
2.2.2	The Development Phase.....	75
2.2.3	Management of the SDLC Phases	76
2.2.4	System Development Lifecycle Methodologies	77
2.3	Project Management Lifecycle.....	82
2.3.1	Project Initiation Phase.....	83
2.3.2	Project Planning Phase	84
2.3.3	Project Execution Phase	84
2.3.4	Project Monitoring and Controlling Phase.....	85
2.3.5	Project Closure Phase	86
2.4	Acquisition Lifecycle Management	87
2.4.1	Pre-Award Phase	88



2.4.2	Award Phase.....	89
2.4.3	Post-Award Phase.....	90
2.5	Data Lifecycle Management.....	91
2.5.1	Technical vs. Non-Technical Data	92
2.5.2	Data Lifecycle Management Phases	93
2.6	Alignment of Lifecycles	97
2.6.1	Lifecycle Management (LCM) Interactions	97
2.6.2	Aligning SDLC and PMLC	98
2.6.3	Aligning ALC to SDLC.....	99
2.6.4	Aligning SDLC, ALC, and PMLC to DLC.....	99
2.6.5	Aligning SDLC and the APD Process	99
2.7	Summary.....	101

Chapter Acronyms

ALCM	Acquisition Lifecycle Management
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representatives
DDI	Design, Development, and Implementation
DLCM	Data Lifecycle Management
PMLC	Project Management Lifecycle
RFI	Request For Information
RFP	Request for Proposal
SDLC	Systems Development Lifecycle



For definitions of terms used in this handbook please see appendix **A1 Acronyms and Glossary of Terms.**

2.1 Lifecycle Management – An Overview

It is common knowledge that humans, animals, and plants have a “lifecycle.” But, so do non-living things. Equipment, software, hardware, and even systems, projects, and programs all have a beginning, middle, and end of life. A “lifecycle.”

All lifecycles can be managed to produce desired outcomes. The purpose of lifecycle management is to control, direct, and make decisions about priorities over the entire lifecycle of the project in order to achieve desired results.

If, for example, a project is established for developing an information technology (IT) system, several elements have to be managed concurrently to achieve the desired outcome of a successfully implemented system. The system may be implemented by a contractor who must be procured and financed. The vendor must be acquired within funding constraints and within a reasonable amount of time. The system also must be implemented on schedule. This all involves careful planning. To be successful, all elements (planning, implementation, acquisition, financing, and scheduling) have to be managed throughout the life of the project and the life of the system. Each element is dependent on the other and must be synchronized. When one element takes priority, it provides direction for the other elements and the course of the project at that moment.

Often, each stakeholder has a specific lifecycle which is core to their role, and these will interact with one another. These must be well managed to work together in concert toward a successful result. Within projects that are typically covered under the APD process, there is an order of precedence and relationship between these lifecycles. The SDLC is focused on the process of delivering an IT solution. The PMLC, focuses on the activities necessary to complete the SDLC. The APD is focused on documenting the process and activities (i.e., the PMLC, and the SDLC). Merging and meshing of these lifecycles is the key to successful planning.



This chapter does not describe the APD Process or FNS requirements, but rather, describes the industry standards and practices around which the APD process is built. Chapter **3.0 The Advance Planning Document Process** provides guidance for how the APD process and the lifecycle management principles in this chapter interact.

2.2 Systems Development Lifecycle Management

2.2.1 Overview of Systems Development Phases

Systems Development Lifecycle (SDLC) is a term used to describe a phase-based process for planning, creating, testing, and deploying a system. It includes maintaining the system, operating the system, and eventually retiring the system (i.e., disposal). A system can be described as “an assemblage, or combination of things or parts, forming a unitary whole.” The SDLC serves as a programmatic guide to the activities necessary to put a system in place. It provides a flexible, but consistent way for conducting system development to a depth matching the scope of the needs the system is intended to support.

There are many SDLC models used by private sector and public sector. Some have as few as five phases while others have as many as ten. Within these phases, there are multiple activities. In some models these activities are promoted to their own phases. For the purposes of the HB901, we are using a five phase model, as shown in **Figure 12**.

These phases are:

1. Initiation
2. Development
3. Implementation
4. Maintenance and Operations
5. Disposal



Figure 12: SDLC Phases

Planning, Analysis, Design, Development, Testing, Implementation, and Maintenance & Operation are interdependent activities of the SDLC phases. They are accomplished in sequential order to produce a successful result. Each phase of the SDLC consists of a set of activities, which has multiple steps. Each uses the results of the previous one.

Over the course of a system’s lifecycle, there will be a multitude of projects to accomplish the various activities of each phase. Some projects will last years, as in the case of initially implementing a system. Others will be shorter, such as upgrading system capabilities. All of the SDLC phases must be properly managed to ensure a successful outcome.

2.2.1.1 The Initiation Phase

Initiation is all about getting started. This phase begins when a sponsor identifies a need or an opportunity that requires action. Analysis and planning are the focus of this phase, and involve several activities which are important to getting the project off on the right foot and setting it up for success.

These activities include:

- Craft a concept proposal including high level objectives
- Identify Stakeholders
- Conduct a Needs Assessment to determine the scope and urgency of the need
- Devise an initial schedule
- Determine probable resource needs
- Estimate total cost
- Establish cost allocations among stakeholders

Analysis activities continue during the initiation phase, which include defining the scope or boundary of the concept. These activities include:

- Feasibility Studies
- Alternatives Analysis
- Cost Benefit Analysis
- Risk Management Planning
- Budget Estimating
- Proposed Schedules



More information on planning and analysis activities
can be found in chapter **5.0 System Planning**.

The initiation phase concludes with design activities. Design activities provide a detailed description of features and operations within the system. During the course of the design, hardware requirements are outlined and specific software for the system is delineated. The majority of planning the system development occurs during the initiation phase. The design activities are important because they provide the blueprint for the Development Phase.

2.2.2 The Development Phase

The Development Phase uses the guidance from the Initiation Phase in order to create software and procure hardware necessary for the system to work. This is the point when the system design is converted into a functioning system.

Development Activities include:

- Installing the system's environment
- Creating and testing databases
- Preparing test cases and procedures
- Compiling and refining software programs
- Integrating the system as a whole and interfacing with external systems

Development also includes thorough system testing when a product is tested and errors are fixed. Troubleshooting frequently occurs during this phase before the product is released to customers. Testing is typically performed by developers, quality assurance staff, users, and program staff. User acceptance testing (UAT) is typically the last major activity in the development phase.



For more information on troubleshooting and testing,
please see chapter **6.0 Test Planning**.

2.2.2.1 Implementation Phase

Implementation describes the point when a system is finally ready to be distributed for business and customer use. All the quirks that manifested in the Development Phase testing activities have been fixed or mitigated. Implementation includes a pilot test to a limited user community before full deployment to all users. Once implemented, the system begins operation.

2.2.2.2 Maintenance & Operation Phase

The Maintenance & Operation Phase is defined by continual evaluations and updates of the operating system in order to ensure the system continues to perform according to end-user specifications. If the system has an issue during the course of the Maintenance Phase, the system is assessed for corrections. If necessary, system updates or enhancements are handled by means of the SDLC. In other words, updates to the system are made by the same means of planning, analysis, design, development, testing, and implementation that were used in initial development.

2.2.2.3 Disposal Phase

The system enters the Disposal Phase when it has outlived its usefulness. This is often the result of advances in technology that mean the system slowly loses its capability to perform according to end-user specifications without costly upgrades. When a system is retired, it is replaced by a new system which has its own SDLC. The older system, now referred to as the “legacy” system, is not turned off until the replacement system has successfully been implemented. There is a strong emphasis on data migration and conversion in the transition from the legacy system to the replacement system. Preservation of data is critical.

2.2.3 Management of the SDLC Phases

Systems take months, often years to build and rely on effective collaboration of individuals. However, these systems can often outlive the original team members who Initiated, Developed, and Implemented it. For this reason, effective System Development Lifecycles depend on effective management at all phases of the lifecycle. It is vital to the SDLC that management has timely, complete, and accurate information on the status of the projects and the system as a whole throughout its entire lifecycle.

To achieve this goal, management of the SDLC is divided into three areas of focus:

1. **Schedules and Timelines:** Permit management to understand where in the SDLC the system is. Documented correctly, the schedules and timelines illustrate system integration at a glance.
2. **Activities and Milestones:** Allow management to see if a system is progressing in a timely manner. This supports the addition of items placed on a watch list and the elevation of watch items to project risks.
3. **Key Decision Points and Gate Reviews:** Management provides a decision to move to the next phase of the SDLC. Decision points and gates exist for all phases of the system. The amount of time spent in each phase is controlled by management, in collaboration with the research and development team.

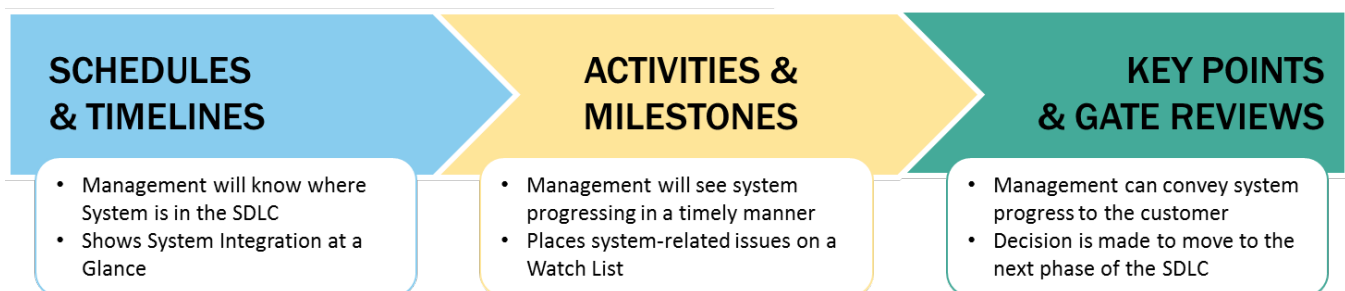


Figure 13: Management Areas of Focus of the SDLC

These three areas of focus serve as a yardstick to measure the proficiency of the system’s plan and its objectives. The SDLC ensures planning estimates can be put together before there have been any significant expenditures of

resources, time, and money on the project. If system development is on target, it needs to be verified. If there are exceptions, these must be detected as early as possible so that corrective actions can be taken in a timely manner.

The SDLC management areas of focus are on-going throughout the system’s lifecycle. For example, plans must be continually updated to reflect the current understanding of the system’s scope. Likewise, risk assessments must be revised at various points over the system’s lifecycle. The SDLC must identify all the points in the lifecycle where it is necessary to revisit each of these topics and define exactly what must be addressed at each point. For the SDLC to really work, each manager, team member, and stakeholder must have a solid understanding of how their individual work contributes to the overall project, system, and phase in the lifecycle. This way, the SDLC evolves along with the system throughout the years even if it outlives the original team members who created it.

2.2.4 System Development Lifecycle Methodologies

Any project can be better managed with a structured hierarchy of phases, stages, activities, tasks, and steps. That segmentation is the fundamental purpose of any SDLC methodology. There are many different methodologies employed for various system development projects including derivative methods developed to better handle complex environments. The methodology selected will impact all elements of the project, especially management. For instance, the initial level of detail found within various plans will be greatly affected by the chosen methodology.

The challenge in selecting and following a methodology is to do it wisely by taking all factors into account. Methodologies may be driven by the application development tools; by the software architecture within which the application will operate; or by the “build versus buy” decision. However, there are standard activities that all system development projects should follow, regardless of environment and tools, as illustrated in **Figure 14: Common SDLC Activities**.

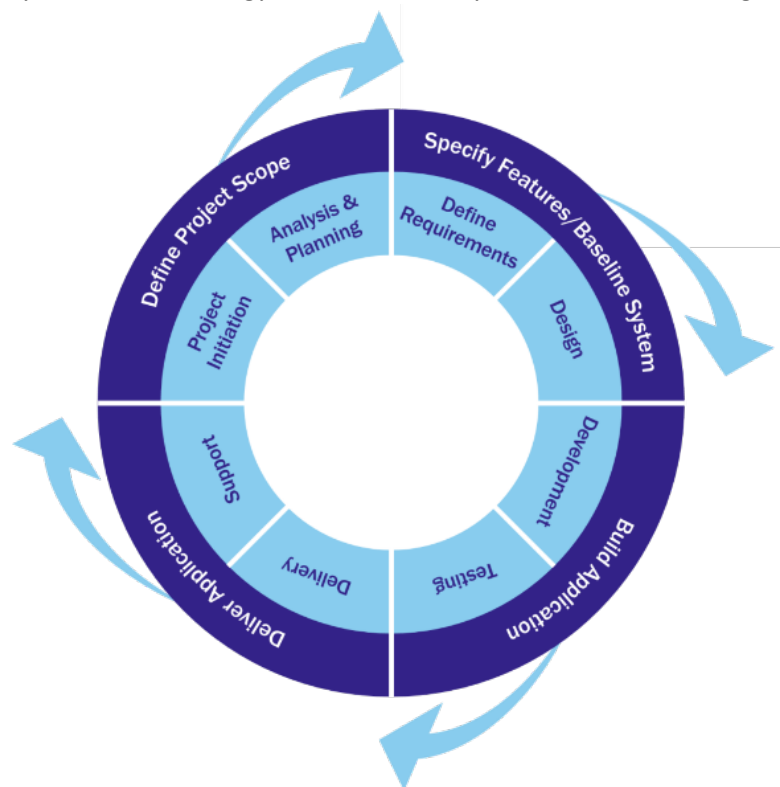


Figure 14: Common SDLC Activities



There are three broad categories that most SDLC methodologies fall into based on execution sequence:

- **Linear**
- **Iterative**
- **Incremental**

Linear methodologies progress stage by stage and are sequential. Progress occurs in order from project initiation to project completion. The initial project plans will be highly detailed, setting exact expectations for product functionality and implementation. Waterfall is the most common linear methodology.

Iterative methodologies progress through the stages of a project multiple times. Each iteration results in a new version of the final product. The initial project plans will set an overall direction, but details will be developed as the project progresses. Iterative methodologies allow the project to be successively refined over time and address a project's highest risk items as the highest priority task for each version. Given the time it takes to develop large, sophisticated software systems, it is not always possible to define the problem and build the solution in a single step. Requirements will often change throughout a project's development as a result of architectural constraints, customer needs, or a better understanding of the original problem. Agile methodology is a combination of this style of execution and the third style: Incremental.

Incremental methodologies break a project into components that are developed individually. The basic idea behind developing a software system incrementally is to allow the developer to take advantage of what was learned during the development of earlier increments. Learning comes from both the development and use of the system where possible. Key steps in the process start with simple implementations of a subset of the software requirements and enhance the evolving sequence of increments until the full system is implemented. Design modifications are made at the beginning of each increment, and new functional capabilities are added within the scope of the project. Similarly, project plans will initially contain a clear direction and the relevant details to successfully execute the first increment, however later increments may lead to alterations to the initial plans to include the further elaboration of the details.

The following sections describe the two more common methodologies in use with systems development: Waterfall and Agile.

DECISION FACTORS	WATERFALL	AGILE
	Suitable for very large projects	Best suited for projects with fewer stakeholders
	Not sensitive to staff changes	Sensitive to staff changes
	Must have well defined risk	Risk driven
	Rigid	Flexible
	High time and cost requirements	High speed development that suits short time constraints
	Very well defined requirements/scope	Loosely defined requirements/scope
	Limited user input/feedback during development	High degree of user input/feedback during development process
	Lower engagement from user needed because of high detailed plans	Higher engagement from user needed because of lack of details in plans
	Management focuses on project as a whole	Management occurs for the project as a whole but additional attention required for each increment/iteration
	Ease of maintenance	Complex maintenance
	Highly documented	Documentation less of a concern
	Focus on producing a product once in accordance with established plans	Focus on expanding or improving products by multiple iterations

Figure 15: Methodology Decision Factors

2.2.4.1 Waterfall

As previously mentioned, the simplest and most common type of linear SDLC methodology is called “Waterfall.” The waterfall methodology presumes that the system requirements have already been defined and refined exhaustively, which is probably the most important step toward project success.

The waterfall model illustrates a few critical principles of a good methodology:

- Work is done in stages
- Content reviews are conducted between stages
- Reviews represent quality gates and decision points for continuing

Waterfall provides an orderly sequence of development steps and helps ensure the adequacy of documentation and design reviews to promote the quality, reliability, and maintainability of the developed software. It is suited to projects where requirements and scope are fixed, the product itself is firm and stable, and the technology is clearly understood. A drawback of waterfall is that upon final product release it is potentially more difficult to make changes. This is because waterfall is structured to produce a product only once in accordance with the established plans. Any major changes identified after the final product release, which were not accounted for in the planning, may necessitate an entirely new project to produce the next version of the product to integrate the changes. Although many IT professionals believe the waterfall methodology is slow and cumbersome, it does illustrate sound principles of lifecycle development and is used widely throughout the public and private sector.

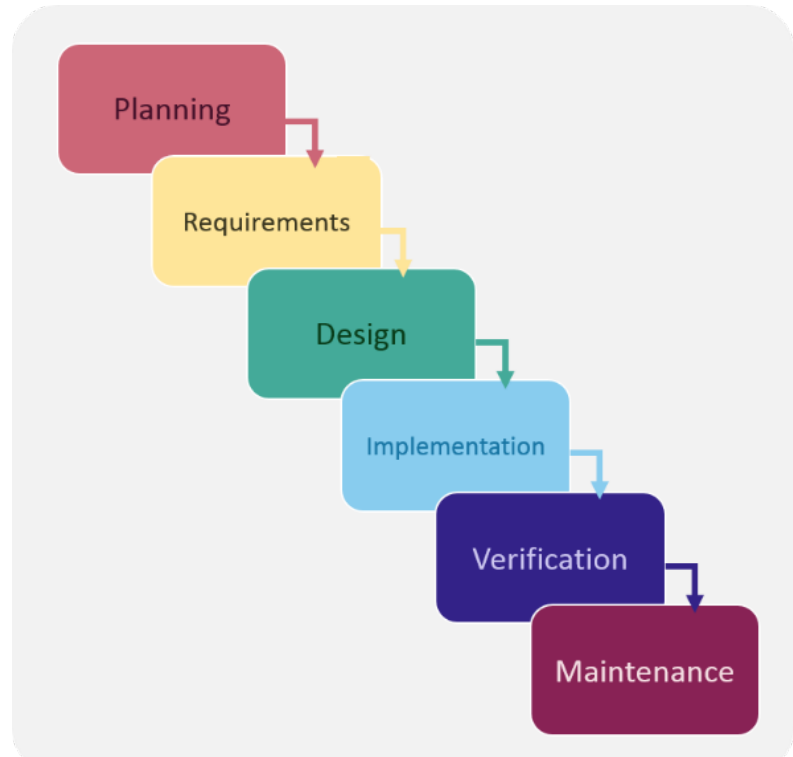


Figure 16: Waterfall SDLC

2.2.4.2 Agile

The Agile development methodology occurs incrementally and has short iterations. As mentioned before, this makes Agile a hybrid of two of the broader SDLC methodology types. In Agile, small teams work together with a stakeholder or Product Owner to define quick prototypes, proof of concepts, or other visual means to describe a problem to be solved. The high speed of development sometimes comes at the price of documentation. Initial documentation may be left intentionally vague to leave room for additional requirements later on. The fundamental approach to documentation may be altered to incorporate use cases, rather than more traditional forms of documentation. The goal of each increment is to produce a working component of the system. Within each increment the team defines the requirements for the iteration, develops the code, conducts testing, and then verifies the results through user acceptance testing. This could lead to many versions of a system or component, thereby complicating maintenance. A higher priority must be placed on configuration management

to mitigate this risk. The goal of each iteration is to produce a version of the working component that solves a particular problem or mitigates a particular risk.

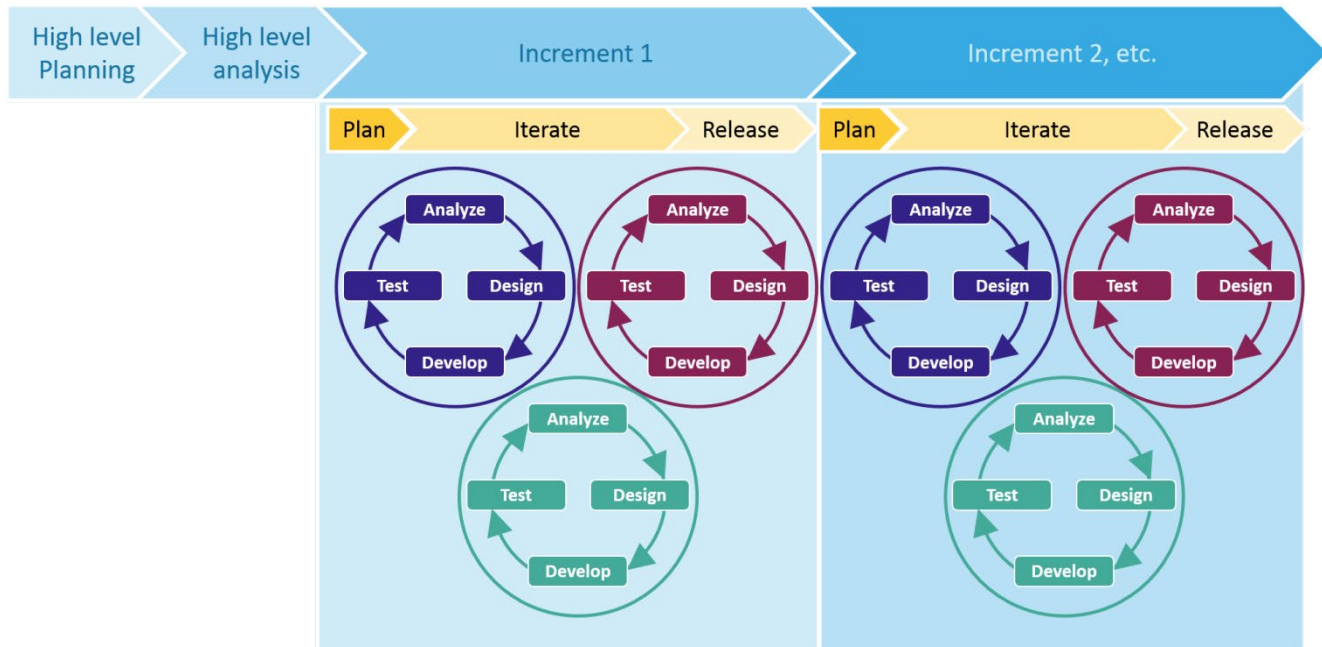


Figure 17: Agile SDLC

Agile promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change. Agile also focuses on lightweight processes which allow for rapid changes based on the incremental releases. Agile is adaptive in that changing requirements can be integrated into future iterations and may be time blocked. However, when used incorrectly, Agile can result in a series of iterations which simply replicate and correct earlier iterations. Excessively vague planning may distort Agile into a process of continuously correcting issues, such as poorly defined requirements, which is not the intent.



A potential drawback of Agile (and all iteration based SDLC methodologies) is that it requires high levels of stakeholder engagement to be successful. This is because of the high fluidity in requirements and the need to more frequently evaluate the results of each iteration.

2.3 Project Management Lifecycle

Projects are divided into phases to provide better management control. Collectively, these phases are known as the project management lifecycle (PMLC). The PMLC defines the phases that connect the beginning of a project to the end of the project. Each project is a unique endeavor, and each lifecycle phase is built upon that principle. Therefore, how you define the lifecycle depends on the requirements and conditions of that unique project. A “phase” within the PMLC is a specific portion of a project that is defined by a collection of related activities and a defined set of deliverables. The transition from one phase to the next generally involves the completion of the related activities, a milestone reached, or a technical delivery or handoff. Generally, phases are sequential. However, monitoring and control activities are not and could redirect the project back to an earlier phase if the requirements specified within that phase must be completed before moving on.

There is no specific limit on the number of phases a project can have, but, for the purpose of this handbook, we will focus on the five most common project phases and activities as defined by the Project Management Institute’s (PMI) Project Management Body of Knowledge (PMBOK):

1. Initiating
2. Planning
3. Executing
4. Monitoring and Controlling
5. Closing



Figure 18: PMLC Phases



For more detailed information on Project Management, refer to chapter **7.0 Project Management**.



2.3.1 Project Initiation Phase

The purpose of the Project Initiation phase is to begin defining the overall parameters of the project and establish the appropriate project management and quality environment required to complete the project. A project manager is assigned at the beginning of this phase. Successful projects begin with a detailed project definition that is understood and accepted by stakeholders. Some State agencies hold a meeting at the beginning of Project Initiation at which all potential stakeholders come together to review the project proposal, discuss required roles, and assign project team members.

A budget or further management commitment for the project may be required before a project manager is actually assigned and the project is authorized to progress. A time delay between the project's proposal and selection and its actual initiation may occur. The following processes occur during the initiating phase:

Prepare for the Project—Identify the project sponsor and the initial project team and work with the project manager to create the charter and conduct a kick-off meeting. The charter documents critical success factors and defines and secures commitment for the resources required to complete the Project Initiation phase. The charter also documents the project's mission, history, and background; describes the business problem the project is intended to resolve; and lists the benefits to be realized as a result of implementing the product or service.

Define Cost/Scope/Schedule/Quality—The project manager and project team define the scope of the project, the preliminary budget, a high-level schedule, and quality standards to complete the project. Defining scope may consist of a formal scope statement that includes the business need the project will address, what the project will accomplish, how it will be accomplished and by whom, what the end result of the project will be, a list of deliverables, and critical success factors. Establishing the preliminary budget requires the project manager to be aware of existing resource acquisition policies, guidelines, and procedures as well as any constraints on how resources may be acquired.

Perform Risk Identification—Identify and document any risks associated with the project, including cultural, technology, impact on work units, and various other internal and external areas.

Develop Initial Project Plan—The project manager and project team identify all stakeholders and document their involvement in the project, develop means of communicating with them, and compile all documentation created during Project Initiation to produce the initial project plan. Establishing status meeting and status report frequency and format up front is a key step to ensuring all stakeholders are involved and kept informed of the project activities.

Confirm Approval to Proceed to the Next Phase—The project manager reviews and refines the business case, secures resources required for the Project Planning phase, and prepares the formal acceptance package for review and approval by the project sponsor.



2.3.2 Project Planning Phase

The purpose of project planning is to define the exact parameters of the project and ensure that all prerequisites for project execution and control are in place. Planning builds on the work performed during the initiation phase. Project planning consists of the following activities:

Project Planning Kick-off—The project manager conducts a meeting to formally begin the Project Planning phase, orient new team members, and review the documentation and current status of the project. Useful information and topics include organization charts for the project team and information on roles and responsibilities, logistics, and project procedures.

Refine the Cost, Scope, Schedule, and Quality Standards of the Project—It is during this step that the team establishes performance baselines for the project. A baseline represents the approved plans for Cost, Scope, and Schedule. These baselines are useful for measuring deviations from the plan during and at the end of the project such as going over schedule or over cost. Before setting baselines it is important to break down each project deliverable into smaller components to clearly define them. This is known as the Work Breakdown Structure (WBS) and assists in assigning work to team members, developing budgets, and monitoring performance in manageable units. For Scope, clearly state what will be done to complete the work and what will not be done. For Schedule, have an estimated time to complete the components. And, for Cost, have an assigned dollar value to the cost of completing the work. Using a WBS greatly enhances the ability to monitor and control (i.e., PMLC Phase 4) these elements.

Perform Risk Assessment—The project team and project manager review the list of risks identified, identify new risks, evaluate each risk based on the likelihood of its occurrence and the magnitude of its impact, and develop a formal risk management plan to respond to each risk. Risks require continual review at each phase of the project.

Refine Project Plan—Develop all required management processes and plans for team development and project execution and implementation. Examples include the definition of a contract management plan (including acceptable performance criteria), change control process, acceptance management process, risk management and escalation process, organizational change management plan, stakeholder management plan, project implementation and transition plan, and establishing time and cost baseline.

Confirm Approval to Proceed to the Next Phase—The project manager reviews and refines the business case, secures resources required for Project Planning, and prepares the formal acceptance package for review and approval by the project sponsor.

2.3.3 Project Execution Phase

The purpose of this phase is to develop the system. It is the longest phase of the project management lifecycle and where most resources are applied. It uses all the plans, schedules, procedures, and templates that were



prepared and anticipated in previous phases. The conclusion of the phase arrives when the product is fully developed, tested, accepted, implemented, and transitioned to operational. Accurate records need to be kept throughout this phase because they serve as input to the final phase, Project Closeout. The following processes generally occur during this phase:

Conduct Project Execution and Control Kick-off—The project manager conducts a meeting to formally begin this phase, orient new team members, and review the documentation and current status of the project.

Manage Project Execution—The project manager must manage every aspect of the project plan to ensure that all work is being performed correctly and on time. This includes deliverable acceptance, test results and documentation, organizational change, the project team, project transition, as well as executing the communications plan and managing change control.

Deliverable Acceptance—The project manager may want to maintain an “acceptance log” in the project status report to track the status of deliverables as they go through iterations of the acceptance process. The project manager should be concise and clear in both written and verbal messages and solicit feedback to determine if messages have been received and interpreted correctly. In addition to conducting regular status meetings, the PM will use the status report to drive the meeting discussion points.

Gain Project Acceptance—The customer formally acknowledges that all deliverables have been completed, fully tested, accepted, and approved, and that the product or service has been successfully transitioned to an operational environment.

2.3.4 Project Monitoring and Controlling Phase

This is not a phase in the traditional, sequential sense. It is happening constantly, throughout the project, and controls all other phases. Think of it as the phase that fixes things that go awry in all other phases. Monitoring and control activities could redirect the project back to an earlier phase if the requirements specified within that phase must be revised before moving on. That is why in **Figure 18: PMLC Phases**, the phase is shown wrapping around the other phases. It is in effect most of the time.

Manage Cost, Scope, Schedule, and Quality Standards—The project manager handles changes to project scope and schedule, and controls and manages costs established in the budget. The PM also implements Quality Assurance (QA) and Quality Control (QC) processes according to the quality standards. QA defines the methodology to be followed to meet the customer requirements; whereas, QC ensures that the defined standards are followed at every step. Successful QC processes always strive to see quality through the eyes of the customer, and should be performed throughout the course of the project.

Manage and Control Risks—The project manager and team use the risk management plan, created in the Planning phase, and develop and apply new response and resolution strategies to any unexpected events.

Change Control—During Project Planning, the project manager refines the project scope to clearly define the content of the deliverables to be produced during Project Execution. This definition includes a clear description of what will and will not be included in each deliverable. The process used to document and control changes is documented in the project plan through the use of a Configuration Management Plan. Even if a change is perceived to be very small, exercising the change process using the Configuration Management Plan’s procedures ensures that all parties agree to the change and understand its potential impact. As part of managing change, one of the project manager’s functions is to ensure that the project produces all the work, but **ONLY** the work, required and documented in the project scope. Any deviation to what appears to be in the scope document is considered change and must be handled using the change control process.

The change control process defined in the Configuration Management Plan should describe the following:

- The definition of change and how to identify it
- How requests for change will be initiated
- How requests for changes will be analyzed to determine whether they are in or out of scope versus more appropriate for later enhancements
- The process to approve or reject changes
- How funding will be secured to implement approved changes.

If the project manager revises the baseline established in the planning phase as a result of change control, they should be sure to save the original baseline for historical purposes.

2.3.5 Project Closure Phase

The purpose of the Project Closeout phase is to assess the project and derive any lessons learned and best practices to be applied to future projects.



See chapter **3.0 The Advance Planning Document Process** for FNS formal close-out procedures and requirements.

This final phase consists of the following processes:

Conduct Post-Implementation Review—The project manager assesses the results of the project by soliciting feedback from team members, customers, and stakeholders. These results may be communicated in a post-implementation report. The project manager should not wait to get feedback from the project team, but should spend the time reviewing the project, and understanding what was done correctly and incorrectly. Sometimes the Post-Implementation Review reveals incomplete tasks or deliverables. This enables the project team to reassess and ensure completion before resources are dismissed or funding is closed out. The project manager

should concentrate on what is important in the feedback, prioritize the comments, and select those that may be of use to other projects. The results of the reviews should be documented as generically as possible.

Perform Administrative Closeout—The project manager formally closes the project by providing performance feedback to team members and archiving all project information.

2.4 Acquisition Lifecycle Management

The terms “procurement,” “contracting,” and “acquisition” are often used interchangeably. In general, “acquisition” is the process used to formalize business relationships between two parties. The “contract” is the written and legally binding document for the business relationship. The primary purpose of these business relationships is to “procure” goods and services needed to accomplish the procuring organization’s mission.

Most large IT projects involve contractor support of some type. This may be as minor as assistance with testing or as major as complete system development from concept through system disposal. It may involve a single contract or multiple contracts. Contracts may overlap or run concurrently. Contract periods of performance may be as short as 90 days or last for years. Managing each contract, as well as multiple contracts, should be planned as an integral part of any IT system project.

As depicted in **Figure 19**, Acquisition can be broken into three major phases:

- Pre-Award
- Award
- Post-Award

Within these phases, there are multiple activities:

- Pre-Award Phase
 - Acquisition Planning
 - RFP Development
 - Solicitation
- Award Phase
 - Source Selection
 - Award
- Post-Award Phase
 - Contract Management
 - Closeout

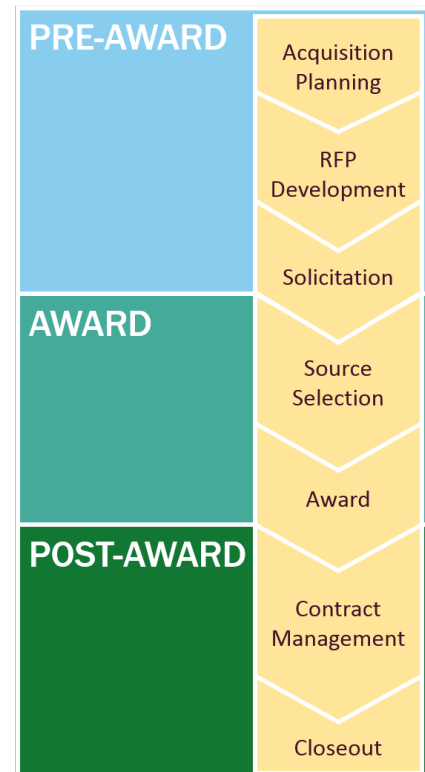


Figure 19: Acquisition Lifecycle Model



For full details on acquisitions and procurements, see chapter **4.0 Procurement**.

The acquisition lifecycle impacts determination of needs, research, development, production, deployment, support and finally disposal of solutions. It is a vital part of generating solutions, which is present from project conception until end of life. The acquisition lifecycle may be tailored to support specific situations, but there should always be an acquisition strategy which matures over time resulting in a comprehensive plan detailing how acquisitions will be managed to meet project objectives.

2.4.1 Pre-Award Phase

Acquisition, by necessity, requires collaboration among the contracting and other program/project managers, legal counsel, finance, budget, and other experts as required. The Pre-Award phase is all about laying the necessary groundwork for eventually soliciting offers and awarding a contract.

The Acquisition Planning tasks generally performed include:

- Identifying the requirement for products or services
- Preparing a performance work statement
- Researching the market for the supplies/services
- Committing sufficient funds to acquire the deliverable
- Determining the extent of competition for award (e.g., full and open and small business set-aside)
- Establishing technical, price-related, past performance, and other evaluation criteria for competitive acquisitions
- Drafting the solicitation
- Publicizing the solicitation
- Answering inquiries from potential offerors and conducting pre-bid or pre-proposal conferences
- Determining the method of acquisition (e.g., invitation for bid or negotiation) and type of contract.

During the course of the Pre-Award phase, several SDLC activities contribute to acquisition planning. Business and technical needs are detailed and translated into requirements. Often, an alternatives analysis is conducted to assess possible solutions. A feasibility analysis is used to help guide the SDLC efforts during design, development, and implementation (DDI), which are often the primary focus of an IT contract. Finally, a cost benefits analysis provides information for acquisition planning based on the affordability of a feasible alternative. For example, is a system transfer more practical and affordable than using resources to build a custom solution in-house? If the answer is to procure a solution through an acquisition, the acquisition Pre-Award phase activities proceed.

The Pre-Award phase is a time to seek as many alternatives as possible. The goal is to competitively acquire the appropriate external resources needed for solution development. This may mean releasing a request for information (RFI), or using other market research techniques, or both. Following the research results, the generation of a draft request for proposal (RFP), or a similar procurement document, occurs. The RFP is then released, with an appropriate response period stipulated to enable vendors to properly respond.



The RFP response period must provide sufficient time to allow vendors to put together a competitive response. Short response deadlines may lead some vendors to opt out, or to assume that another vendor has been pre-selected.

In order to solicit the most bids, publicizing the acquisition is vital. More bidders mean more competition and ideally more options for the customer. A bidders' conference or similar method may be used to answer vendors' questions during the response period. Vendor proposals are submitted for evaluation and source selection in the award phase.

2.4.2 Award Phase

The award phase begins when vendors have submitted their proposals. Once the response period has ended, all submissions from vendors are evaluated based on established criteria and the contract is awarded.

Tasks during this phase include:

- Evaluating bids or proposals based on the evaluation plan for the acquisition and the criteria in the solicitation
- Setting the competitive range and discussing proposals with offerors, as necessary
- Determining the responsibility of the potential awardee based on procurement requirements
- Responding to Pre-Award protests by offerors
- Awarding the contract
- Responding to protests of the award by unsuccessful offerors

Acquisition activities in this phase are focused on executing the plans established in the previous phase. The primary objective of acquisition activities in this phase is to procure the products or services, or both, identified in the RFP. A draft contract is generated based on the released RFP and the awarded vendor's response. This period includes negotiations and revisions with the vendor to produce the most accurate contract. Depending on

federal thresholds, the proposed contract may need to be submitted for federal approval. The contract is then signed and work may begin.

2.4.3 Post-Award Phase

In the post-award phase, focus of acquisition activities shifts to managing the vendor's execution of the contract:

- Conducting orientation of personnel who will be responsible for contract administration (e.g., Contracting Officer's Technical Representatives (COTR) or Contracting Officer's Representative (COR))
- Conducting contractor orientation
- Monitoring compliance by both contractor and customer personnel with the terms and conditions of the contract, including performance standards
- Inspecting and accepting contract deliverables
- Addressing contract performance issues, including determining whether to stop work, extending delivery dates for excusable delays, or applying formal contractual remedies (e.g., rejecting contract deliverables, termination)
- Determining the timing and amount of payments to contractors based on the contract terms
- Modifying contracts as necessary
- Resolving contractor claims



Figure 20: Contract Management Overview

Contract management should ensure that cost, schedule, and performance are meeting established performance standards and metrics. As with corresponding SDLC activities, Acquisition Lifecycle Management (ALCM) activities should ensure that there is acceptable interoperability and operational supportability. Additionally, there should be assurances that the acquisition is affordable throughout the lifecycle and optimally funded.

Eventually, all of the deliverables, services, and work specified in the contract are completed and accepted by the customer. The contract will be closed administratively and all accounting and funding activities finalized. Any assets or property acquired in support of the contract must be properly disposed in accordance with applicable laws and procedures.

2.5 Data Lifecycle Management

“Data” is one of those terms that can mean different things to different people, depending on how they interact with it. Generally defined, data is “facts or information usually used to calculate, analyze, or plan something” and also “information that is stored by a computer.” With regard to the lifecycle of a system, there can be various types of data to consider. There is data OUTSIDE the system: Data ABOUT the system and data SUPPORTING the system. Then there is the data stored INSIDE the system itself.

Depending on the requirements of the system and the procedures of those handling it, data can be stored in multiple places at once; in the cloud, in on-site and offsite hardware, on devices such as laptops, tablets and smartphones, as well as hard copies. Private, proprietary, or sensitive information falling into the wrong hands can be devastating. Like any asset, data needs to be accounted for until no longer needed. When data, despite its type, is appreciated as the valuable asset that it is, the idea of properly managing it achieves its real importance.

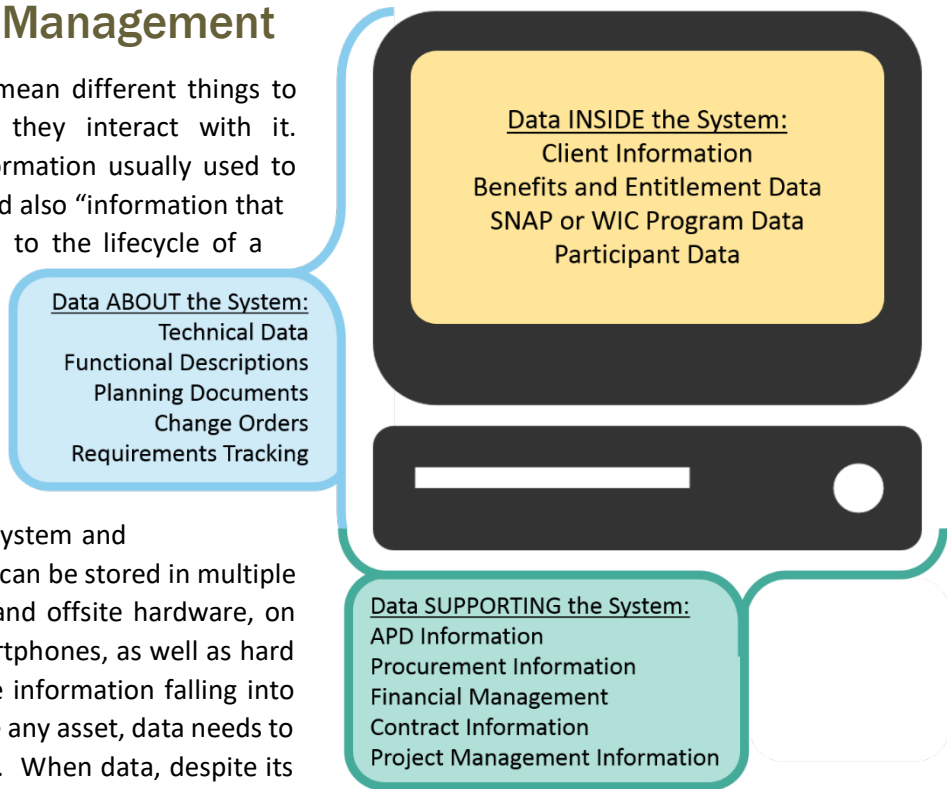


Figure 21: Types of System Data



For more information on securing valuable Data, see chapter **9.0 Systems Security**.

That is where Data Lifecycle Management (DLCM) comes in. Implementing Data Lifecycle Management provides more than just a place to store the important information. It provides proper organization, security and disposal of data by creating processes that control where data lives, how it is documented, who has access to it, how it is accessed, at what point it becomes out of date, how long it sticks around after obsolescence, and how and when it is destroyed, if ever.



Data lifecycle management is particularly important when implementing a new IS to replace a legacy system. Data conversion is significantly influenced by the principles of DLCM.

2.5.1 Technical vs. Non-Technical Data

Data INSIDE the system is of more interest to program managers, but Data OUTSIDE the system is more pertinent to project managers. Think of data OUTSIDE the system as the “User’s Manual” for the system. It describes what the system can do, what had to happen to make the system work, and importantly, how to sustain it over time. Sometimes the line between data ABOUT the system and SUPPORTING data can be blurred. You can also think of Data OUTSIDE the system in terms of technical data and non-technical data.

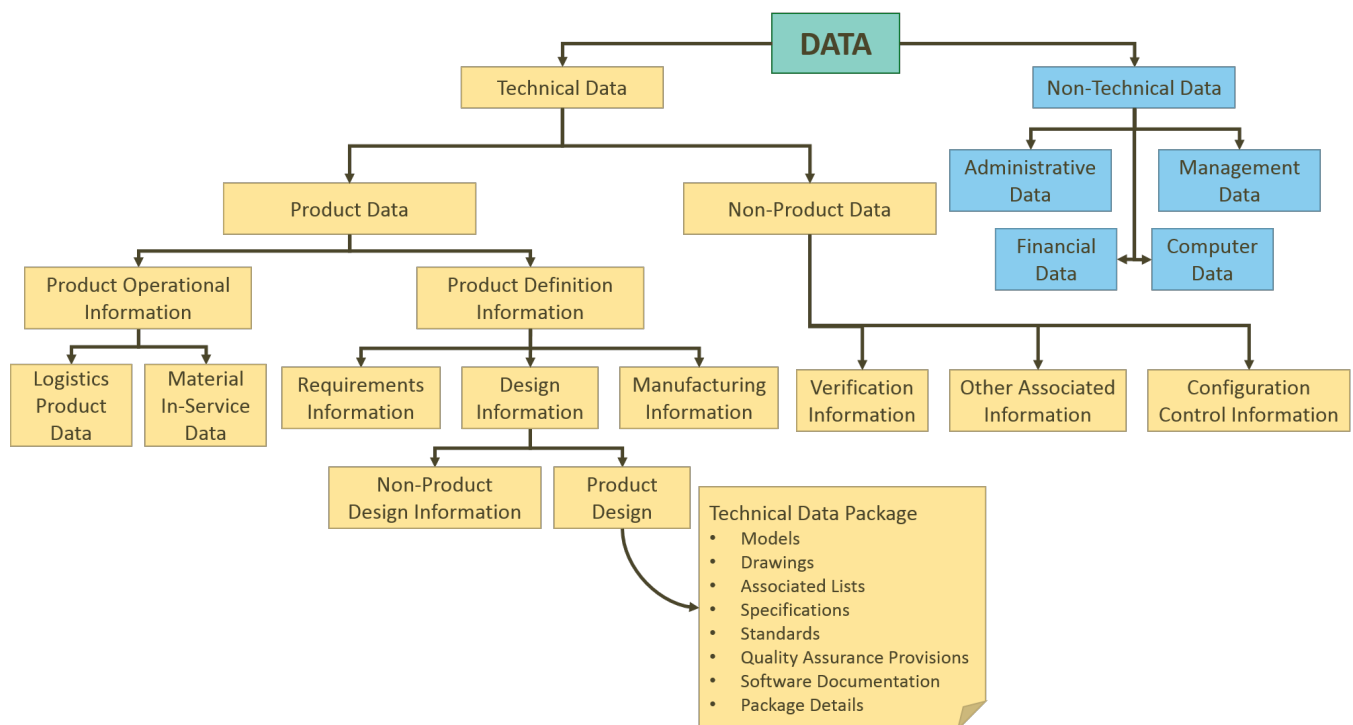


Figure 22: Technical vs. Non-Technical Data



For more information on Data INSIDE the system, see chapter **5.0 System Planning** for a discussion on Data Migration and Data Conversion.

Non-technical data is the support data. As shown in **Figure 22** this details the financial, management, and administrative tasks and results that made system production feasible.

Technical data is important because it focuses on the “nitty-gritty” details of the system (i.e., “the Product”) that makes it work and keeps it working. Product care and system sustainability make up the majority of the total ownership cost of the system over its entire lifecycle, so an efficient maintenance roadmap is key. Lack of technical data significantly impedes an organization’s ability to properly plan and execute effective and efficient sustainment strategies. This can lead to the system owner’s inability to reduce total ownership costs throughout the system’s lifecycle.

2.5.2 Data Lifecycle Management Phases

Each organization may have their own unique DLCM plan in place and each will have policies and procedures that govern how they collect, use and disseminate their data throughout the project. These DLCM procedures run separately and concurrently as data are shared between them. A Data Lifecycle will vary according to the requirements of the project or program implementing it.

However, DCLM generally consist of the following phases:

- Acquire or Create
- Store
- Use
- Share
- Archive
- Destroy



Figure 23: Data Management Lifecycle

2.5.2.1 Acquire Phase

There are myriad ways data can be created or acquired. Most data will be generated during the activities occurring over the life of a system, and is also subject to federal requirements. Some data will come in the form of the various documents internal to the organization, or from external sources that are closely associated with the



internal workings of the organization. In addition to official documentation, any of the “paper” trail, whether electronic or hard copy, generated over the course of the project is data. As an example, consider the possible sources of data and examples of data which are commonly produced over the life of a system, as shown in **Table 6**.

Table 6: Examples of Data for DMLC

Data Origin	Data Examples
Needs Assessment	• Case Studies • Survey results • Research
System Technical Documents	• Technical Specifications • Functional Requirements • Test Plans • Security Plans
Acquisition and Procurement	• Request for Proposals • Contracts • Contract Amendments • Quality Assurance Surveillance Plan • Contractor Performance Reports
Project Management	• Schedules • Communications • Project Management Plan • Change Control • Quality Control
Financial Management	• Budgets • Expenditure Reports • Cost Benefit Analysis
Security Management	• Security Plans • Contingency Plans • Cybersecurity
Program Information	• Client Information • Policies and Guidance • Entitlements and Benefits Information • Regulations

2.5.2.2 Store Phase

It is up to the organization implementing the process to decide which of the data produced counts as a record that needs to be stored. Storing data and records is basically keeping the data in a central location where it can be accessed by approved users. Decisions on how long the data is stored, how it is stored, who has access to it, how they access it, and what they are allowed to do with it once they access it, all need to be determined and documented as part of a DMLC plan.



It is also important to consider the many ways data can exist. Email correspondence and text or voicemails can sometimes be data that needs to be stored. Project or customer files and financial records can exist both on paper and digitally, and need to be stored accordingly.

Electronic data is stored in many forms:

- Hard drives on laptops, desktops, and servers
- USB jump or flash drives
- Zip disks
- Magnetic tapes
- Audio/visual media such as CDs/DVDs

2.5.2.3 Use, Share, and Archive Phases

Data usage is the application of information to tasks that the organization needs to perform functions. For instance, much of the data generated during the development and implementation of an information system has a very specific purpose. However, other forms of data, while not requirements, may still have a useful life as research or reference for future projects.

The ability to prepare and share data with stakeholders, staff, and other entities is an important part of its lifecycle. Sharing can occur digitally or via hard copy. Either way, the data should be shared with the proper controls in place to protect any proprietary data and to assure that the data is only being distributed to appropriate parties.

When data becomes obsolete or simply is not needed, the data can be archived. This means the data is stored, but no maintenance or usage occurs. It may be needed again in the future, or it may not. The same decisions regarding access and length of storage are similar to those of the Store phase, and need to be determined and documented as well.

2.5.2.4 Destroy

At a certain point some data may reach the end of its life. When that occurs, every copy of a data item must be permanently removed. It is important to dispose of the data, thoroughly and completely, especially with regard to sensitive materials. Deleting files does not automatically and permanently erase data.

Electronic data must be disposed of in the following ways:

- **Destruction** is used when the storage device is no longer required at all and can be completely destroyed. Examples include shredding, pulverizing, and incinerating

- **Purging** can be accomplished via degaussing or secure erasing on a hard drive. Degaussing magnetically erases electronic information from tape devices and hard drives, but it isn't effective in clearing data from DVDs and CDs
- **Clearing** electronic data is commonly achieved by overwriting existing data using software that incorporates a fixed sequence or patterns of letters, numbers, or symbols

The general rule of thumb is to use two forms of destruction to ensure stored data is no longer accessible. For example, devices with no removable storage should be reset and purged per manufacturer instructions before being destroyed. Magnetic media, such as tapes and floppy disks, need to be degaussed before being shredded or incinerated. Optical media or solid state disks should be pulverized and then incinerated or shredded.



See “Guidelines for Media Sanitization” ([NIST Special Publication 800-88](#)) for additional information regarding media disposal and handling.

2.6 Alignment of Lifecycles

All lifecycle management frameworks (SDLC, PMLC, ALCM, and DLCM) share a common organization. Aligning them has many benefits, but synchronizing the actual performance of work within the lifecycle frameworks can be complicated. Despite the potential complexity, aligning lifecycles is important. Not only do project activities impact one another from across the lifecycles, but aligning lifecycle activities keep costs down by mitigating the risk of duplicating work and ensuring requirements don't get missed.

All lifecycles consist of four broad types of phases. Aligning lifecycles can be accomplished by matching phases of a similar type.

These types of phases include:

1. **Plan** – Establish the objectives and processes necessary to deliver results in accordance with the expected output.
2. **Do** – Implement the **plan**, execute the process, and make the product. Collect data for charting and analysis in the following steps.
3. **Check** – Study the actual results (measured and collected in **Do**) and compare against the expected results from the **Plan** to identify differences.
4. **Act** – If there is a difference from the **Plan** and the **Do** activities detected by the **Check** phase, then the difference needs to be addressed by proceeding through the cycle again to resolve the deviation and establish a new baseline for performance.

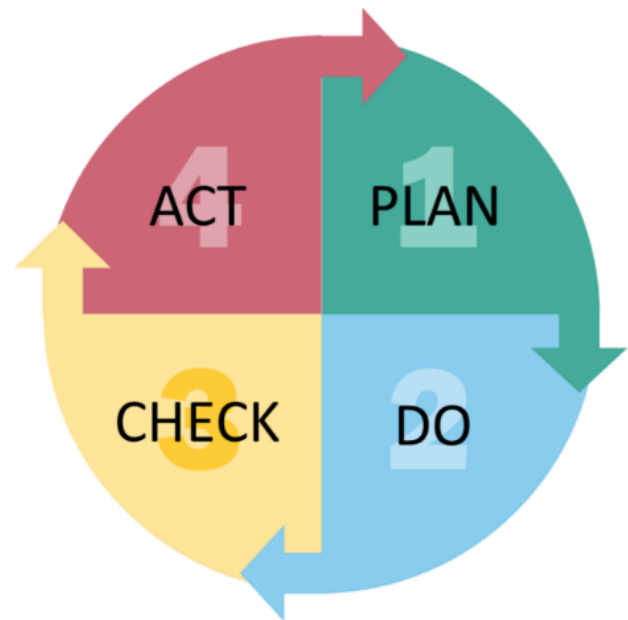


Figure 24: Common Lifecycle Phase Types

2.6.1 Lifecycle Management (LCM) Interactions

Figure 25: PMLC, ALC, SDLC, and DMLC Alignment, below, is a visual representation of how the different phases of each lifecycle, PMLC, ALC, SDLC, DLCM align. The following sections will describe how the lifecycles interact and work together to produce a successful result.

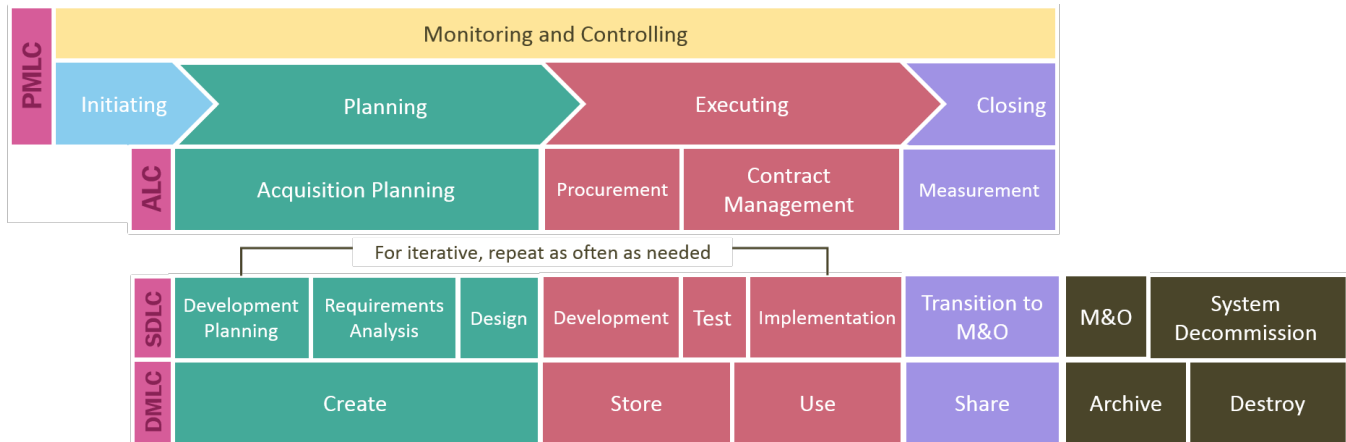


Figure 25: PMLC, ALC, SDLC, and DMLC Alignment

2.6.2 Aligning SDLC and PMLC

The system development process is composed of many complex tasks which must be accomplished in the correct order to produce a successful result. This is why the SDLC is needed. Also, precision and completeness of tasks relies on the structure an SDLC provides. It provides division of responsibilities and collaboration between stakeholders, developers, management, and users. Most projects involving system development include contractor support and specialists in various fields (e.g., software engineers, business analysts, quality control, testing engineers, etc.). The SDLC provides a process for forming clearly defined tasks, defined deliverables, and defined collaborative relationships among the various team members. This is achieved through the SDLC in phases. Where the SDLC focuses on the system being developed as a process, PMLC focuses on the orderly performance of the many activities within the SDLC.

PMLC organizes the SDLC activities into work packages using the WBS. The SDLC processes of Planning, Analysis, Design, Development, Testing, Implementation, and Maintenance & Operation can all be easily organized to align to the project phases of Planning, Execution, and Closure. As previously mentioned, Monitoring and Controlling is not a distinct phase, but an activity that provides “management” oversight of the project phases and activities.

The phases of the SDLC generally align with the phases of the project management lifecycle; however, the SDLC phases do not correspond on a one-to-one basis with the project management phases. The degree of alignment varies by the methodology used. The SDLC and PMLC work in conjunction with each other. The PMLC defines how to manage a project and parallels the SDLC. The PMLC describes the tasks that must be completed to produce a product or service. Different project lifecycles exist for specific products and services. However, most processes and deliverables are required for all projects, although in smaller projects they may require less formality and a lower level of effort.



2.6.3 Aligning ALC to SDLC

The organization of the acquisition lifecycle is similar to that of the system development lifecycle and the project management lifecycle. ALC organizes procurement into a planning and preparation stage (Pre-Award) followed by execution and closure (Award and Post-Award). In an IT procurement, the acquisition activities are tightly coupled to the SDLC. All of the contractual requirements are derived from the SDLC's planning activities. The contract performance requirements and deliverables are the manifestation of the SDLC's implementation activities. These include the transition to the SDLC's maintenance and operations activities. Once all contract deliverables are accepted, the contract is closed, which is directly related to project closure. SDLC benefits the ALC by allowing the customer to more effectively manage contracts. The SDLC provides a basis for planning and receiving long lead time items during system development. Purchases can be segmented and spread across the SDLC activities in a timely fashion that allows the customer to better manage and mitigate risks. The SDLC provides a means to schedule acquisitions and budget for them across the life of the system. The SDLC benefits individual contracts by establishing a specific schedule of deliverables and identifying the exact scope of work for performance work statements. The SDLC also establishes milestones to effectively manage contractor performance.

2.6.4 Aligning SDLC, ALC, and PMLC to DLC

All of the SDLC, ALC and PMLC activities rely on data and documentation. Managing the data and documents over the duration of these lifecycles should be done with attention and discipline equal to the other activities within each lifecycle model. Data lifecycle management provides a framework that shares a phase orientation with the other lifecycles. All these steps work together to achieve the goal of accountability and all produce myriad documents, records and other information, all of it vital data. That data must be properly maintained to prove adherence to procedure and provide accountability, as well as maintain privacy and security when necessary.

Project managers should ensure data management is incorporated into all of their project activities. This means ensuring the maximum availability of all essential information to support continued competitive acquisitions to support the system over its lifecycle. Simply having the data available is not sufficient if the most current information cannot be efficiently retrieved. The process of data management begins at the very beginning of the PMLC Initiating phase and lasts until after the SDLC disposal phase.

2.6.5 Aligning SDLC and the APD Process

In any project involving the APD process, the basic SDLC processes must be performed—what differs is the timing of their execution. While no two development efforts are alike (and different methodologies may refer to these processes by different names), all projects should progress through the same processes or disciplines:

- **System Initiation**—The business case and proposed solution are re-examined to ensure they are still appropriately defined and address an organizational need. A high-level schedule is developed for subsequent SDLC phases.
- **Systems Requirements Analysis**—The needs of the business are captured in as much detail as possible.
- **System Design**—Builds on the work performed during systems requirements analysis and results in a translation of the functional requirements into a complete technical solution. The completion of system design marks the point in the project at which the program manager should be able to plan, in detail, all future project phases.
- **System Construction**—The project team builds and tests the various modules of the application, including any utilities that will be needed during system acceptance and system implementation. Documentation and training materials are developed during this phase.
- **System Acceptance**—Focuses on system testing and validation by those who will ultimately use the system to execute their daily processes. In addition to confirming the system meets functional expectations; activities also validate all aspects of data conversion and system deployment.
- **System Implementation**—The final phase, which includes training, installation of the system in a production mode, and transition of application ownership from the project team to the State agency.



Project means a related set of information technology related tasks, undertaken by a State, to improve the efficiency, economy and effectiveness of administration and/or operation of its human services programs. A project may also be a less comprehensive activity such as enhancements to an existing system, or an upgrade of computer hardware. – 7 CFR 277.18(b)

Ultimately, the purpose of the Advance Planning Document is to provide accountability to stakeholders and to ensure proper stewardship of federal funds. Inherent to the APD process are review and approval cycles, as well as required documentation and processes for procurement, project management, security, and testing.

The APD process parallels the SDLC. There are different models and methodologies, but each generally consists of basic steps or stages during which defined IT work products are created or modified. The last phase occurs when the system is disposed of and the task performed is either eliminated or transferred to other systems.

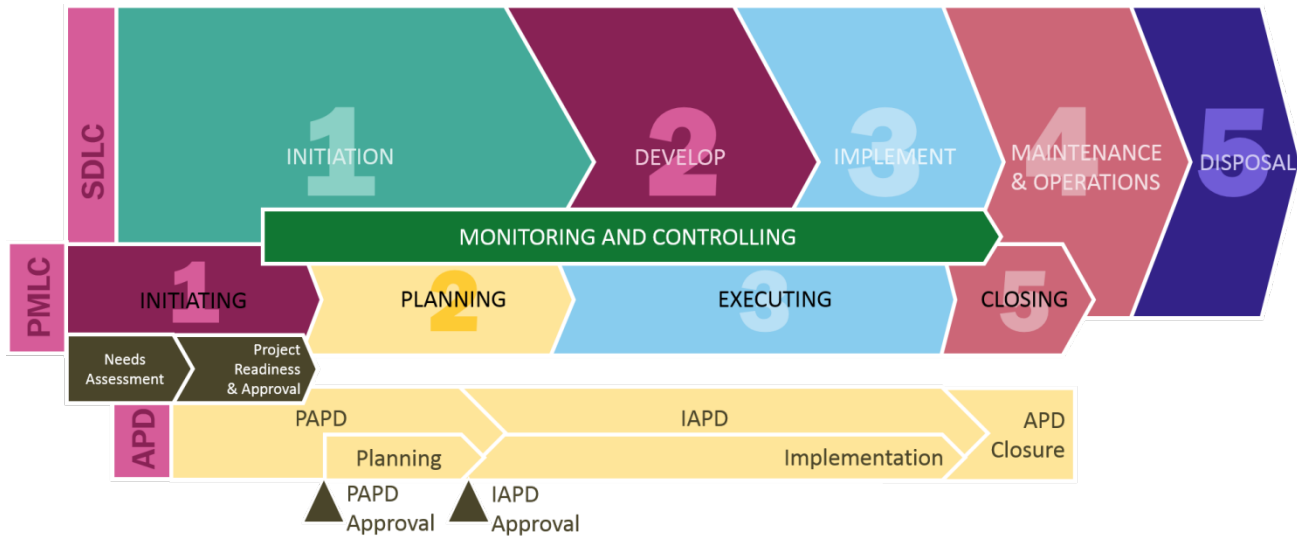


Figure 26: SDLC, PMLC, and APD Integration

2.7 Lifecycle Management Summary

This chapter has provided a brief overview of all of the lifecycle activities related to an IS project and how they interact with one another.

- Systems Development Lifecycle (SDLC) is a phase-based process for;
 - Planning, creating, testing, and deploying a system
 - Maintaining the system, operating the system, and retiring the system (i.e., disposal)
- Project Management Lifecycle (PMLC) is phased to provide management control for;
 - Initiating, Planning, Executing, Monitoring, Controlling and Closing
- Acquisition Lifecycle Management (ALCM) impacts determination of needs, research, development, production, deployment, support and disposal of solutions. It can be broken into three major phases:
 - Pre-Award Phase – Acquisition Planning, RFP development and Solicitation
 - Award Phase – Source Selection and Award
 - Post-Award Phase – Contract Management and Closeout
- Data Lifecycle Management (DLCM) creates processes for proper organization, security and disposal of data that control data storage, access, retention, and destruction
- All lifecycle management frameworks (SDLC, PMLC, ALCM, and DLCM) share a common organization
 - Aligning them has many benefits such as cost control by mitigating the risk of duplicating work and ensuring requirements don't get missed



The following chapters will explain the APD process and how it demonstrates the State agency's path through the various lifecycles. At a high level, State agencies must prepare for their own internal State clearance and compile the products resulting from the typical SDLC phases into the following key documents:

- A Planning APD (PAPD) to address initiation, system concept development, planning, and requirements analysis
- An Implementation APD (IAPD) to address design, development, integration and testing, implementation
- APD closure and transition to maintenance and operations



3.0 The Advance Planning Document Process

Key Points

The information in this section should allow you to understand the following:

- What is the process for submitting APDs for FNS review?
- What happens to APDs after they are submitted?
- What are the different types of APDs and their purpose?
- What are the required elements of each type of APD?

Chapter Contents

3.1	Overview of the Advance Planning Document.....	106
3.2	The APD Process	107
3.2.1	Introduction.....	107
3.2.2	Preparation & Submission	111
3.2.3	Review	113
3.2.4	Disposition.....	118
3.2.5	Performing APD Activities.....	120
3.2.6	Relationship Between Procurements and the APD Process	120
3.2.7	APD Closure	122
3.2.8	Post-Implementation Reviews.....	123
3.2.9	Regional Office Fiscal Closure	124
3.3	APD Information Specific to Program or Project Type.....	124
3.3.1	Planning APD	125
3.3.2	Implementation APD	130
3.3.3	APD Update	136
3.3.4	APDU As-Needed	139



3.3.5	Emergency Acquisition Request	143
3.4	Post-Implementation APDs	146
3.5	APD Components	147
3.5.1	Actual Expenditures to Date	147
3.5.2	Annual APD Update Revised Documents.....	147
3.5.3	Alternatives Analysis.....	148
3.5.4	Capacity Plan or Study	149
3.5.5	Changes to the Approved APD	149
3.5.6	Contractor Performance	149
3.5.7	Conversion or Transition Plan.....	149
3.5.8	Cost Allocation Plan	149
3.5.9	Cost Benefit Analysis	150
3.5.10	Detailed Design Document	150
3.5.11	Disaster Recovery Plan	150
3.5.12	EBT Disaster Recovery Plan	151
3.5.13	Executive Summary – General Guidelines	151
3.5.14	Feasibility Study.....	153
3.5.15	Functional Requirements Document	153
3.5.16	General System Design	154
3.5.17	Project Management Plan	154
3.5.18	Project Status	154
3.5.19	Proposed Budget	154
3.5.20	Request for Waiver of Depreciation	155
3.5.21	Resource Requirements	155
3.5.22	Schedule of Activities, Milestones, and Deliverables.....	156
3.5.23	Security Plan	156



3.5.24	Test Plan	157
3.5.25	Training Plan.....	157
3.5.26	Transmittal Letter	158
3.6	APD Process Summary	158

Chapter Acronyms

APD	Advance Planning Document
APDU	Advance Planning Document Update
CBA	Cost Benefit Analysis
EAR	Emergency Acquisition Request
EBT	Electronic Benefits Transfer
FFP	Federal financial participation
IAPD	Implementation Advance Planning Document
IAPDU	Implementation APDU
MOU	Memorandum of Understanding
PAPD	Planning Advance Planning Document
PAPDU	Planning APDU
RFP	Request for Proposal
SDLC	Systems Development Life Cycle
SOW	Statement of Work



For definitions of terms used in this handbook please see appendix **A1 Acronyms and Glossary of Terms**.

3.1 Overview of the Advance Planning Document

State agencies may receive federal funding to develop, acquire, and/or implement Information Systems (IS) that support the operation of FNS programs. State agencies are required to submit an Advance Planning Document (APD) to FNS in order to obtain prior approval to receive or utilize federal funding for IS supporting these programs.

In general, the Advance Planning Document (APD) describes in broad terms the State agency's plan for managing the design, development, implementation, and operation of an information system (IS) supporting SNAP, WIC programs, and related EBT systems. The system must meet Federal, State, and user needs in an efficient, comprehensive, and cost-effective manner. The APD records information for the planning and implementation of the IS that is reviewed by FNS through the APD process.

APDs are designed to:

- Establish system and program performance goals in terms of projected costs and benefits
- Provide the budget basis for securing Federal financial participation (FFP) for the State agency SNAP or a grant for the WIC State Agency

The APD is comprised of several documents resulting from activities related to the Systems Development Lifecycle (SDLC). The APD process is not the same as the SDLC, but is closely associated with it. Where the SDLC focuses on system planning, development, and implementation, the APD focuses on documenting these SDLC activities. In addition to gaining FNS approval for FFP or other associated funding for IS projects, the APD is also used as a means for FNS review and oversight of IS projects. The APD enables FNS to fulfill its stewardship responsibilities for FFP. Where chapter **1.0 Getting Started with the Advance Planning Document (APD) Process** provides a general overview of the APD process, this chapter focuses on the specific elements of the different APDs and the process for submitting and obtaining approval for APDs.



HOW TO USE THIS CHAPTER

Chapter **1.0 *Getting Started with the Advance Planning Document (APD) Process*** and chapter **3.0 *The Advance Planning Document Process*** must be used together. Determining the need to submit an APD is described in Chapter 1. Chapter 3 describes the common process details for all APD types and the specific details for each APD type. This chapter also explains the details of the process for preparation, submission, review, decisions related to each APD, and APD closure.

1. Read the APD common process (section **3.2 *The APD Process*** and all sub-sections) to understand the general process requirements for APDs.
2. Read the specific information for the APD you are preparing in the appropriate sub-section of section **3.3 *APD Information Specific to Program or Project Type***
3. Each type of APD has specific required documentation components. Refer to section **3.5 *APD Components*** for descriptions of the documentation an APD requires.

3.2 The APD Process

3.2.1 Introduction

In general, the APD process is the same for each FNS program (i.e., SNAP and WIC). Likewise, most of the APDs follow a common process, differing in the specific APD contents and how these are reviewed based on the contents. The APD explains the State agency's intended activities and projected expenditures implementing IS in advance of carrying them out and incurring costs. The differences between APDs are based on specific requirements and nuances for each FNS program that alter the APD contents and process slightly. This section explains the *common processes* for preparation, submission, review, and disposition for each type of APD. Specific details for each APD will be explained in section **3.3 *APD Information Specific to Program or Project Type***.

In general, the APD describes in broad terms the State agency's plan for managing the design, development, implementation, and operation of an IS supporting SNAP, WIC, and related EBT systems. It is a period of communication and cooperative oversight between the State agency and FNS lasting the duration of the project. Submission is determined by relevant thresholds for APD documents and procurement documents. State agencies may not execute contracts or obligate funds without this approval.



See chapter **1.0 Getting Started with the Advance Planning Document (APD) Process** for the applicable thresholds for determining submission requirements for each type of APD.

The APD process focuses on areas of SNAP and WIC program functionality that may benefit from IT solutions. Together, the Planning APD (PAPD) and Implementation APD (IAPD) communicate the State agency's plans for using program resources, improving federal reporting and accountability, and achieving local agency efficiencies using IS to support SNAP, WIC, and related EBT systems. Planning and implementation using FFP is constrained by allowable costs, budget, and staffing levels. In addition to these, planning takes into consideration maintenance and security issues, compatibility with other existing or anticipated State projects, procurement rules, contractual terms, and transitioning costs from development to operations. FNS reserves the right to be included in planning and project meetings as appropriate. This chapter explains in more detail the purpose, document requirements, preparation, and submission for each type of APD.

3.2.1.1 The General APD Process

The APD process is a series of successive steps through which a State agency can meet federal oversight requirements. The APD process has eight basic steps that are the same for PAPDs and IAPDs.

These include:

1. Prepare the APD (State agency)
2. Submit the APD to FNS (State agency)
3. Review the APD (FNS)
4. Notify State agency of decision (i.e., approve or disapprove) (FNS)
5. Conduct procurements when applicable (State agency)
6. Perform activities described in APD (e.g., planning or implementation) (State agency)
7. Provide annual APD updates as appropriate (State agency)
8. Close the APD when the activities described in the APD are complete (FNS and State agency)

Figure 27 provides an overview of the APD processes. Typically, the activities conducted after a PAPD is approved will lead to the creation of an IAPD as shown in **Figure 27**. An APD approval means FFP is approved for conducting the activities described in the APD. PAPD funding is used for planning only. IAPD funding is used for implementation only. When planning and implementation activities exceed one year, the State agency must provide FNS with an annual APD Update (APDU). The APDU is one of the requirements for continued funding.

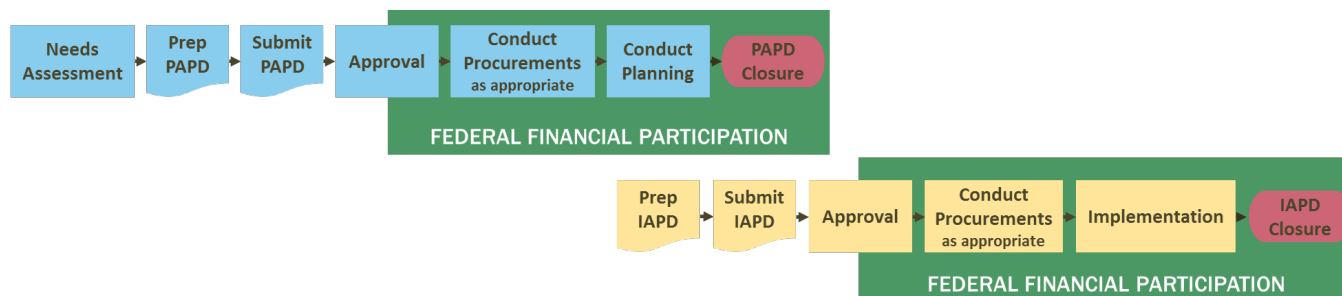


Figure 27: Overview of PAPD and IAPD Processes

When the activities described in the approved APD are completed, the APD is closed using a final APDU. At this point the system enters the M&O phase of the SDLC. See section **3.4 Post-Implementation APDs** for more information of APD activities during the M&O phase.



State agencies must be able to properly follow the APD process, regardless of the size of the project or procurement (e.g., enhancement, upgrade, interim, or full-scale projects), and submit the appropriate documentation based on funding thresholds.



See chapter **1.0 Getting Started with the Advance Planning Document (APD) Process** for “Thresholds” (section **1.5.1**).

State agencies are urged to communicate with FNS early and often when undertaking an IS project to verify information required and avoid disallowances. Retroactive approvals are granted only in the most extreme circumstances. Poor planning or communication is not considered valid reasons for retroactive approval of expenditures.



See chapter **4.0 Procurement** for the applicable thresholds for determining submission requirements for RFPs and contracts (section **4.3.1**).

3.2.1.2 Relationship of APD Process to SDLC

The APD process parallels the SDLC for developing IS through multiple phases of investigation of initial requirements through analysis, design, implementation, operations, maintenance, and disposal. The APD process is designed to be flexible and adaptable to different system design methodologies (e.g., waterfall, incremental, or iterative) and operational management strategies.



See chapter **2.0 Lifecycle Management** for details on the relationships between the SDLC, the APD process, and development methodologies.

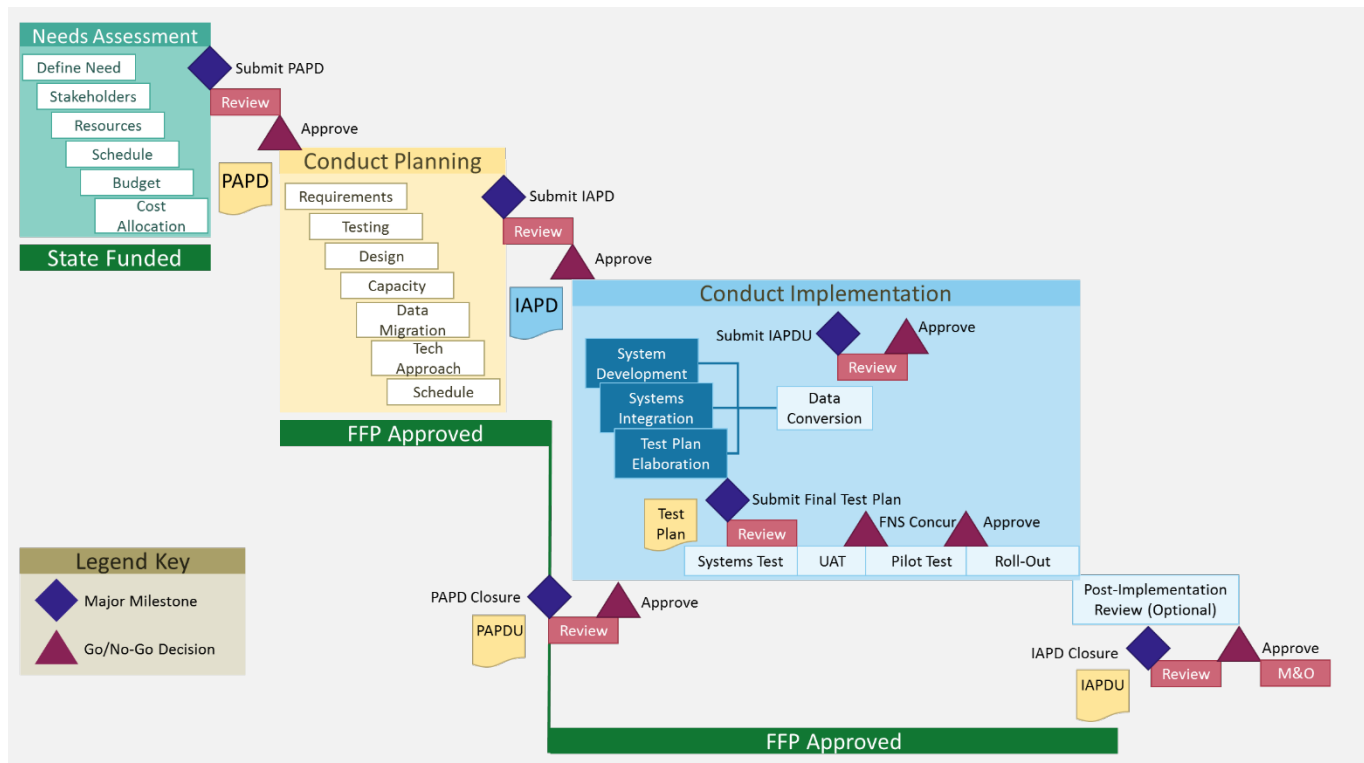


Figure 28: Major SDLC Activities Related to the APD Process

Figure 28 illustrates the major SDLC activities corresponding to the PAPD and IAPD over the course of a typical IS project.^{††} More information on the SDLC activities is included in this chapter's sections describing each type of APD.

^{††} The APD process in Figure 28 assumes all APD activities are approved.



FFP payments may be disallowed if FNS finds that any approved system project fails to comply with the criteria, requirements, or other specifications described in the approved APD or APD Update.

3.2.2 Preparation & Submission

3.2.2.1 Preparation

The documentation required for each APD varies by type of APD and program. To receive approval and subsequent funding, all documentation must be present and include sufficient content to allow FNS to make an informed decision on the APD request. Complete information and good communication among partners expedites review. Because the contents of each type of APD varies, documentation requirements and preparation of each is described later in this chapter in the appropriate section for that type of APD.

- Planning APD
 - Preparation – see sections **3.3.1.3 PAPD Documentation Requirements** and **3.3.1.4 Preparing the PAPD**
 - Submission – see section **3.3.1.5 Submitting the PAPD**
- Implementation APD
 - Preparation – see sections **3.3.2.3 IAPD Documentation Requirements** and **3.3.2.6 Preparing the IAPD**
 - Submission – see section **3.3.2.7 Submitting the IAPD**
- APD Update
 - Preparation – see sections **3.3.3.3 APDU Documentation Requirements** and **3.3.3.4 Preparing the APDU**
 - Submission – see section **3.3.3.5 Submitting the APDU**
- APDU As-Needed
 - Preparation – see sections **3.3.4.3 APDU As-Needed Documentation Requirements** and **3.3.4.4 Preparing the APDU As-Needed**
 - Submission – see section **3.3.4.5 Submitting the APDU As-Needed**
- Emergency Acquisition Request (EAR)
 - Preparation – see sections **3.3.5.3 EAR Required Documentation** and **3.3.5.4 Preparing the EAR**
 - Submission – see section **3.3.5.5 Submitting the EAR**



Before preparing the APD, the State agency should also consult with the internal State IT oversight department to determine whether any additional documents or procedures are required as part of the State's internal monitoring process or if the APD requirements will suffice.

The State agency must prepare for its own internal State clearance and State-level regulatory compliance for IS projects in addition to complying with federal regulatory requirements. (See appendix **A2 Regulations** for a listing of applicable general federal policies and guidance, as well as those for each program.) The Planning APD and the Implementation APD are the two key documents that must be submitted based on dollar threshold submission requirements. (See **1.5 Determining the Need for an APD**.)



State agencies need not format documents exactly as described in this handbook to receive FNS approval. As long as all the required information is provided, FNS will consider a State's APD in any standard, professional format. FNS review may be facilitated by the State agency providing a cross-walk or document map to the FNS required APD content.

3.2.2.2 Submission

The State agency prepares and submits all APDs to FNS electronically, including a scanned copy of a transmittal letter signed by an official authorized to commit State resources.



The electronic submission should be sent to the appropriate FNS Regional Office, with a copy to the appropriate State Systems Office analyst, if known. See the FNS website for the State Systems Office and RO contact list (<http://www.fns.usda.gov/apd/contacts-and-stakeholders>).

When a project involves multiple federal partners, one combined APD is developed. The State agency is required to submit the APD separately to each agency that is providing FFP. The State Agency should ensure that all FNS required content is included in the combined APD.



The FNS HB901 provides guidance for USDA APD processes ONLY. It does not provide guidance for APD requirements for other Federal agencies, such as DHHS, who may also be providing Federal financial participation.

In the event a project originally estimated to cost less than the \$6 million threshold for SNAP or \$1,000,000 for WIC encounters changes in prices or scope that increase the costs to exceed these thresholds, the State agency must submit an APD to FNS for approval of the entire project, not just the portion over the threshold. In such a circumstance, the State agency should work with FNS to ensure that all information requirements of the APD are met prior to submitting the APD for approval. This will assist FNS in reviewing and making an approval determination and obviate or shorten any project slowdown during the approval process.



For SNAP EBT, FNS approves the RFP and negotiated contract prior to the State incurring any costs. Under the new contract, the State must submit the IAPD to FNS for review and approval, one copy each to the RO and SSO. Failure to complete this step will jeopardize FNS FFP.

3.2.3 Review

3.2.3.1 APD Reviews in General

In general, when FNS reviews APDs, it seeks to ascertain the program benefits and overall process improvements to be obtained through the proposed IS. FNS review typically addresses the following questions:

1. Who is/are the requesting State agency(ies)?
2. What is the purpose of the project?
3. Which Federal/State programs are involved/affected?
4. How will the project be conducted (contractor support, in-house, combination)?
5. Will the project involve any lease/purchase of software/hardware, etc.)?
6. Which State and federal funding agencies are involved?
7. What is the projected cost of the project, and is the cost reasonable and necessary?
8. What are the benefits of the project to the affected program(s)?

9. Will the project benefits support the costs (Cost Benefit Analysis (CBA))?
10. What is the project schedule?
11. Does the budget reflect all allowable costs (staff time, training, equipment, travel, testing, etc.)?

Figure 29 summarizes the overall FNS review process. The process assumes the State agency will start with planning activities that require a PAPD, even though there are some circumstances when this is not the case. The “Needs Assessment” is a precursor to the PAPD, but is not part of the APD process and is not part of FNS’ review process. The process assumes the PAPD will lead to successful planning activities that will generate continuation of the process into the implementation phase that requires an IAPD. The “Activity” block represents either planning or implementation, depending on where the State agency is in the process. The “Document” block represents each type of APD (e.g., PAPD, IAPD, APDU, APDU As- Needed, or EAR), again depending on where the State agency is in the process. The “Review” block represents FNS actions to review the documents within applicable timelines (see section 3.2.3, including all sub-sections). The “Approval” block is an assumption to illustrate the most likely sequence of events for an IS project. The “Closure” block is the end of the process and is applicable to each type of APD (PAPD and IAPD) when appropriate. The PAPD is closed sometime near the beginning of the implementation, commonly after the IAPD is approved. The IAPD is closed when implementation is completed and FNS has approved system roll-out.

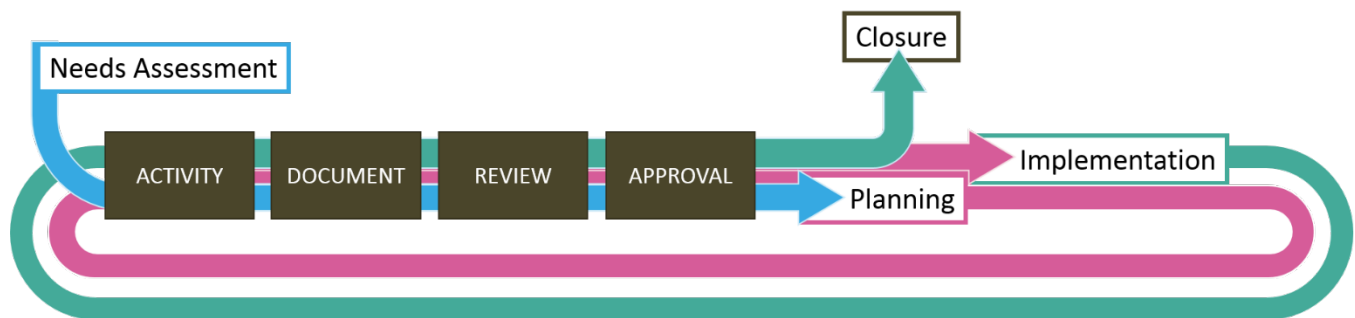


Figure 29: General FNS Review Process

3.2.3.2 APD Evaluation in General

When reviewing the APD (PAPD or IAPD), FNS follows several steps before deciding to approve or disapprove the State’s request for federal funding of its proposed costs. FNS:

- Examines the transmittal letter to ensure that it is signed by an appropriate project sponsor with the authority to commit state resources
- Notifies the State agency of receipt of the document(s)
- Conducts a preliminary review of the document for completeness

- Evaluates whether the document adequately addresses IT technical and security issues, cost and benefit issues, Federal/State procurement regulations, and program needs assessment by meeting the following review criteria:
 - Describes planning activities that justify the costs involved or that are otherwise consistent with the objectives of FNS programs
 - Identifies key stakeholders in the planning process and explains how relationships with other programs or organizations will be considered
 - Demonstrates availability of funds, resources, and skills to conduct the proposal in a satisfactory manner
 - Reflects an itemized planning budget by federal fiscal year and quarter and identifies the sources and amounts of federal and non-federal funding and the basis for the allocation of costs among the sources
 - Includes proposed cost allocation, if applicable
 - Describes the scope of the appropriate planning activities that meet the identified project objectives and needs
- Notifies the State agency if more information is needed or changes are required
- Notifies the State agency if documentation is missing or incomplete
- Coordinates comments and requests for information between financial, and program entities at different organizational levels at FNS, as needed
- Notifies the State agency in writing of FNS' final action (approval, disapproval, or conditional approval)
- Meets with the State agency on all negotiable matters
- Provides technical assistance to the State agency, as appropriate and necessary
- Notifies the State agency of APD closure (PAPD or IAPD) after it has successfully completed all APD activities



In reviewing the IAPD, FNS will focus on successful project management (see chapter **7.0 Project Management**) to ensure the IAPD provides a project plan the State agency can follow for a successful implementation. Identification and management of risks are key elements FNS looks for in the project plan.

State agencies are encouraged to work closely with FNS to facilitate document review and funding approval in a timely fashion. States may also request that FNS performs reviews in parallel with their internal State reviews, when possible. Comments and changes should be shared to expedite a project's approval. FNS strives to complete its reviews as soon as possible. Good communication between parties can serve to facilitate the review process.

3.2.3.3 FNS APD Review Timeframes

Document review timeframes are defined for all APDs and associated documents submitted to FNS. With the exception of the EAR⁸, FNS has 60 days to review a document. It is important that both submitters and reviewers understand how the review “clock” works.

i

The review period for Emergency Acquisition Requests is 14 days, not 60 days.

Once FNS receives an APD or associated document, the review “clock” starts ticking. FNS has 60 days to review and approve, disapprove, or request additional information. The clock stops when FNS communicates to the State agency the approval, disapproval, or a request for additional information. If FNS requests additional information, the clock starts another 60-day review cycle when FNS receives the State response.

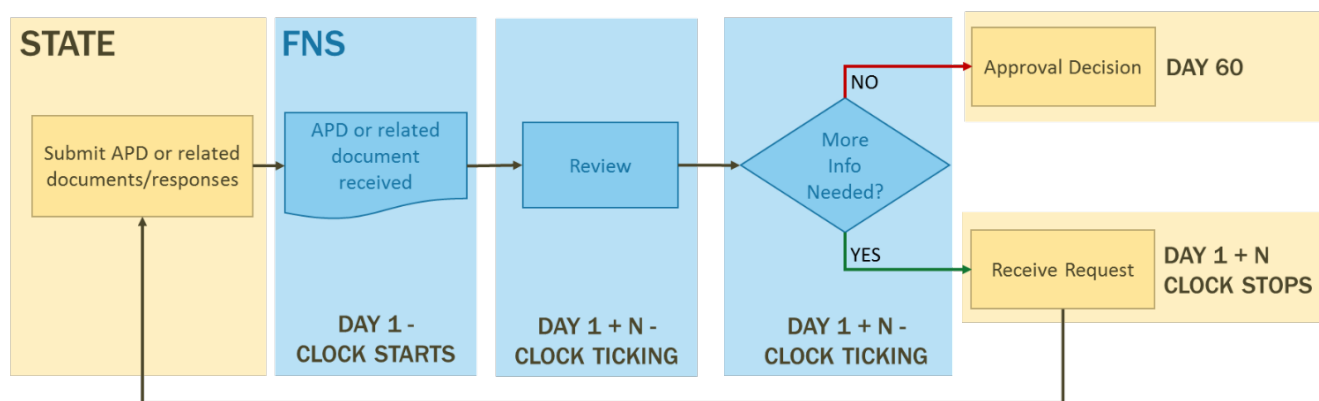


Figure 30: APD Review Clock

FNS strives to review all documents in less than the allotted 60 days. State agencies are asked to consult with FNS as frequently as needed to address FNS questions and comments in a timely manner. FNS views the APD process as a Federal/State partnership and strives to implement a team effort in fulfilling the requirements of the process.

Figure 30 illustrates how the APD Review Clock is applied by FNS.

Table 7 is a sample timetable that presents a timeline using the full 60 days provided for document review and approval for both APDs and procurement documents. State agencies that provide complete required information can minimize the review period because key documents would be approvable with few or no revisions.



Table 7: APD Federal Review Sample Timetable

Process Step	Expected Completion Date		Approval/Recommended Time Period
	Month	Year	(when applicable)
Planning Phase (24 months)			
SA submits Planning APD to FNS	January	year 1	
PAPD approved by FNS	March	year 1	60 days
SA submits Planning RFP to FNS	March	year 1	
Planning RFP approved by FNS	May	year 1	60 days
SA releases Planning RFP	June	year 1	90 days
Proposals evaluated/selection made	September	year 1	30 days
SA submits contract to FNS	October	year 1	
Contract approved by FNS	December	year 1	60 days
PAPDU submitted	January	year 2	
Contract signed	February	year 2	
PAPDU approved by FNS	March	year 2	60 days
Planning phase begins (contractor-on-board)	March	year 2	
Planning phase completed (one year for planning activities)	February	year 3	
PAPD Closure (submit final PAPDU)	February	year 3	60 days
PAPD Closed (final PAPDU approved by FNS)	April	year 3	As needed
Implementation Phase (12 months to contractor-on-board)			
SA submits IAPD to FNS	October	year 2	
IAPD approved by FNS	December	year 2	60 days
SA submits Implementation RFP to FNS	December	year 2	
RFP approved by FNS	February	year 3	60 days
SA releases Implementation RFP	March	year 3	
Proposals due from bidders	May	year 3	at least 90 days



Table 7: APD Federal Review Sample Timetable

Process Step	Expected Completion Date		Approval/Recommended Time Period (when applicable)
	Month	Year	
Proposals evaluated/selection made	August	year 3	
SA submits contract to FNS	November	year 3	
Contract approved by FNS	February	year 4	60 days
Contract signed	May	year 4	
SA begins implementation activities	November	year 4	
SA submits IAPDU to FNS	October	year n	
IAPDU approved by FNS	December	year n	60 days
IAPD Closure (submit final IAPDU)	Month	year n	
IAPD Closed (final IAPDU approved by FNS)	Month	year n	As needed
Total Estimated Time Before Beginning Implementation Activities: 34 months (Does not account for simultaneous or iterative activities)			

3.2.4 Disposition

After FNS reviews APD documents, including additional information that may have been requested, a decision will be made and provided to the State agency in writing. There are two possible decision outcomes: approved and disapproved.

3.2.4.1 Approval Decision

Approvals for APD documents and funding requests are issued by FNS Regional Offices (RO). The State Systems Office (SSO) works closely with the ROs and coordinates the APD process for FNS. Centralized coordination promotes the consistent application of policy and procedures across regions and provides an opportunity for enhanced customer service.

If approval is granted for an APD, FNS will notify the State agency and include one of the following conditions of approval:

- **General** - Related to availability of federal funds and compliance with FNS regulations

- **Specific** - Funding might be approved for a specific time period or incrementally based on satisfying specific conditions, such as submitting additional documents requested by FNS

Some examples of specific conditions that FNS could require include the following:

- Due to high risk or funding conditions for a project, monthly progress reports are required
- Specific contractor deliverables must be shared with FNS



Any planning or implementation costs incurred prior to APD approval will remain the responsibility of the State agency. No retroactive approval will be granted.



Approval of planning activities does not guarantee approval of FFP for implementation activities.

3.2.4.2 Disapproval Decision

FNS may disapprove a project plan if it determines that one of the following conditions occurs:

- Cost, scope, or methodology proposed are not feasible
- Analysis conducted by the State agency was insufficient and did not result in a valid outcome
- Procurement proposed or conducted was not allowable
- Plan will result in a system that is not sustainable within the State agency's budget constraints

FNS rarely disapproves a project plan completely. Whenever possible, FNS will work with a State agency to identify and remedy possible concerns throughout the planning phase or help the State adjust the plan to reach approval.

3.2.4.3 Provisional Approval in SNAP

Provisional approval is in effect if a SNAP State agency does not receive approval, disapproval, or a request for additional information within 60 days of receipt of the FNS acknowledgment. This would not, however, exempt a State from meeting all other federal requirements that pertain to the acquisition of IS equipment and services.



Such requirements remain subject to federal audit and review. FNS will make every effort to respond to State agencies within the targeted review periods.



Provisional approval does not apply to WIC.

3.2.5 Performing APD Activities

Assuming the APD (i.e., PAPD or IAPD as appropriate) is approved, the State agency proceeds with the SDLC activities. If contractor services are required, the State agency prepares and submits the Request for Proposal (RFP). FNS reviews the RFP and notifies the State agency if more information is needed. FNS approves or denies the RFP and informs the State agency of the decision. **Figure 31** depicts the general RFP and contract review process.

3.2.6 Relationship Between Procurements and the APD Process

Many planning and implementation projects involve procuring contractor services, equipment, software, or all of these. The costs of these procurements are part of the total project costs used for determining whether an APD is required. If procurement is needed, the RFP and contracts resulting from the RFP must be submitted for review and approval prior to the issuance of the RFP or the execution of the contract. States may submit RFPs simultaneously with APDs. States may submit the draft contract prior to the release date of the RFP. Changes (i.e., amendments) to existing contracts may also need FNS review and approval. Like the APD, this is based on the potential dollar value of the contract or amendment. While related to APD thresholds, the need for FNS RFP and contract review determination is separate from APD thresholds. Also, the thresholds are different for competitive and non-competitive procurements.

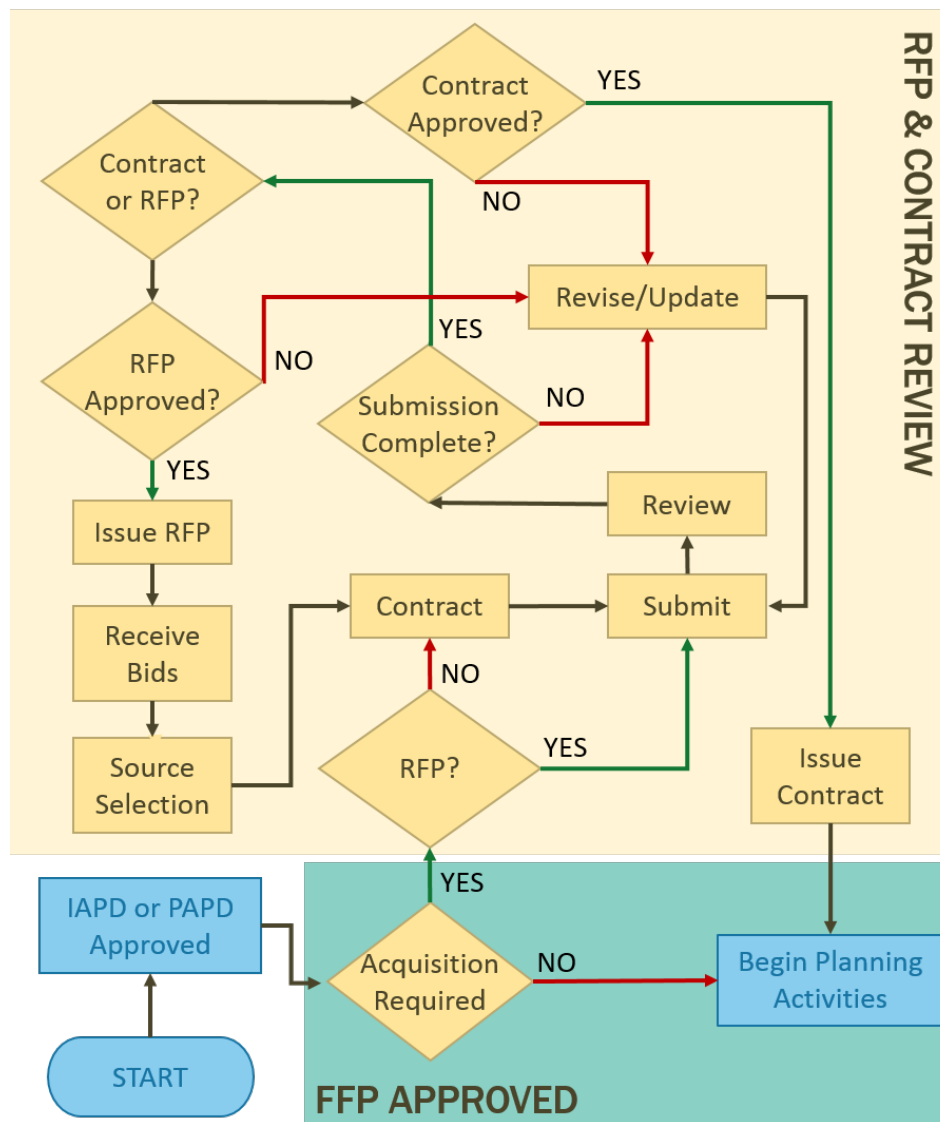


Figure 31: RFP and Contract Process Review

Once the procurement activities are completed and a contract is ready to be executed, the State agency follows the same process as for the RFP. The State agency prepares and submits the contract. FNS reviews the contract and notifies the State agency if more information is needed. FNS approves or denies the contract and informs the State agency of the decision. Once contractors are on board, the appropriate activities begin. Annual APDUs are submitted accordingly until the activities in the APD are completed.



Because the activities described in each type of APD are different, performance of the specific activities is described in the APD type descriptions later in this chapter.

- Planning APD – see section **3.3.1.6**
- Implementation APD – see section **3.3.2.8**
- APD Update – see section **3.3.3.6**
- APDU As-Needed – see section **3.3.4.6**
- Emergency Acquisition Request (EAR) – see section **3.3.5.6**

3.2.7 APD Closure

When all APD activities have been completed, the State agency provides a final APDU (i.e., Planning APDU or Implementation APDU) to advise FNS that all APD activities have been completed. Closing a PAPD or an IAPD entails confirming that the project objectives have been met and determining the actual costs incurred. The recommended timeframe for submitting the final IAPDU is after a post-implementation review is conducted or at the end of the system warranty period. The final APDU includes the final budget showing actual costs. Official closure of the APD must occur to document the end of the approved activities, the actual costs incurred, and to begin the process to close-out FNS funding activities. FNS notifies the State agency of APD closure in writing.

FNS requires submission of final documentation to validate all aspects of the project prior to closure. FNS verifies that the State agency has successfully completed all APD activities and notifies the State agency of APD closure. Since the closure process may include document review as well as on-site review(s), the standard FNS 60 day review timeframe does not apply. To close out a PAPD or an IAPD, the State must submit the information as shown in **Table 8**.

Table 8: Closure Documentation Requirements

Documents	PAPD	IAPD
Transmittal Letter (3.5.26)	●	●
Final project plan showing all work complete		●
Final summary of work complete	●	●
Final budget showing all expenditures by line item by federal fiscal year and quarter	●	●
Final cost allocation across all contributing entities (if applicable)	●	●
List of all deliverables and payments made to contractors or State IT staff	●	●
Description of the goals met by the project and any deviations from the last approved APDU	●	●



Table 8: Closure Documentation Requirements

Documents	PAPD	IAPD
Description of any problems encountered during system development and implementation and their resolutions		●
Description of any outstanding issues and how these will be resolved (these should be minor or closure cannot occur)		●
Estimate of annual operating costs for the new system		●
Documentation of any post-implementation reviews or reports conducted by the State or contractors, if available		●

If projects become dormant (display no activity for a substantial period of time) or are abandoned (no longer being conducted by the State agency) before they attain the goals set forth in the APD, FNS will contact the State to determine if a need still exists for the project. FNS may close the APD at its own discretion, terminate funding availability, and recover any unused funds owed, as applicable to each program. FNS will make every effort to close an APD only when the project has been completed or when there is mutual agreement with the State agency.

3.2.8 Post-Implementation Reviews

Before closing the IAPD, FNS may conduct a post-implementation review of costs and system functionality once the system is fully operational statewide.⁹ A critical reason for the post-implementation review is to ensure that the system is reviewed and evaluated before the warranty period expires. After implementation, a State agency may have a limited time to identify any problems or shortcomings with the system and to get them fixed during the warranty period.

The post-implementation review typically occurs approximately 6 months after system deployment statewide to accommodate the initial user learning curve. FNS may conduct an onsite post-implementation review to ensure the State accomplished the goals stated in its APD. This review encompasses the program, technical, security, and financial aspects of the system. FNS will require submission of a final Implementation APDU to update all aspects of the project.

FNS' post-implementation review may include verifying the following:

- Program policy is correctly implemented by the system
- The system reflects the specified system requirements as approved in the IAPD
- The system meets the FNS program's system functional and technical standards
- The system satisfies requirements in the areas of accountability, management, user training, documentation, security, and use of automated tools



- The information systems equipment and services are being properly used in meeting objectives described in the IAPD, and accurate equipment inventory records exist as required by [2 CFR 200.313\(a\)\(1\)](#)-Title and Use of Equipment by Non-Federal Entities¹⁰
- The actual costs of the project and any significant divergence from the cost estimates in the most recently approved APDU
- The cost allocation methodology was complied with and all charges made were for eligible costs
- All aspects of the system have been validated before the warranty period expires

The financial management (FM) portion of the review is often conducted separately as part of the planned FM reviews of State agencies conducted by FNS Regional Offices.

FNS will prepare a detailed report of its findings and submit the report to the State agency within 60 days of the review. The State agency has 45 days from the date of receipt of the review findings to inform FNS of its proposed corrective actions, if required.

3.2.9 Regional Office Fiscal Closure

Once FNS has determined a project may be closed from an APD standpoint, the APD will be referred to the FNS RO for fiscal closure. The FNS RO will compare expenditures reported in the annual APDU with reported expenditures for IS development from both of the following forms:

- Form FNS 798: WIC Financial Management and Participation Report
- Form SF-425/778: Financial Status Report with addendum

Any differences are to be examined and reconciled. There should be no significant differences between expenditures reported on the FNS 798 or SF 425/778 and those reported in the annual APDU. Reconciled expenditures should be compared with the approved APD budget to determine if budget revisions are required. In addition, the FNS RO should examine that the State has complied with the requirement to submit an APDU-As Needed with revised budget projections. The FNS RO must notify the designated SSO representative of any inconsistencies or inaccuracies in project budgets that cannot be reconciled. Otherwise, the SSO should be notified when the budget is reconciled and send a closure letter to the State agency.

3.3 APD Information Specific to Program or Project Type

Now that the general APD process has been described, this section describes the purpose and specific content of each type of APD along with unique preparation and submission requirements. It also describes the activities the State agency will perform as described in each type of APD once the APD is approved.



3.3.1 Planning APD

3.3.1.1 Purpose of PAPD

The Planning APD is a brief document (usually 6–10 pages) describing the plan of action to accomplish the planning activities for an IS project supporting certification, eligibility, or related EBT systems. It documents necessary planning for a State agency to determine the need for, feasibility of, and projected costs and benefits of an IS equipment or services acquisition. It includes a brief explanation for procuring IS equipment and/or services and developing information necessary to carry out the planning process and prepare an Implementation APD. A State agency must use a PAPD to declare its assurance that the system will meet program requirements; request prior approval; and obtain a commitment for federal funding from FNS to plan major system development efforts, enhancements, or upgrades.

The PAPD provides FNS and State agency officials with notification of the State agency’s intent to begin a formal planning process, describes the planning activities to be done, and explains how the State agency will manage the activities. It also describes the project purpose and goals. Submission and approval of a PAPD is required before a State agency begins to incur planning costs for system development efforts, system enhancements, or upgrades. Therefore, it is important to consult with FNS before initiating any planning activities.

Should the State agency decide to expand the scope of planning activities after the PAPD has been approved, an FNS-approved “PAPD Update As-Needed” is required to expend any additional funds.



An associated “PAPD Update As-Needed” funding request may also be necessary in WIC.

3.3.1.2 Related SDLC Activities for PAPD

After the PAPD is approved, the State agency will begin planning SDLC activities. These include requirements definition, a feasibility study including alternatives analysis, and a Cost Benefit Analysis (CBA). The purpose of these activities is to evaluate the existing system and its business practices, define the future system business requirements, identify feasible solutions, assess systems acquisition methodologies, and prepare the Implementation APD.

Planning activities can vary by State agency, with the primary aim of developing a viable Implementation plan suitable for the specific State agency program and operational environment. Among the typical planning activities, a State agency will conduct an evaluation of changes to the State IS. Planning should consider possible



replacement of the current system and assess State agency and local operational and policy changes. Planning should identify resource needs and determine the State or contractual resources necessary to implement and operate the system. The State agency may also use the planning period to explore specific approaches and technologies with critical stakeholders such as retail vendors, State and local staff, and technology staff. FNS recognizes that State agencies often start the planning process with a specific technology in mind. The focus of the planning activity is to perform activities and make decisions, as well as develop supporting information, that will be presented in the IAPD. The last step of the planning phase is the preparation of an IAPD, which is submitted to FNS for approval.

It is incumbent upon the State agency to notify FNS when the State legislature approves funding to support major IS initiatives that will affect program administration. Examples of State legislature activities that could impact program initiatives include deadlines for overhauling the system interfaces or organizational restructuring of the State agency that includes the program. This will provide FNS ample time to assess the magnitude and possible policy implications that a change from the legacy system may present. Information on any mandate, requirement, deadline, or funding from the legislature that is driving a project should be included in the submission. Please see section **3.2 The APD Process** or [7 CFR 277.18.\(d\)\(2\)](#)¹¹ for details of the PAPD process in its entirety.

3.3.1.3 PAPD Documentation Requirements

PAPDs are usually short, simple, and concise documents. Because of the nature of PAPDs, the required documentation tends to be a single narrative stand-alone document with attachments that include an initial planning phase schedule, an estimated budget, and a preliminary cost allocation plan. However, this varies depending on the complexity of the planning activities being undertaken. Consult with FNS for guidance and samples of the required PAPD documents, as needed.



For SNAP and WIC EBT, a PAPD is only required if the State agency is exploring new technology or expects to incur excessive planning costs. Otherwise, a PAPD for SNAP or WIC EBT is not required.

The components required when submitting a PAPD are outlined in **Table 9**. For detailed descriptions of each required document, refer to section **3.5 APD Components**.

Table 9: PAPD Documentation Requirements

Document Components	SNAP	SNAP EBT	WIC	WIC EBT
Transmittal Letter (See 3.5.26)	●	n/a	●	n/a
Executive Summary (See 3.5.13)	●	n/a	●	n/a
Schedule of Planning Activities, Milestones, and Deliverables (See 3.5.22)	●	n/a	●	n/a
Proposed Budget (See 3.5.19)	●	n/a	●	n/a
Resource Requirements (See 3.5.21)	●	n/a	●	n/a
Cost Allocation Plan (See 3.5.8)	●	n/a	As appropriate	n/a
Cost Analysis (See <i>Error! Reference source not found.</i>)		n/a		n/a



If the State agency uses in-house resources for the planning activities, then a statement of work (SOW) or description of the planning activities must be submitted to FNS.



After a State agency implements a WIC EBT delivery method statewide, the State agency must submit an IAPD for a replacement WIC EBT delivery method based upon the thresholds described in chapter **1.0**, section **1.5.1**.



For WIC or WIC EBT, the Cost Allocation Plan is needed only when multiple programs are participating in the planning.

3.3.1.4 Preparing the PAPD

The PAPD is preceded by a needs assessment conducted by the State agency. The results should be documented in a Business Case, which can serve as the basis for developing the PAPD.



For guidance on needs assessment and business cases, see chapter **5.0 System Planning**.

In the PAPD, the State agency will identify its intended planning activities. The PAPD should describe plans for evaluating the existing system and its business practices as well as plans to define the future system business requirements. The PAPD should explain in general terms how the State agency will prepare a Functional Requirements Document and conduct a Feasibility Study with an Alternatives Analysis to determine which option can best meet those requirements.

3.3.1.5 Submitting the PAPD



Submission and approval of a PAPD is required before a State agency begins to incur planning costs. Failure to do so may result in the disallowance of unapproved project costs. Any costs incurred prior to approval will remain the responsibility of the State agency. Approval of planning activities does not guarantee approval of FFP for implementation activities.

To initiate the planning phase, State agencies are required to submit a PAPD to FNS for prior approval. If seeking approval and funding from more than one federal agency, State agencies should submit all PAPDs and related documents directly to both FNS, the Department of Health and Human Services (DHHS), or any other participating federal agencies. These agencies are independent and submission to and/or receipt by one agency does not suffice as submission to and/or receipt by all participating agencies.

Figure 32 provides an overview of the PAPD Process from submission to beginning the planning activities described in the PAPD.

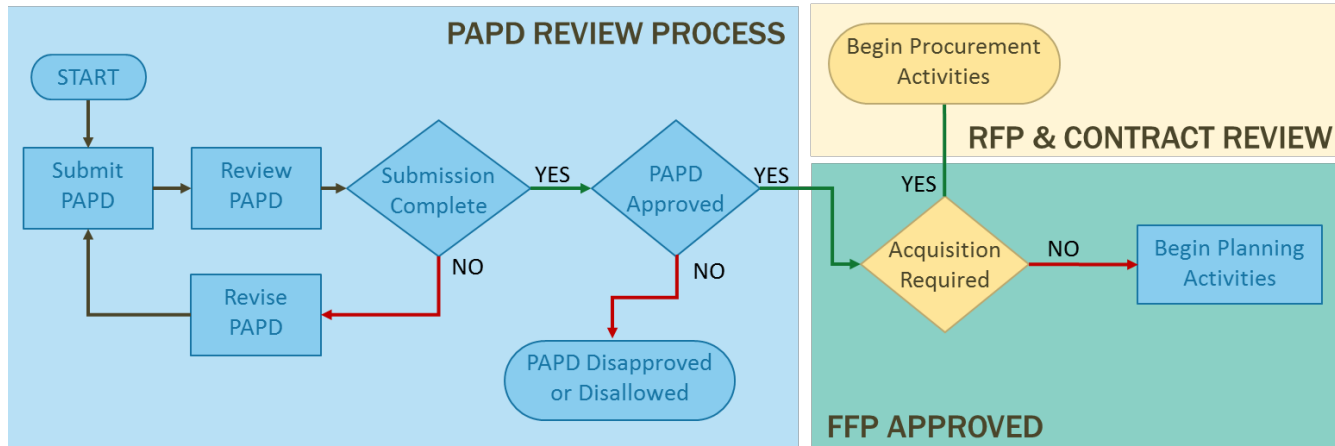


Figure 32: PAPD Process Map

Even if not seeking approval to expend federal funding for planning activities, the State agency is advised to notify FNS when embarking on system planning activities. This allows FNS to ensure efficiency in all ongoing systems efforts and confirm that no federal approval is required.

3.3.1.6 Performing Planning Activities

After the PAPD is approved, the State agency initiates the planning activities for requirements and objectives described in the PAPD. Planning activities will include preparing a Functional Requirements Specification or Document and conducting a Feasibility Study with an Alternatives Analysis and Cost Benefit Analysis. These activities include evaluation of the existing system and its business practices, definition of the future system business requirements, and development of a General Systems Design (GSD). These are SDLC Initiation phase activities the results of which are presented in the IAPD.

Other related planning activities include acquisition and procurement planning, project management planning, and financial planning (e.g., resource analysis, budgeting, and cost allocation). Preparation of an Implementation APD and a Request for Proposals (RFP) and development of a General Systems Design (GSD) begin when all planning activities are completed as described in the approved PAPD.



For guidance on the Feasibility Study, Alternatives Analysis, and Cost Benefit Analysis, see chapter **5.0 System Planning**.

Key tips for successful planning include the following:

- Collaborate early with program policy and IT staff



- Establish and maintain communications with all State and Federal partners based on long-term business goals to ensure that all agencies with potential program involvement are aware of the project when it is still in the planning stage
- Know all federal APD requirements and document approval time frames
- Know Federal and State contracting laws and requirements
- Talk with and visit other States with successful models and strong project management
- Engage workers, recipients, and other stakeholders in the system design as early and as much as possible
- Understand that communication is vital to successful planning and throughout the entire process

During the SDLC planning activities, which often take more than a year to complete, the State agency must submit APDUs annually and APDUs As-Needed when necessary.

The groundwork laid by activities accomplished and deliverables completed during the planning phase provides analysis, information, and decisions that will lead the State agency to prepare for and meet the requirements of the implementation phase and the IAPD. The State agency submits the results of the planning phase to FNS in the IAPD.

3.3.2 Implementation APD

3.3.2.1 Purpose of the IAPD

After the planning activities are completed and the results are analyzed, the State agency may request federal funding, or FFP, for the acquisition, development, testing, pilot, and full implementation of the proposed IS or EBT systems through an IAPD. The IAPD describes a project's completed planning activities, such as the identification, analysis, feasibility, and cost of various system alternatives; the general design of the chosen alternative; and the project's estimated budget and schedule. It also demonstrates the State agency's thorough preparation of and commitment to the design, development, and implementation SDLC phases to meet program requirements. The IAPD component parts provide the overall management plan for systems design, development, testing, implementation, and enhancements to operational systems.

3.3.2.2 Related SDLC Activities for IAPD

The IAPD addresses the details for the design, development, integration and testing, implementation, and maintenance and operations of a certification and eligibility system. The IAPD marks the completion of the planning phase of the SDLC and is the product of the planning process. The SDLC activities captured by the IAPD include the results of the feasibility study (e.g., requirements analysis, alternatives analysis, cost benefit analysis),



general systems design, development approach (e.g., waterfall, incremental, iterative), data conversion, test planning (e.g., user acceptance and pilot), security planning, and implementation planning (i.e., training, roll-out plan, schedule). Other related activities include project planning, financial planning (e.g., cost allocation, estimated costs, budget), and procurement. Guidance for these activities is provided in other chapters of this handbook.

3.3.2.3 IAPD Documentation Requirements

The State agency should consult with the internal State IT oversight department before preparing the IAPD. The State's internal monitoring process may require additional documents or procedures. However, it is possible the IAPD requirements may satisfy these internal monitoring requirements. The documents outlined in **Table 10** are required but are not necessarily submitted with the IAPD. Instead, some of these documents must be created but would only be submitted to FNS when requested. For detailed descriptions of each required document, refer to section **3.5 APD Components**.

Table 10: IAPD Documentation Requirements

● = Required for Submission

◆ = Not Required for Initial Submission

Document Components	SNAP	SNAP EBT	WIC	WIC EBT
Transmittal Letter (See 3.5.26)	●	●	●	●
Executive Summary (See 3.5.13)	●	●	●	●
Functional Requirements Document (FRD) (See 3.5.15)	● ^{##}		●	
Feasibility Study/Alternatives Analysis (See 3.5.14)	●		●	
Cost Benefit Analysis (See 3.5.9)	●		●	
General System Design (See 3.5.16)	●	●	●	
Capacity Plan or Study (See 3.5.4)	● ^{§§}	As appropriate	● ^{§§}	As appropriate
Project Management Plan (See 3.5.17)	●	●	●	
Resource Requirements (See 3.5.21)	●	●	●	
Schedule of Activities, Milestones, and Deliverables (See 3.5.22)	●	●	●	
Proposed Budget (See 3.5.19)	●	●	●	With funding sources table



Table 10: IAPD Documentation Requirements

● = Required for Submission

◆ = Not Required for Initial Submission

Document Components	SNAP	SNAP EBT	WIC	WIC EBT
Cost Allocation Plan (See 3.5.8)	●	●	As appropriate	
Security Plan ^{††} (See 3.5.23)	◆ ^{§§}	◆	◆	
Training Plan (See 3.5.25)	●	As appropriate	●	
Test Plan and/or Test Reports (See 3.5.24)	●	●	●	
Request for Waiver of Depreciation (if desired)	●		●	
Disaster Recovery Plan (See 3.5.11) for SNAP or EBT Disaster Recovery Plan for SNAP EBT (See 3.5.12)	◆	◆		
Implementation Plan	◆ ^{§§}			
Conversion or Transition Plan (See 3.5.7) - when the EBT service provider changes - when the SA changes technologies	◆ ^{††}	●	As appropriate	Submitted later, not part of IAPD
Data Conversion Plan	●	●	●	Submitted later, not part of IAPD
Detailed Design Document (See 3.5.10)		◆ ^{††}		
Request to “go live” with the pilot	●		●	
Request to “go live” with Statewide expansion	●		●	

^{††} These must be outlined at a high level and detailed plans submitted when finalized.

^{§§} Submit or commitment to generate, including a description of the process to be used.

3.3.2.4 SNAP EBT Required IAPD Documentation



If the State remains with the incumbent processor when re-procuring EBT transaction processing services, only changes in the system's design should be noted in the IAPD. If the State is transitioning to a new processor, then the additional documentation described below is required. If information is included in the RFP, contract, or vendor proposal, there is no need to duplicate it in the IAPD. FNS reserves the right to review additional documents or to require testing and documentation at its discretion, even if the State remains with the incumbent processor. Once the IAPD budget has been approved, the State agency can encumber costs under the contract.



Test plan(s), test scripts, and test reports may be submitted as part of an overall EBT conversion plan, but they are often separate because they involve different contractor/State staff and become critical at different points in the timeline.

In addition to the document requirements in **Table 11**, the following documents must be provided to FNS upon request:

- EBT-Only Retailer Conversion Plan
- Problem resolution/regression testing reports
- Dry run results
- Retailer agreement
- Training material for retailers and clients
- Retailer manuals
- Client, retailer, and Third Party Processor (TPP) notices



See the SNAP website for information on [waivers of rules](https://www.fns.usda.gov/snap/waivers/rules) at <https://www.fns.usda.gov/snap/waivers/rules>.



State agencies should keep in mind that tasks involving client contact are restricted to State merit system personnel unless FNS approves use of non-merit or vendor staff to perform certain tasks. Find this guidance on the SNAP website at [Federal Support for Enrollment and Application Processing Costs Supplemental Nutrition Assistance Program \(SNAP\) | Food and Nutrition Service](http://www.fns.usda.gov/snap/federal-support-enrollment-and-application-processing-costs-supplemental-nutrition-assistance).
(<http://www.fns.usda.gov/snap/federal-support-enrollment-and-application-processing-costs-supplemental-nutrition-assistance>)

3.3.2.5 WIC EBT Required IAPD Documentation



The WIC EBT IAPD process is aligned with the SNAP EBT IAPD process. Accordingly, states must submit an IAPD after a new WIC EBT transaction processor contract is negotiated and prior to the beginning of the new contract period before incurring any cost under the contract. At that point, the State agency will have more accurate cost data upon which to estimate the budget for the life of the new contract. The contents of the IAPD for EBT re-procurement are brief – as little as few pages. The IAPD need only include a transmittal letter, executive summary, cost allocation plan (if applicable), and anticipated budget. See **Table 11: IAPD Documentation Requirements** for more information.

3.3.2.6 Preparing the IAPD

The Implementation APD is a “document of documents.” The component documents are developed from the various SDLC activities such as **Lifecycle Management** (Chapter 2.0), **System Planning** (Chapter 5.0), and **Test Planning** (Chapter 6.0). Other key activities such as **Project Management** (Chapter 7.0), **Financial Management** (Chapter 8.0), and **Systems Security** (Chapter 9.0) contribute to the development of the IAPD. These chapters provide detailed information and critical factors that must be met to document the State agency’s plans for all aspects of the project’s success in the IAPD.

Consult with FNS for samples of the required IAPD documents as needed. FNS encourages State agencies to refer to existing materials and documents created for other recent projects as a guideline for preparing their own IAPDs. This enables States to benefit from each other’s experiences, streamline their efforts, and efficiently use their planning dollars. However, it is vital that all components of the IAPD accurately reflect each State agency’s individual and unique needs, expectations, resources, and so forth. When referring to sample documents, it will be necessary to revise and adapt the information to the current, proposed project.

3.3.2.7 Submitting the IAPD

Submission and approval of an IAPD is required before a State agency begins to incur implementation costs. Failure to do so may result in the disallowance of unapproved project costs. Any costs incurred prior to approval will remain the responsibility of the State agency. **Figure 33** provides an overview of the IAPD Process from submission to beginning the implementation activities described in the IAPD.



If the Security Plan and the Disaster Recovery Plan are to be completed as project deliverables, the State may submit the preliminary standards to which the new system must adhere, along with a commitment to complete and submit the full plan during the appropriate project phase.

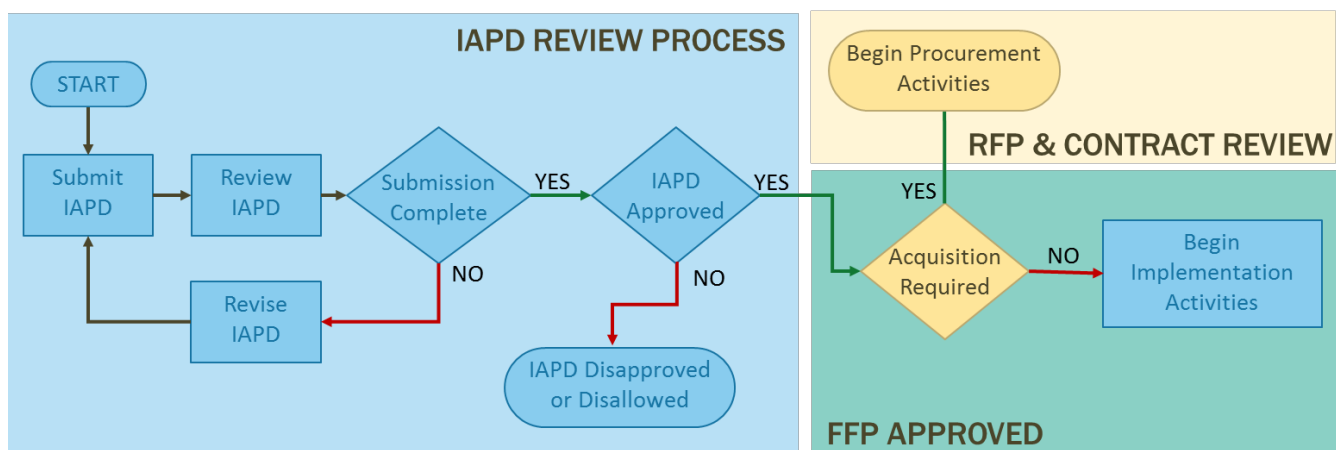


Figure 33: IAPD Process Map

3.3.2.8 Performing Implementation Activities

After the IAPD is approved, the State agency initiates the implementation activities necessary to produce and implement a successful IS or EBT System that meets the requirements and objectives described in the IAPD. Implementation activities will include design, construction, testing, and implementation. During these SDLC activities, which often take more than a year to complete, the State agency must submit annual APDUs and APDUs As-Needed when necessary.



Under the authority of federal regulations, FNS will monitor progress of the State's project using the APD Update (APDU) process, including regular conference calls and FNS site visits as needed. Other FNS oversight activities include required review and concurrence of the user acceptance testing (UAT) and approval of pilot results. This monitoring approach supports the high degree of interaction expected between FNS and the State agency as the project moves forward. The State agency is responsible for having performance expectations, prescribed remedies, and penalties in place that protect the State agency in the event of a failure in performance by the vendors.



Acquisitions and subsequent undertakings that fail to meet approved APD requirements will be subject to disallowance of costs in accordance with [7 CFR 277.18 \(h\)](#) or [7 CFR 246.14\(d\)](#).

Key tips for successful implementation include the following:

- Proper adherence to the IAPD process
- Including federal review periods in the schedule
- Allowing enough time for critical steps

Following these key tips can help States avoid project delays, estimate project progress and outcomes more realistically, and contribute to a successful project completion.

3.3.3 APD Update

3.3.3.1 Purpose of the APDU

To conduct its oversight responsibility properly for multi-year IS projects, FNS requires State agencies to provide annual updates for ongoing projects using APD approved FFP. The APDU keeps a State's PAPD or IAPD current by updating FNS on the project's progress, including accomplishments, adjustments in plans or approaches, problems, and changes in budget or schedule. Continued FFP for a long-term project depends on FNS approval of the APDU. When an approved APD provides limitations for a phased project, the APDU is the way the State agency obtains approval for successive phases of their projects. Any changes made in an Annual APDU will be carefully reviewed to ensure that they do not fall within the criteria for an APDU As-Needed. APDUs are not required to approve funding for maintenance and operations.



Annual APDUs are not required for SNAP or WIC EBT. An “APDU As-Needed” is required if costs will exceed the approved budget, the contract period changes from what is covered by the IAPD, or there is a significant change in the services provided.

3.3.3.2 Related SDLC Activities for APDU

Annual APDUs are for routine reporting only. Because the APDU is used for projects lasting longer than one year, it provides information related to the status of the SDLC activities that have occurred during the reporting period.

3.3.3.3 APDU Documentation Requirements

State agencies should include the components listed in **Table 11: Annual APDU Documentation Requirements** in the Annual APDU. For detailed descriptions of each required document, refer to section **3.5 APD Components**.

Table 11: Annual APDU Documentation Requirements

Documentation / Document	SNAP	SNAP EBT	WIC	WIC EBT
Transmittal Letter (See 3.5.26)	●	n/a	●	n/a
Project Status	●	n/a	●	n/a
Changes to the Approved APD	●	n/a	●	n/a
Revised Schedule of Activities, Milestones, and Deliverables (See 3.5.2.5)	●	n/a	●	n/a
Revised Budget (See 3.5.2.1)	●	n/a	●	n/a
Actual Expenditures to Date	●	n/a	●	n/a
Contractor Performance (optional) (See 3.5.6)	Optional	n/a	Optional	n/a

Any changes made in an Annual APDU should be carefully reviewed. If changes fall within the criteria for an APDU As-Needed, then the additional content requirements of the APDU As-Needed (see section **3.3.4.3**) must be met.

3.3.3.4 Preparing the APDU



Information for preparing the APDU is based on the State agency's financial records and project status reports for the project. The focus of the document should be on project progress in planning or implementing IT solutions, and the State agency's confirmation of its plans for the next 12 months. The APDU should answer the following questions:

- Does the document adequately update the APD since the last update or submission?
- What are the major accomplishments during the reporting period?
- Have significant changes in scope, schedule, or funding occurred?
 - If so, how do they affect the overall project?
 - Have project management plan and project schedule changes been reported?
 - Is adequate information and justification for the change(s) included?
 - Is the most current budget reflected in the document?
 - Is the most current schedule included in the document?
- Have changes occurred to the proposed functionality and/or hardware/software?
 - Have there been changes in technical solutions and IT solutions for program functions?
 - If so, how do they affect the overall project?
 - Are they adequately addressed/justified?
- Are there any changes to the cost allocation plan?
 - If so, has the budget been updated accordingly?
- Have significant changes in resources occurred?

3.3.3.5 Submitting the APDU

The State agency must submit electronic copies of the annual APDU no later than 60 days prior to the anniversary of the corresponding APD approval date unless the submission date is specifically altered by FNS. As shown in **Table 12**, Annual APDUs are required for all active PAPDs and IAPDs.

Table 12: APDU Documentation Submission Thresholds

Stakeholders		Project/Funding Source			
State Agency	FNS	SNAP MIS	SNAP EBT	WIC MIS	WIC EBT
Prepares and submits APDU no later than 60 days before the anniversary of initial PAPD/IAPD approval	Reviews within 60 days	For all approved PAPDs/IAPDs	n/a	For all approved PAPDs/IAPDs	n/a

Annual APDUs are reviewed and approved in the same manner as APDs. FNS reviews the APDU and notifies the State agency in writing if more information is needed. Once FNS is satisfied with the APDU, it approves the APDU and notifies the State agency in writing. FNS approval of an Annual APDU constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated. The approval includes approval for continued FFP, but is subject to the availability of funds. **Figure 34** illustrates the APDU process.

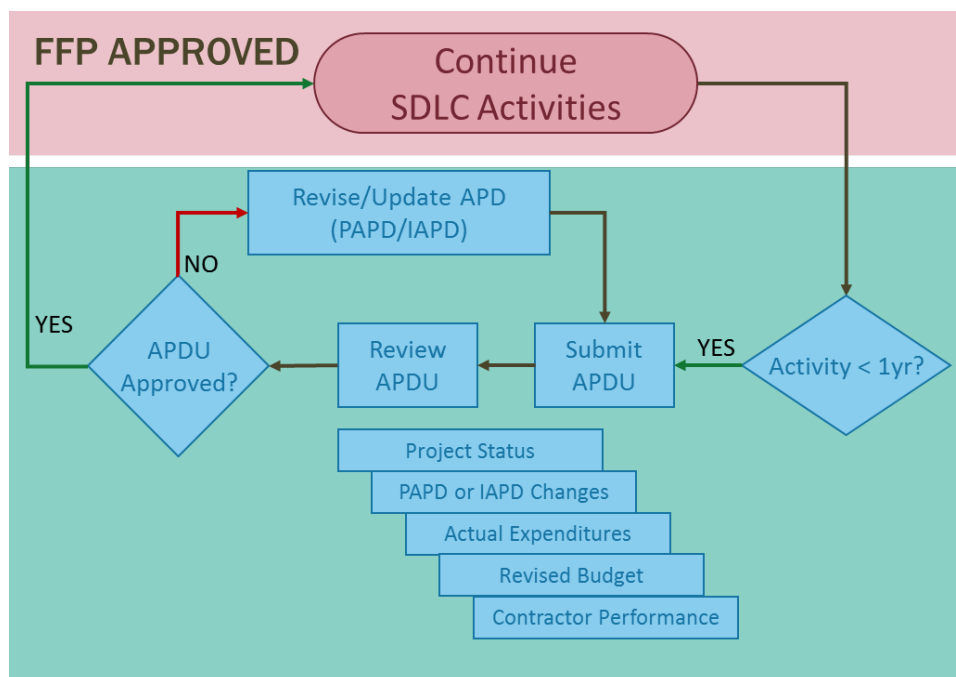


Figure 34: APDU Process Map

3.3.3.6 Performing On-Going APD Activities

Once the APDU is approved, the State agency continues performing the planning or implementation activities. If the APDU includes significant changes to an open PAPD or IAPD, State agencies may proceed with the changes without FNS approval to avoid project disruption, but would be liable for costs associated with the changes in the event of FNS disapproval.

3.3.4 APDU As-Needed

3.3.4.1 Purpose of the APDU As-Needed



The APDU As-Needed is used when a project encounters major changes in scope, cost, or schedule that require additional funding or approval from FNS. It is triggered by certain situations or events that require more immediate update and approval than the Annual APDU.

3.3.4.2 Related SDLC Activities for APDU As-Needed

The APDU As-Needed presents major changes that significantly affect the selected IS technical approach, scope, system architecture, or all of these. Depending on the needed change, many of the relevant SDLC activities for planning, implementation, or both may need to be done again on a smaller scale for the needed changes. Any ripple effects of the changes need to be considered for their impact on the approved SDLC activities.

3.3.4.3 APDU As-Needed Documentation Requirements

The APDU As-Needed is similar to an initial APD in that it identifies key factors to consider when changing the course of a project, especially as they relate to cost, scope, or schedule. The APDU As-Needed is not optional, but mandated by the triggers discussed below. An APDU As-Needed must be submitted whenever any of the following changes occur or are anticipated:

- A change in the availability of a funding source or an unanticipated change in a previously approved funding request
- A significant increase in total costs
 - **SNAP MIS and SNAP EBT** >\$10 million or 10 percent of the total project cost, whichever is less
 - **WIC MIS** >\$250,000 or 10 percent of the total project cost, whichever is less
- A significant schedule change for major milestones
 - **SNAP MIS** >120 days
 - **WIC MIS** ≥120 days
- A significant change in procurement approach and/or scope of procurement activities beyond that approved in the APD, such as:
 - A change in procurement methodology
 - A reduction or increase in the procurement activities that were described in the APD
 - A change in an acquisition (e.g., changing from a State blanket purchase agreement to issuing an RFP)
- A significant change in an approved system concept or scope of the project, such as a proposal of a different system alternative, a proposal for a different mix of system hardware and software (a change in platform), a change in the project plan, or a change in the cost-benefit projection
- A change to the approved cost allocation methodology



For WIC EBT, IAPDU As-Needed updates are only required once the total projected costs of the project exceed the approved IAPD amount.

State agencies must include the document components listed in **Table 13** in an APDU As-Needed. Some of these are necessary according to the situation causing the APDU As-Needed to be submitted. If there is no change to a particular component, a short statement to that effect is helpful to FNS when it reviews the APDU As-Needed. For detailed descriptions of each required document, refer to section **3.5 APD Components**.

Table 13: APDU As-Needed Documentation Requirements

Document	SNAP	SNAP EBT	WIC	WIC EBT
Transmittal Letter (See 3.5.26)	●	●	●	●
Executive Summary (See 3.5.13)	●	●	●	●
Project Status	●	●	●	●
Changes to the Approved APD	●	●	●	●
Revised Technical Approach (See 3.5.2.6)	As appropriate	As appropriate	As appropriate	As appropriate
Revised Functional Requirements (See 3.5.2.3)	As appropriate	As appropriate	As appropriate	As appropriate
Revised Project Management Plan (See 3.5.2.4)	As appropriate	As appropriate	As appropriate	As appropriate
Revised Schedule of Activities, Milestones, and Deliverables (See 3.5.2.5)	As appropriate	As appropriate	As appropriate	As appropriate
Resource Requirements (See 3.5.2.4)	As appropriate	As appropriate	As appropriate	As appropriate
Revised Budget (See 3.5.2.1)	As appropriate	As appropriate	As appropriate	As appropriate
Revised Cost Allocation Plan (See 3.5.2.2)	As appropriate	As appropriate	As appropriate	As appropriate
Contractor Performance (See 3.5.6)	Optional	Optional	Optional	Optional

3.3.4.4 Preparing the APDU As-Needed

The APDU As-Needed should discuss accomplishments to date, any problems that may have caused delay and/or affect cost estimates, and provide an updated project schedule and budget. It is specifically used for prior approval of changes in funding levels, project timeline extensions or delays, changes in procurement methodology, changes in cost allocation methodology, or changes in scope or system architecture. These include not only the nature of the proposed change, but also the effect that change will have on those portions of the project in which FNS and the State agency have already invested. Budgets should be itemized by federal fiscal year and by quarter.



See appendix **A8 Sample Budgets** for examples of budget formats.

3.3.4.5 Submitting the APDU As-Needed

It is imperative the State agency submit the APDU As-Needed as soon as it becomes aware of major changes in scope, cost, or schedule. Significant changes not reported in a timely manner may not be approved, and costs may be disallowed. State agencies are at risk for the costs of IS projects' attributes that do not comply with the approved APD until written FNS approval is granted. To avoid any gaps in funding approval, the State agency must submit an APDU As-Needed as soon as significant changes are known but no later than 90 days from the time when significant changes are anticipated to occur.

If a State submits an APDU As-Needed document and shortly thereafter an Annual APDU, information provided in the former will likely be included in the latter. This could divert limited State resources for preparing a relatively unnecessary document and FNS resources to reviewing a redundant one. In such instances, there may not be a need to submit an Annual APDU. To maintain consistency with other federal agencies and lessen the State agency reporting burden, FNS may waive the submission of another Annual APDU for up to 18 months.

FNS may waive the requirement for a State to submit its Annual APDU when it has submitted an APDU As-Needed within 6 months. FNS may either:

1. Reset the State's anniversary date for submitting its next Annual APDU from the date of the original APD approval to that of APDU As-Needed approval
2. Waive the Annual APDU for that year if the budget submitted for the APDU As-Needed covers the full period. FNS reserves the right to request additional information or updates in the interim.

When the State agency submits the APDU As-Needed to FNS, FNS responds to it in the same manner and time frame as an APDU (See **Figure 34**, page 139). FNS approval of an APDU As-Needed constitutes its acceptance of the State's activity update and any significant changes, unless otherwise stipulated.



3.3.4.6 Performing As-Needed Activities

The State agency continues to conduct its systems development activities (i.e., planning and implementation) as described in the PAPD or IAPD.

Federal approval of the APDU As-Needed for project changes is required no later than the time when the next Annual APDU is due. State agencies may proceed with the change without first obtaining federal approval to avoid disruption in project activities. In such instances, the State agency would be liable for costs associated with the project change until FNS approval is granted. If the APDU is subsequently disapproved, the costs associated with the project change would not be allowed.

3.3.5 Emergency Acquisition Request

3.3.5.1 Purpose of the EAR

An Emergency Acquisition Request (EAR) is a brief written request from the State agency to FNS for FFP to allow the State agency to take prompt action due to extenuating circumstances that require immediate action. The EAR often impacts acquisitions that under normal circumstances would be approved under IAPD time frames. An EAR may be submitted when both of the following conditions exist:

1. The State agency can demonstrate to FNS an immediate need to acquire IS equipment or services to continue system operations
2. The State agency can clearly document that the need could not have been anticipated or planned for and that the need prevents the State from following the prior approval requirements

Examples of such situations include equipment failure attributed to physical damage or destruction caused by natural or other disasters and changes imposed by federal legislative requirements that necessitate immediate acquisition of IS equipment or services.

FNS will not consider circumstances arising from poor planning by the State agency to be an emergency situation. Failure by the State agency to begin acquisition procedures of equipment or services in a timely manner to meet the requirements, deadline, situation, or event does not constitute an emergency. The State agency may not submit an EAR for approval of a sole source selection of a vendor to continue operations. Each State is responsible for knowing the procurement and contracting processes and their timeframes and must plan accordingly.

All acquisitions approved under an EAR must be included in an IAPD submitted after the emergency situation is under control. This allows FNS sufficient time to establish that funding for the acquisition can otherwise be approved under normal IAPD provisions. Following the approval of an EAR, FNS will work with the State agency to determine what portions of the IAPD process are applicable and what steps must be taken.



3.3.5.2 Related SDLC Activities for EARs

Because an EAR is an unexpected event, there is not a routine SDLC activity associated with it as is the case with other types of APDs. The EAR will correspond to whichever SDLC activity is ongoing when the emergency occurs. When coordinating with FNS to determine which IAPD activities apply, the relevant SDLC activities will be clarified for preparing the IAPD.

3.3.5.3 EAR Required Documentation

The information required by the EAR may be included in the State's transmittal letter to FNS, or the EAR can be a separate document enclosed with the transmittal letter. Requirements for an EAR are listed in **Table 14**.

Table 14: EAR Required Documentation

Document Components	STATES
Transmittal Letter (See 3.5.26)	●
Description of the IT equipment or services to be acquired	●
Cost estimate of the IT equipment or services to be acquired, to include only costs not recovered by insurance	●
Description of the circumstances that have resulted in the State agency's need to proceed with the acquisition before obtaining formal FNS approval through the normal prior approval procedures. The State agency must document that its immediate need to acquire IT equipment or services was unexpected and could not have been anticipated or planned.	●
Description of the adverse effect that would result if the State agency did not immediately acquire the IT equipment or services	●
Justification of any sole-source procurements	●

The letter must identify the request as an EAR and include the name, title, telephone number, and e-mail address of the project manager. Moreover, the State's letter must specify the requested level of funding. It must also include a statement specifying which method of procurement will be used and that the procurement will be conducted in accordance with [7 CFR 277.18 \(c\)\(2\)\(iii\)](#) – Procurement Requirements¹².

3.3.5.4 Preparing the EAR

The EAR is prepared in either a letter format or a document that includes the information required to describe the emergency situation, required needs to resolve the situation, and the plan of action to resolve the situation.

3.3.5.5 Submitting the EAR

The State agency must submit electronic copies of the document as soon as practical before the occurrence of the emergency situation. If the emergency is the result of a natural disaster (e.g., flood, tornado, hurricane, earthquake, etc.), or destruction from an accident (e.g., damage not resulting from a natural disaster), the submission should be made as soon as is practical.

The State agency must submit an approvable IAPD or IAPDU no later than 90 days after the date of the initial EAR, or the federal funding for the EAR may be disallowed. An IAPD submitted in conjunction with an EAR will be evaluated in the same manner as other IAPDs.

The State agency should confirm receipt by FNS of its request. FNS has up to 14 days to render an approval recommendation and to inform the State agency of the results. To expedite communications during emergency situations, FNS may provide its decision informally, followed by an official written statement. Based on the severity of the emergency, FNS may electronically acknowledge the EAR as soon as possible, ensuring that copies of all correspondence, written or electronic, are retained as a record in the official files and available for review and formal IAPD response purposes.

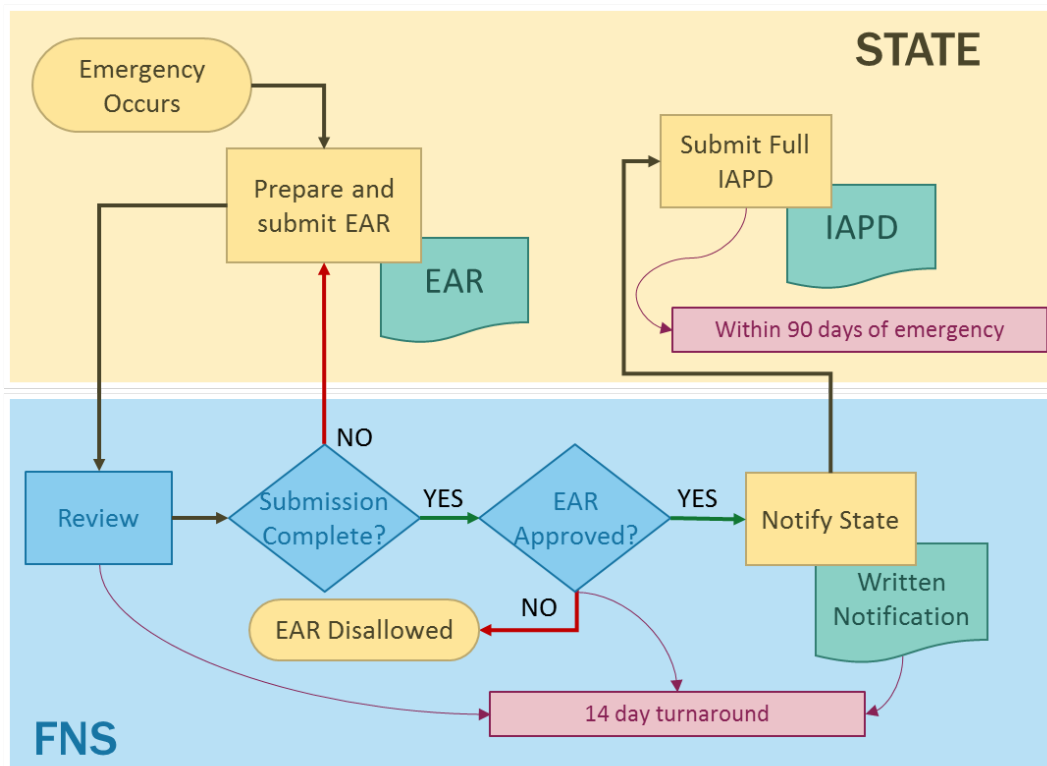


Figure 35: Emergency Acquisition Request Process Map

3.3.5.6 Performing EAR Activities

If the EAR is approved, FFP will be available to the State from the date the State agency acquires the IT equipment or services. State agencies may proceed with such acquisitions after they receive FNS written acknowledgment that an emergency situation exists, which will constitute FNS approval to proceed and ensure the availability of federal funds for allowable costs. This acknowledgment must be in specific reference to the State's request for an emergency IT acquisition. Any other FNS correspondence regarding disasters, disaster declarations, or other emergencies will not constitute an approval for emergency IT acquisitions.

If a State agency elects to proceed before receiving FNS written acknowledgment, it does so at its own risk, pending an FNS decision or until an approvable IAPD or IAPDU is submitted. Likewise, if the State agency does not submit the required IAPD or IAPDU within 90 days or submits a document that cannot be approved, FNS may disallow the FFP claimed for the emergency acquisition.

3.4 Post-Implementation APDs

Once implementation activities have been completed and the closeout Implementation APDU (IAPDU) has been approved, the maintenance and operations (M&O) phase of the SDLC begins. Prior approval of APDs (PAPD and IAPD as appropriate) during M&O are required only under specific conditions. Generally, these include significant hardware upgrades, platform changes, and software enhancements made to the system. APDs during the M&O phase specifically address any changes or needs that may arise during the remainder of the system's life.



For information on M&O, see **1.5.1.3 Maintenance and Operations**.

Otherwise, the following information requirements are necessary during the M&O phase:

- A description of hardware or software changes (may be in a Task Order or Contract Amendment)
- A budget reflecting State and federal costs by federal fiscal year and quarter (upon request)
- A description of how these changes will benefit the federal programs being served by the system



These information requirements may be satisfied by using information from an MOU, SOW, RFP, and contract or other document. Submission also requires a transmittal letter signed by the State official who has authority to commit State resources.



During M&O, the APD process is the same as when the system was first implemented, except the APDs don't encompass replacing the whole system. Instead, the APD process involves major enhancements or upgrades to the current system. However, the details of the APD process and related SDLC activities for enhancements and upgrades are no less important and must be followed with the same due diligence by the State agency as when the IS was first implemented.

3.5 APD Components

This section describes the various documents identified as components for each type of APD in previous sections of this chapter. No APD uses every one of these documents. Refer to the appropriate APD "Required Documentation" sections above to determine which of these documents is included with which APD.

3.5.1 Actual Expenditures to Date

Report of actual funds expended to date as opposed to estimated amounts.

3.5.2 Annual APD Update Revised Documents

When submitting the Annual APDU, the following documents should be revised as appropriate:

- Budget
- Cost Allocation Plan
- Functional Requirements
- Project Management Plan and Resource Requirements
- Schedule of Activities, Milestones, and Deliverables
- Technical Approach

3.5.2.1 Revised Budget

This addresses any increase or decrease in the approved budget, presented in required federal fiscal year and quarter line item format, identifying funding sources (both actual costs to date and estimates).

3.5.2.2 Revised Cost Allocation Plan

This addresses any change in the approved cost allocation plan resulting from budget increases or the addition or removal of participating programs.



3.5.2.3 Revised Functional Requirements

This incorporates additions to or deletions from the last defined functional requirements for the system. Examples include removing an interface or a function such as growth chart plotting or adding customized reports.

3.5.2.4 Revised Project Management Plan and Resource Requirements

This addresses changes in key personnel, staffing, and associated duties. Examples include moving project management in-house instead of contracting it outside, replacing key State or contracted personnel, losing essential resources in either the program or technical area, or changing the scope of quality assurance (QA) duties.

3.5.2.5 Revised Schedule of Activities, Milestones, and Deliverables

This includes changes (increase or reduction) in the amount of time needed to complete any activities, milestones, or deliverables, the addition or deletion of new activities or deliverables, or the combining of activities to reach a milestone or deliverable.

3.5.2.6 Revised Technical Approach

This addresses significant changes that affect the technical specifications and requirements of the system under development. Examples include a change from a distributed closed system to a web-based system or a change from a proprietary programming language to an open-source language.

3.5.3 Alternatives Analysis

This documents the results of the Alternatives Analysis performed during system planning activities feasibility study. An analysis of the option of transferring an existing system from another State or jurisdiction is required for SNAP and WIC.



See section **5.3** for details on the activities associated with a **Feasibility Study** including the **Alternative Analysis** (section **5.3.2**).



Appendix **A5 Feasibility Study Worksheet** has been provided to help the State agency document the feasibility study before preparing the detailed narrative for each system.

3.5.4 Capacity Plan or Study

This documents the capacity plan or results of the capacity study performed as part of system planning. It describes the size and expansion capabilities of the new system or the scope of enhancement to an existing system. A capacity plan or study determines the overall size, performance, and resilience of an information system and relates organizational needs to the system's configurations to establish a computer installation that adequately meets the organization's current needs and projections for growth. If the Capacity Study is not completed when the IAPD is submitted, a commitment from the State agency to complete the study will suffice until the Capacity Study can be submitted during the appropriate project phase.



See section **5.4** for details on the activities associated with **Technical Planning**.

3.5.5 Changes to the Approved APD

This addresses significant changes that affect the project plans approved in the APD. Examples include transferring from another State a system that performs similar functions instead of developing a new system; performing project management in-house instead of contracting it outside; or adding another program as a system user. It also identifies all changes to the approved APD including schedule, budget, scope, and/or requirements.

3.5.6 Contractor Performance

This identifies any issues, resolutions, strengths, weaknesses, and any significant change orders.

3.5.7 Conversion or Transition Plan

This is a detailed plan of all activities needed for the migration from the current system with minimal disruption. The plan should include a description of the overall approach, the order in which the transition activities will occur, tasks to be performed, the parties responsible for performing each task, and a back-up plan if any or all transition activities are delayed. The plan should define milestones and timelines.

3.5.8 Cost Allocation Plan

This describes the methodology used to determine the share each entity or program will pay in a joint effort.



A Cost Allocation Plan is only necessary if the planning activities are conducted in support of more than one program.



See section **8.5** for details on the activities associated with **Cost Allocation**.

3.5.9 Cost Benefit Analysis

This summarizes the results of the Cost Benefit Analysis (CBA) performed as part of the feasibility study. The CBA determines which alternative will provide the greatest benefits relative to its costs. The CBA provides a meaningful comparison of the costs of the alternatives under consideration.



See section **5.3** for details on the activities associated with a Feasibility Study including the Cost Benefit Analysis (section **5.3.3**).

3.5.10 Detailed Design Document

This is the developer's blueprint for system construction. The detailed design document provides precise directions to software programmers on how basic control and data structures will be organized. It typically consists of tables and diagrams that translate the functional specification into data structures, data flows, and algorithms. The document is written before programming begins and describes how the software will be structured and what functionality will be included. This document forms the basis for all future design and coding. The document includes a description of the overall design concept, a high-level summary of the design, standards and conventions to be used, program design describing the structure to be used via narrative, tables, flow charts, etc., and file designs and system data sets to be utilized.

3.5.11 Disaster Recovery Plan

Each State agency is required to develop a formal disaster recovery plan that encompasses the program certification and eligibility system. This plan can be part of a larger, overarching State agency plan, but it must detail how the State agency plans to recover and restore the system to normal operations. The Disaster Recovery

Plan is not submitted with the APD, but should be available if FNS requests it. Often, the Disaster Recovery Plan is part of the State agency's Security Plan.



See section **9.3.4.2** for details on the activities associated with ***Disaster Recovery Plans***.

3.5.12 EBT Disaster Recovery Plan

Responses to natural and man-made disasters have demonstrated EBT can effectively deliver SNAP benefits during a disaster situation, as well as the continued need for well-planned disaster EBT delivery methods, designs, and operational processes and procedures. As the only operational benefit delivery mechanism, EBT systems must deliver benefits during disasters. It is imperative that each State develops a disaster plan that provides for a system that can deliver SNAP and WIC EBT benefits during an emergency while successfully interacting with the State's eligibility system and its EBT contractor's system.



See section **9.3.4.2** for details on the activities associated with ***Disaster Recovery Plans***.

3.5.13 Executive Summary – General Guidelines

Additional requirements will vary based on the APD it is summarizing. When developing the Executive Summary, be aware that this document may be used to brief FNS management on the nature of the APD. State agencies should prepare the Executive Summary carefully, ensuring that all pertinent information is included.

The Executive Summary for the PAPD describes at a high level the business need for a new IS or EBT system, its advantages, the challenges and shortcoming the system will address and identifies the stakeholders who will benefit from it.

The Executive Summary for an IAPD contains more details particularly regarding the technical, financial, and program impacts of the project. **Table 15** provides general guidance on the type of information to include in the IAPD Executive Summary.



Table 15: Executive Summary Guidelines

Content/Issues	Information to be Addressed
General Information	• The nature of the project and the program needs or requirements the proposed information system is intended to meet or improve • The IS functions to be included and to what level (e.g., business rules engine and web services) • How the project fits into the State agency's IT strategy and plans (e.g., statewide telecommunication plan, central computer processing center) • The involvement of the State's top management in the project to ensure success and the proposed project management organization and responsibilities • A brief statement of the anticipated time period for the effort, including a statement about the State agency's ability to meet this preliminary schedule • The expected impact on State organizational entities that will be affected by system implementation, including issues such as staffing, business process, union contracts, and communications • A description of the State's planned mechanisms for quality assurance during project development
Program	• Commitment to involve State/local/county policy staff in project development as well as any other means necessary to ensure that the system implements program policy correctly • Commitment to meet all functional requirements necessary to achieve program compliance, as specified in program regulations and policy) • Commitment to ensure the system produces required program reports (e.g., for SNAP the FNS-388 and FNS-46)
Financial	• A statement indicating if the cost allocation plan has been approved by all appropriate federal partners and a description of any approved plan • A statement of proposed costs budget • A statement indicating whether a waiver of depreciation is being requested
Technical	• A summary of any analysis performed by the State agency to determine the availability of transferable systems or subsystems • A brief description of the proposed system architecture
Procurement	• A summary of the procurement process that describes plans for either single or multiple procurements and whether ownership rights for software will be affected

Table 15: Executive Summary Guidelines

Content/Issues	Information to be Addressed
	- A summary of the - Ongoing/planned management and operations approach - If in-house staff is to be used, assurance that technical expertise is available
Security	A statement of commitment to comply with FNS security requirements, including development of a disaster recovery and business continuity of operations plan

3.5.14 Feasibility Study

Summarizes the results of a preliminary study conducted during the planning phase that determines whether the considered project is technically, financially, and operationally viable, and presents the results of the alternatives analysis. The State agency must consider the transfer of an existing system or provide justification for excluding a transfer alternative from further consideration.



See section **5.3** for details on the activities associated with a **Feasibility Study**.

3.5.15 Functional Requirements Document

A Functional Requirements Document (FRD) is required for all programs receiving federal funding. The FRD is a comprehensive description of critical and desirable functions—a detailed set of processes and business rules—that must be contained in the new IS to support the program. As part of the IAPD, the State agency must identify the functions the proposed IS will perform.



See section **5.3.1.7** for details on the activities associated with the Functional Requirements Document and a Requirements Analysis (section **5.3.1**)

3.5.16 General System Design

A general system design consists of a combination of narrative and diagrams describing the generic architecture of a system, as opposed to the detailed architecture. A general system design may include:

- A system diagram
- Narrative identifying overall logic flow and systems functions
- A description of equipment needed (including processing, data transmission and storage requirements)
- A description of other resource requirements that will be necessary to operate the system
- A description of system performance requirements
- A description of the environment in which the system will operate, including how the system will function within the environment

If a system is to be transferred, the State agency may plan to use the general system design of the system to be transferred.

3.5.17 Project Management Plan

This describes the project oversight, reporting requirements for the State and contractor, and how the State will achieve professional project management.



See chapter **7.0 Project Management** for details on the activities associated with project planning and project management.

3.5.18 Project Status

This includes major accomplishments, challenges and resolutions, and outstanding issues for the project for the relevant time period, typically the last year.

3.5.19 Proposed Budget

This identifies estimated State and contractor total project costs associated with the implementation and/or planning phase activities. For example, State costs related to travel, staff time, equipment, IT support, and indirect costs, as well as contractor costs for travel, time, and deliverables. This includes a rough estimate of the cost of

any anticipated design, transfer, or implementation activities, which will be used for determining whether the threshold of prior approval submission is met.

A narrative should explain the basis for the estimated costs. Budgets must be presented by federal fiscal quarter for each year in the project and correspond with the project timeline. A brief narrative describing each budget item must be included. The funding sources should also be identified and addressed. The State agency must include a copy of their identified funding sources, demonstrating all project costs and allocated contributions for all projects.



See chapter **8.0 Financial Management** for details on the activities associated with budgeting (sections **8.6.3** through **8.6.7**).



See appendix **A8 Sample Budgets** for examples of budget formats.

3.5.20 Request for Waiver of Depreciation

This provides a means for expensing capital expenditures, rather than depreciating them, to financially benefit the Federal government. A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. This component is optional based on individual circumstances.



See section **8.4** for details on the activities associated with **Waivers of Depreciation**.

3.5.21 Resource Requirements

This describes what resources (e.g., staff, money) the State expects to apply during the relevant APD period (e.g., planning or implementation) and what the State agency needs from FNS. This should correlate directly to the proposed budget and should specifically outline the State's funding request to FNS.

During annual APDU, this identifies any changes in funding sources or amounts and updates the State's funding request, if applicable. It further addresses any changes in State resources, including staff, assigned to the project.



See appendix **A8 Sample Budgets** for examples of funding sources tables.

3.5.22 Schedule of Activities, Milestones, and Deliverables

This must be presented in narrative and graphical format. It includes detailed descriptions, timelines, and outlines of the key tasks, events, dates, and deliverables for the project. Major milestones with Go/No-go decision points should be identified. Any procurement schedules are to be described when contractor support is determined to be necessary. If the detailed schedule/timeline is to be supplied by a contractor or project manager to be hired after the APD is approved, the State agency may indicate this and explain the State agency's role in managing the schedule. The schedule component establishes how the State agency will accomplish the various tasks in a coordinated and timely manner. FNS staff will review the schedule to ensure that State agencies are accounting for critical aspects of their project, such as retail vendor enablement and external review timelines, and have a well-formed process to evaluate potential schedule modifications that could impact the project or lead to delays and/or cost increases.

3.5.23 Security Plan

The State agency will describe the security and interface requirements to be employed as well as the system failure and disaster recovery/business contingency procedures available to be implemented. The Security Plan will describe the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods. It will describe the approach and requirements that will be delivered as part of the project. This may be a description of the State security and interface requirements to be employed as well as the system failure and disaster recovery/business contingency procedures to be implemented. Preliminary plans may be submitted based on information available at the time of the initial APD and completed in more detail during the appropriate phase of the project.

This should include the State's Disaster Recovery and Continuity of Operations Plan for the system and operations at all levels—State and local/clinic. If the security and disaster recovery plans are to be completed as project deliverables by the contractor, the State may submit the preliminary standards to which the new system must adhere along with a commitment to complete and submit the full plan during the appropriate project phase. Please note, State agencies may indicate that components of the Security Plan are to be completed after contract award since some aspects are often subject to the contractor's proposed system.



See chapter **9.0** Systems Security and appendix **A14 Security Plan Checklist** for details on the activities associated with security.

3.5.24 Test Plan

The Test Plan describes how all system testing will be conducted in order to verify that the system complies with program requirements, design specification, performance standards, usability, capacity, and security. Testing includes, but is not limited to, unit testing, integration testing, performance testing, end-to-end testing, user acceptance testing, and regression testing.

At a minimum, the Test Plan must address:

- The types of testing to be performed
- The organization of the test team and associated responsibilities
- Test database generation
- Test case development
- Test schedule
- Acceptance testing
- Go/No Go criteria
- Contingency plans to revert to the legacy system if testing delays roll-out or the new system is determined to be unusable through testing

Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project.



See chapter **6.0** Test Planning and appendix **A15 Final Test Plan Template** for details on the activities associated with testing and preparing a test plan.

3.5.25 Training Plan

The State agency must describe how all system users, including staff at the State and local levels (including clients, as applicable), will be provided with training on the IS, including EBT systems, when applicable. The training statement must include a commitment to develop a comprehensive training plan that identifies the topic(s), the

training methods to be utilized, the duration, location, and staff identified for each topic. All training materials to be developed must be defined. The training plan must describe the training methodology and provide sufficient detail to encompass all possible users. The training plan must include a budget that identifies travel for the trainers and trainees, materials, facilities, and goods. The training plan may also include recommendations for refresher training and new staff training that may be conducted by the State agency after the system is fully operational. If the training plan is to be completed as a project deliverable by the contractor, preliminary plans may be submitted based on information available at the time of the initial IAPD along with a commitment to complete and submit the full plan during the appropriate project phase.

3.5.26 Transmittal Letter

This is a cover letter, signed by the appropriate State official, identifying the State agency sponsor of the project who has the authority and responsibility to commit State resources to the project, and who is responsible for ensuring the project goals and activities are carried out as identified within the APD. The cover letter requests federal funding and approval. A transmittal letter must accompany any document submitted to FNS that requires our approval.



See appendix **A7** for a ***Sample Transmittal Letter***.

3.6 APD Process Summary

- State agencies may receive federal funding to develop, acquire, and/or implement Information Systems that support the operation of FNS programs
- State agencies are required to submit an APD to FNS in order to obtain prior approval to receive or utilize federal funding for IS supporting these programs
- State agencies may not execute contracts or obligate funds without prior APD approval
- The APD describes in broad terms the State agency's plan for managing the design, development, implementation, and operation of an information system (IS) supporting SNAP, WIC programs, and related EBT systems
- The APD Process encompasses the preparation, submission, FNS review, and approval of the various APDs
 - The APD process is not the same as the SDLC but is closely associated with it
 - Where the SDLC focuses on system planning, development, and implementation, the APD focuses on documenting these SDLC activities



- The APD process is a series of successive steps through which a State agency can meet federal oversight requirements
 - The APD process has eight basic steps that are the same for PAPDs and IAPDs. These include:
 1. Prepare the APD (State agency)
 2. Submit the APD to FNS (State agency)
 3. Review the APD (FNS)
 4. Notify State agency of decision (i.e., approve or disapprove) (FNS)
 5. Conduct procurements when applicable (State agency)
 6. Perform activities described in APD (e.g., planning or implementation) (State agency)
 7. Provide annual APD updates, as appropriate (State agency)
 8. Close the APD when the activities described in the APD are complete (FNS and State agency)
- There are four types of Advance Planning Documents used by FNS
 - The Planning APD
 - Is a brief document describing the plan of action to accomplish the planning activities for an IS project supporting certification, eligibility, or related EBT systems
 - Explains how the State agency will manage the activities
 - Provides FNS and State agency officials with notification of the State agency's intent to begin a formal planning process
 - The Implementation APD
 - Describes a project's completed planning activities, such as the identification, analysis, feasibility, and cost of various system alternatives
 - Includes the general design of the chosen alternative
 - Documents the project's estimated budget and schedule
 - Demonstrates the State agency's thorough preparation of and commitment to the design, development, and implementation SDLC phases to meet program requirements
 - The Annual APD Update (APDU)
 - Informs FNS on the project's progress, including accomplishments, adjustments in plans or approaches, problems, and changes in budget or schedule
 - Supports FNS' oversight responsibility properly for multi-year IS projects
 - Is required annually for ongoing projects using APD approved FFP
 - Keeps a State's PAPD or IAPD current by updating FNS
 - The APDU As-Needed
 - Is used when a project encounters major changes in scope, cost, or schedule that require additional funding or approval from FNS
 - Is triggered by certain situations or events that require more immediate update and approval than the Annual APDU



- An Emergency Acquisition Request (EAR) is a brief written request from the State agency to FNS for FFP to allow the State agency to take prompt action due to extenuating circumstances that require immediate action. The EAR often impacts acquisitions that under normal circumstances would be approved under IAPD time frames.
- Document review timeframes are defined for all APDs and associated documents submitted to FNS
 - With the exception of the EAR, FNS has 60 days to review a document
 - After FNS reviews APD documents, including additional information that may have been requested, a decision will be made and provided to the State agency in writing
 - There are two possible decision outcomes: approved and disapproved
- Many planning and implementation projects involve procuring contractor services, equipment, software, or all of these
 - See Procurement (Chapter **4.0**) for additional information on preparing, submitting and the review of RFPs and contracts

Endnotes

⁸ “Emergency acquisition requirements”, 7 CFR 277.18(i)(2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.277&rgn=div5#se7.4.277_118

⁹ “State Systems Advance Planning Document (APD) process”, 7 CFR 277.18, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=f4d1db2cd8d4c78d879ba6acbc293ca6&mc=true&node=se7.4.277_118&rgn=div8

¹⁰ “Title and Use of Equipment by non-Federal Entities”, 2 CFR 200. 313(a)(1), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6be2b0655b5369194c9d1f70bd206f4f&mc=true&node=pt2.1.200&rgn=div5%23se2.1.200_1401#se2.1.200_1313



¹¹“APD content requirements Implementation APD (IAPD)”, 7 CFR 277.18 (d)(2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=f4d1db2cd8d4c78d879ba6acbc293ca6&mc=true&node=se7.4.277_118&rgn=div8

¹² “Procurement requirements”, 7 CFR 277.18 (c)(2)(iii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=f4d1db2cd8d4c78d879ba6acbc293ca6&mc=true&node=se7.4.277_118&rgn=div8



4.0 Procurement

Key Points

The information in this section should allow you to understand the following:

- When must a request for proposal (RFP) or contract be submitted for FNS review?
- How does FNS review process work for RFPs and contracts?
- What policies and regulations govern the acquisition and procurement processes?
- What are the different types of procurement?
- How does a State agency develop an RFP?
- What are the policy requirements that State agencies must address in all contracts?
- What federal assurances does FNS require to be included in a contract?

Chapter Contents

4.1	Purpose and Goals	165
4.2	Procurement Process Summary	166
4.2.1	Primary Procurement Documents	167
4.2.2	Pre-Award Phase	167
4.2.3	Award Phase	169
4.2.4	Post-Award Phase	172
4.3	Procurement Reviews	176
4.3.1	Determining the Need for Review	176
4.3.2	Overview of the FNS Review Process	179
4.4	Regulations and Policies	182
4.5	Roles and Responsibilities	183
4.5.1	FNS	183
4.5.2	State Agency	183
4.6	Technical Procurement Planning	184



4.6.1	Performance Requirements.....	184
4.6.2	System Transfer Considerations	185
4.6.3	EBT Conversion or Transition Planning.....	187
4.6.4	SNAP EBT Conversion or Transition Planning	188
4.7	RFP and Contract Planning.....	191
4.7.1	Preparing Criteria for Evaluating Proposals	192
4.7.2	Terms and Conditions.....	195
4.7.3	Incentives and Remedies	197
4.7.4	Quality Assurance Surveillance Plan (QASP)	198
4.7.5	Required Federal Assurances	199
4.7.6	Travel and Per Diem in Fixed Price Contracts	201
4.7.7	FNS Procurement Standards for State Agencies.....	201
4.7.8	FNS Specific Procurement Requirements	204
4.7.9	Order of Precedence	204
4.7.10	Disputes.....	205
4.7.11	Debarment and Suspensions.....	206
4.8	Procurement Methods.....	206
4.8.1	Competitive Procurements.....	207
4.8.2	Non-Competitive Procurements.....	211
4.8.3	Cooperative Purchasing.....	212
4.8.4	Contract Periods	215
4.8.5	Contractor Types and Roles.....	216
4.8.6	Conflicts of Interest	222
4.9	Procurement Documents.....	225
4.9.1	Request for Proposals.....	225
4.9.2	Contracts	226



4.9.3	RFP and Contract Components.....	227
4.10	Summary.....	231

Chapter Acronyms

ADR	Alternative Dispute Resolution
BAFO	Best and Final Offer
DDI	Design, Development, and Implementation
FAR	Federal Acquisition Regulation
FFP	Federal financial participation
IS	Information Systems
IV&V	Independent Verification and Validation
M&O	Maintenance & Operations
NASPO	National Association of State Procurement Officials
OMB	Office of Management and Budget
PoP	Period of Performance
QA	Quality Assurance
RFP	Request for Proposal
RO	Regional Office
SAM	State Agency Model
SLA	Service Level Agreements
SSO	State Systems Office
T&I	Transfer and Implementation
T&M	Time and Material Contract



For definitions of terms used in this handbook please see appendix **A1 Acronyms and Glossary of Terms**.

4.1 Purpose and Goals

This chapter is provided for State agencies administering FNS programs that need to acquire or purchase services from a contractor to meet their information system (IS) or EBT system needs. The information contained in this chapter is intended to serve as a guideline and is not meant to be a definitive step-by-step guide to procurement. The degree of detail in the State agency's procurement process will depend upon the extent of needed services and the phase of the Systems Development Lifecycle (SDLC) or APD process. State-specific procurement procedures are not included in this chapter nor are FNS program-specific regulations. It is vital that the State procurement or purchasing office be consulted and involved throughout the procurement process and that the State agency is aware of and adheres to FNS program-specific regulations for procurement.



FNS encourages State agencies to share their experiences and lessons learned related to procurement. Navigating the procurement process is not easy. State agencies should confer with other State agencies and seek assistance from FNS. This assistance might take the form of sample RFPs from States that have recently completed a similar, successful procurement.

The major objective for the State agency in a best value procurement process is to identify the best solution to meet the State's specific IS needs. In submitting a proposal in response to the State agency's Request for Proposal (RFP), the offeror's main objective is to prepare a cost-effective solution meeting State requirements and to win the business based on the strength of the technical proposal. For both parties, a common objective in any procurement process is to minimize the risk, cost, and effort required by all parties in pursuit of these major objectives. It is essential that the State agency and FNS ensure that there is fair and open competition to obtain the best value results from all IS procurements.¹³ **Figure 36** shows examples of situations that inappropriately restrict competition. These will be discussed in detail later in the chapter.

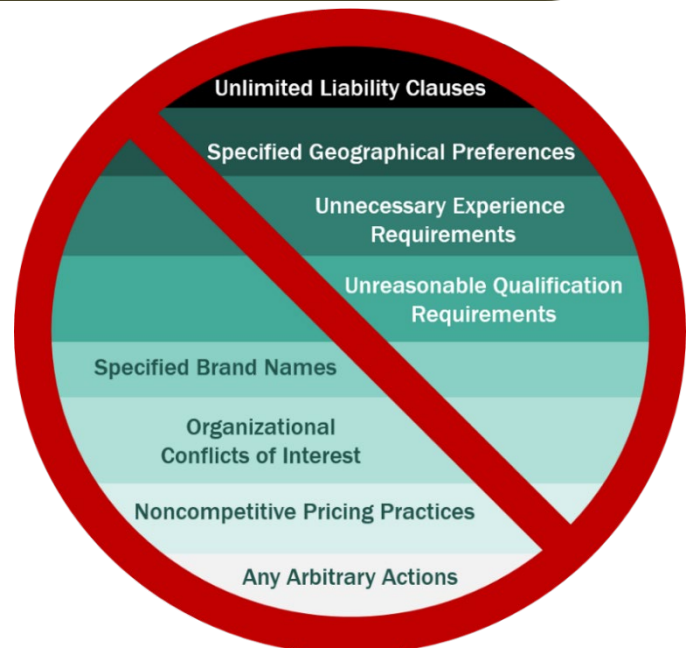


Figure 36: Inappropriate Restriction of

4.2 Procurement Process Summary

FNS recommends that State agencies conduct the procurement and contracting process in accordance with their State-defined processes. In general, most procurement processes include the same basic activities.



Acquisitions and procurements are described in detail in Chapter **2.0**, section **2.4 Acquisition Lifecycle Management**.

Procurements have three overall phases: Pre-Award, Award, and Post-Award.

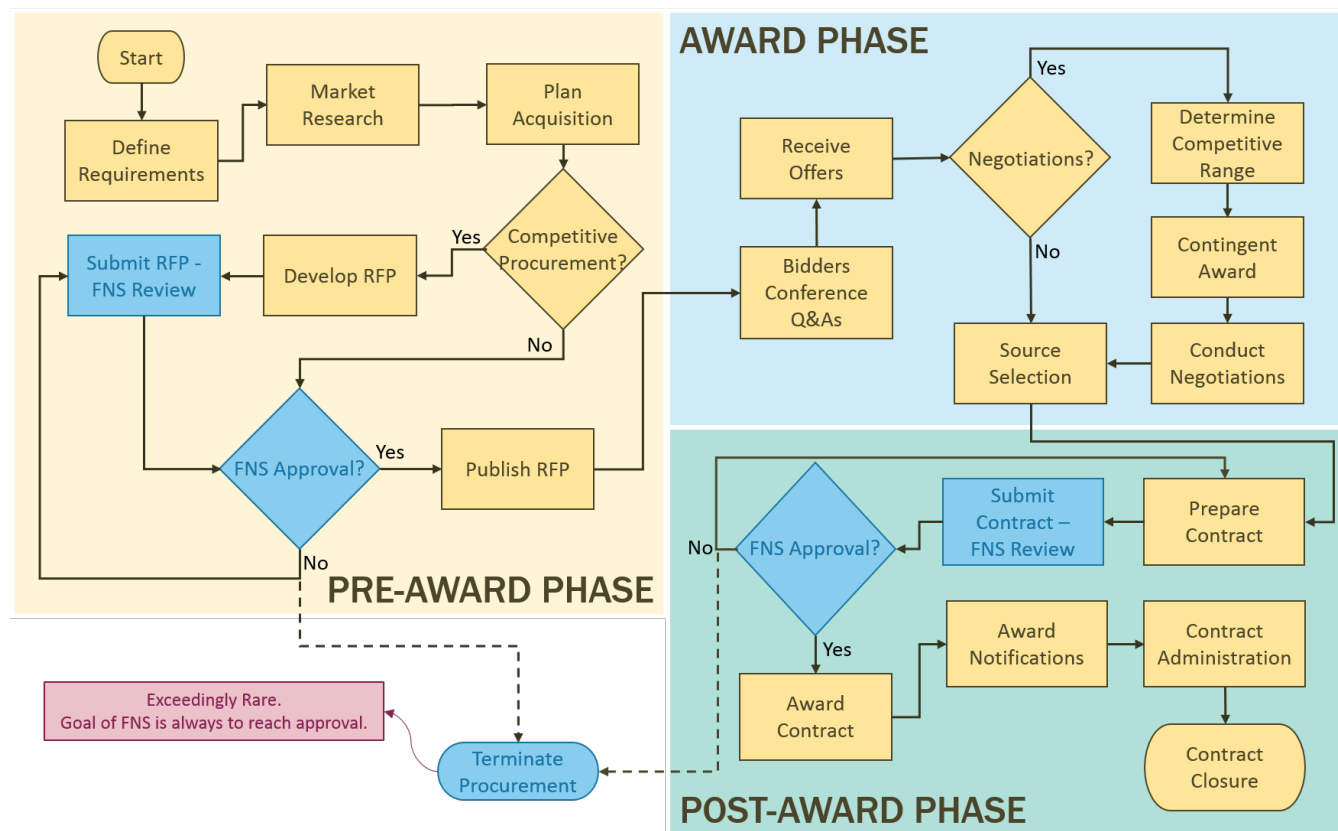


Figure 37: Procurement Process Overview



4.2.1 Primary Procurement Documents

There are two primary documents the State agency will use during the procurement process: the Request for Proposal (RFP) and the contract resulting from the source selection.

An RFP is the document that the State agency uses to obtain contractor support or to purchase hardware and software. The RFP solicits contractor services for a variety of efforts including planning activities, document development, software development, and IS development QA, operations, maintenance, training, change management, business process re-engineering, and other system lifecycle services. The State agency is responsible for ensuring that the RFP contains the components required by FNS and that it is consistent with State procurement regulations.

A contract is an agreement between the buyer (State) and the seller (offeror/contractor). It establishes a legally binding obligation for the seller to furnish goods and services and for the buyer to compensate the seller. The contract must clearly state and accurately describe the goods and services to be delivered or performed. It must include the terms and conditions of the agreement. All contracts must be in accordance with individual State procurement rules and regulations. In addition, contracts must be consistent with federal government regulations, including those of OMB. Therefore, all applicable Federal government requirements and program procurement provisions must be included in all contracts approved by FNS.

4.2.2 Pre-Award Phase

The Pre-Award Phase is when the majority of procurement planning occurs. Planning may include market research to identify availability of providers or to discover possible technology solutions. The definition of requirements may be among the services described in the PAPD to conduct system planning; likewise, definitions may be based on the system requirements definitions submitted with the IAPD.

4.2.2.1 Procurement Planning

A State agency needs to complete several specific procurement planning activities before preparing an RFP. These planning activities have an impact not only on the Pre-Award phase, but also on the post-award procurement phase. Thus, RFP planning is also contract planning. Procurement planning activities are dependent on SDLC planning activities and information from the relevant Planning or Implementation APD.

The State agency needs to answer several questions before drafting the RFP:

- What service or goods are needed?
- Are both services and goods needed?
- What specific requirements and deliverables are needed?



- How long will it take for the contractor to submit the identified deliverables?
- What is the estimated cost for procuring a solution to fit the needs identified?
- What kind of procurement is the best fit based on the needs identified and funding available?
- What kind of contractor seems best suited to deliver the identified needs?
- How can conflict of interest problems be avoided?
- How can fair and open competition be promoted?
- What criteria will be used to evaluate proposals and price quotes?
- What terms and conditions should be included to protect the State's investment in the project?
- What performance standards and penalties should be included?
- How should disputes with the contractor be handled?
- What federal assurances need to be included to remain eligible for FFP?

It is important to remember that source selection planning begins prior to RFP development and must be coordinated with the development of the RFP to ensure an effective evaluation of well-organized proposals. The Source Selection Plan should be agreed upon before the release of the RFP. In order to ensure an effective and defensible evaluation of proposals, the Source Selection Plan must be followed to the letter by everyone involved with the source selection. The RFP Section "Instructions, conditions, and notices to offerors or respondents" and Section "Evaluation factors for award" must mirror the same areas of the Source Selection Plan that address the information to the offerors and list the evaluation factors and sub-factors. The Government and the contractors can be assured of fair, unbiased evaluations of the proposals by ensuring that these areas contained in Source Selection Plan are replicated in the RFP. Likewise, the members of the Source Selection team should adhere to the Source Selection Plan.

Procurement planning produces the information to prepare the RFP. See section **4.6** for more details on procurement planning that takes place during the Pre-Award phase.

4.2.2.2 RFP Preparation

The State agency's acquisition strategy, developed during procurement planning, dictates requirements. The RFP must include terms and conditions, required federal procurement clauses, federal assurances, conflict of interest statements, and other legalities developed during procurement planning. These requirements are as important for the contractor as technical and functional requirements. All offerors must be aware of all requirements when building their proposals and price quotes.



RFPs may be written by State agencies or by their authorized contractors—FNS has no preference. However, the States must avoid any conflict of interest when using contractors to write an RFP. This section is intended to give guidance on FNS expectations and requirements for an RFP, regardless of where the State is in the APD process (e.g., planning, development and implementation, or maintenance and operations (M&O)).

The RFP is not a legally binding document. The contract that results from the source selection, based on the RFP, is the legally binding document. The contract would incorporate the RFP, excluding; the representations and certifications; selection criteria for awarding the contract; and instructions to offerors. The contract would include the offeror’s proposal, any changes in schedule or requirements and any negotiated terms that are different from or in addition to those specified in the RFP. An order of precedence should be included clarifying the relationship of the included RFP, proposal, and final negotiated terms.

4.2.2.3 RFP Review and Approval

Based on planning activities, for competitive procurements, the RFP will be developed and submitted for prior approval to FNS based on anticipated spending thresholds. Once approved, the RFP is published for vendors and contractors to bid. **Table 16: COMPETITIVE – RFP and Contract Document Submission Thresholds (page 177)** indicates the funding thresholds for the programs, and how they relate to each major procurement document (i.e., RFP, contract, and contract amendment). Non-competitive procurements may require FNS approval. (See **Table 17: NON-COMPETITIVE - Procurement Contract Document Submission Thresholds** for approval thresholds.)



The RFP should be available for vendor review and response for at least 90 days. If procuring in a high-demand market or time period, the State agency should be mindful of other States’ procurement schedules so they can benefit from maximum competition between vendors when there are fewer States’ solicitations posted.

4.2.3 Award Phase

Source selection is performed during the Award Phase. The key event during this phase is the evaluation of proposals based on price, technical response, past performance, and other criteria. The State agency may also



choose to have a bidders' conference. The purpose of a bidders' conference is to provide an overview of the procurement and to take questions from potential contractors at the discretion of the State procurement office.

4.2.3.1 Evaluating Proposals

An evaluation team is selected that can commit time for a thorough review of proposals. The evaluation team should include members from diverse stakeholder groups. Examples include the State program director, lead SME or policy specialist, EBT/vendor coordinator, State purchasing representative, IT department representative, and local agency representatives. The team should be trained on the purpose and goals of the solicitation, and on the evaluation criteria, process, and timeline. The evaluation team will assess the proposals in accordance with the evaluation factors specified in the RFP. The offeror with the highest score will be recommended to the procurement office for review and contract award.

When evaluating a proposal, the State should consider the following basic questions:

- To what extent does the proposed solution perform essential functions?
- Are program interests and goals represented?
- Are the proposed solutions appropriate for the tasks they are to perform?
- Is the technical proposal responsive and reflective of up-to-date technology?
- Is the use of industry standards by the offeror apparent in the proposal?
- Do system functions match specific State program needs in detail?

The State should be wary of bids that either offer what was not asked for or simply restate the requirements defined without specifying HOW to meet the requirements. Benefits of each proposed solution should be weighed in the context of managerial requirements and efficiency, as well as technological effectiveness. The evaluation must include an examination of the technical proposal and the proposed management structure based on all source selection criteria in the RFP. Once each proposal has been scored individually, the evaluation team may do a comparative assessment of all proposals. The evaluation team must be able to provide the rationale for its award decision.

Evaluating proposals is based on the information provided in the RFP developed during procurement planning. See section **4.7.1** for additional information on the specific evaluation considerations.

4.2.3.2 Source Selection

Source selection often involves either a sealed bid process or a negotiated competition. Sealed bids are typically used when purchasing noncommercial supplies or services. Negotiated procurements are more common and are described here. Negotiated procurements allow discussions with offerors before making final source selection. It



permits offerors the chance to revise offers before award of the contract and is a flexible process. During source selection, there is a continuum of options available for making an award decision.

These include:

- Best Value is oriented to obtaining the best value based on a combination of source selection approaches
 - Cost/price may dominate source selection criteria when requirements are clearly definable and the risk of unsuccessful contract performance is minimal
 - Technical Approach and Past Performance may dominate source selection criteria when more development work is required and successful contract performance is less certain
- Trade-Off is a process where there may be more benefits to the State agency than awarding the contract to other than the lowest priced offeror or other than the highest technically rated offeror
 - Evaluation factors and rating criteria are critical to this source selection process and must be clearly stated in the RFP
 - The perceived benefits of a higher priced proposal should merit the cost and the rationale for the trade-offs must be documented
- Lowest Price, Technically Acceptable (LPTA) is appropriate when the best value is expected to result in selecting a technically acceptable proposal with the lowest evaluated price
 - Evaluation factors must establish requirements of acceptability
 - Trade-offs are not permitted
 - Proposals are evaluated for acceptability but not ranked using non-cost/price factors
- Alternative Proposals are permitted in negotiated procurements as long as the proposal conforms to the significant or material aspects of the RFP
 - Offerors are allowed to propose changes to the RFP's terms and conditions
 - Alternative proposals may include the statement of work, alternative schedules, and/or alternative products or services

A competitive range is determined on the basis of the ratings of each proposal against all evaluation factors and refers to the range of proposals that are identified as the most highly rated depending on whether it is a best value, trade-off, or LPTA procurement. The competitive range consists of offerors that the contracting officer believes to have a reasonable chance of winning the contract.

Considerations for the competitive range should include:

- Strengths and weaknesses of each technical proposal
- Offeror's understanding of the requirements
- Reasonableness of costing and pricing data
- Management proposal (if applicable)



- Other special requirements of the RFP

Offerors outside the competitive range are eliminated from further consideration. If there is any doubt about whether a proposal is in the competitive range, the proposal should be included. When discussions or negotiations are necessary, the contracting officer should conduct written or oral discussions with all responsible offerors whose proposals are within the competitive range. These discussions should not disclose any information about competing proposals.

At the conclusion of discussions, all offerors in the competitive range should be given the opportunity to revise their proposals. The contracting officer notifies all offerors to submit their final proposals, sometimes call the “best and final offer.” Once final proposals are received, the contracting officer should not reopen discussions. Source selection is based on the final proposals.

4.2.4 Post-Award Phase

The Post-Award Phase begins when award notification is made. Any protests are resolved during the notification process. Once protests are resolved, if there were any, the contract is submitted to FNS for review and approval. Once approved, the contract is awarded, the award is finalized and the contract begins. The State agency oversees contract administration and the completion of deliverables. Once all services are completed and all deliverables are accepted, the contract is closed.

4.2.4.1 Contract Approval

Before the State agency can sign a contract, the contract must be submitted for prior approval by FNS based on anticipated spending thresholds (See **Table 16: COMPETITIVE – RFP and Contract Document Submission Thresholds** and **Table 17: NON-COMPETITIVE - Procurement Contract Document Submission Thresholds**). The draft contract should contain the majority of the information found in the RFP, or incorporate the RFP by reference. Parts that are excluded from the RFP would include the instructions to offerors on the format and content of the proposal submissions, evaluation criteria, and other topics related to source selection. New information in the contract, which would not exist in the RFP, would include requirement changes, scope changes, or other significant updates that occurred between RFP release and source selection. These changes are likely in the result of negotiations with the contractor. FNS will review all of these changes to ensure that the procurement is in compliance with federal policies for procurements and allowable use of FFP for IS projects.

4.2.4.2 Managing Contracts

Contract management and contractor management are processes to ensure that vendor or contractor performance and delivery of requirements meets the terms of the contract. Contract administration includes all

activities performed by the State Agency following contract award. Contractor management requires periodic evaluation of contractor performance to ensure that the State obtains the goods and services for which it will pay. The Quality Assurance Surveillance Plan (QASP) is the State agency's primary tool for this purpose. (See section **4.7.4** for more details.) Use of the QASP or a similar tool assists the State agency's tracking of timely, complete and accurate delivery of work products and services.

It is equally important that the RFP requests that the contractors submit a proposed management approach with their response. The RFP should also request that the contractors develop a project management plan as a deliverable based on the proposed management approach and technical approach. The project management plan describes how the contractors will manage their operations to meet contract requirements, both administratively and for delivering the solutions called for in the requirements section of the RFP. Because the project management plan is a deliverable of the contract, it becomes binding on the contractor to perform to what it describes.



The contractor's project management plan is not the same as the State agency's project management plan. However, the two project management plans should be synchronized to avoid conflicts. The two should be mutually supportive.

Good contract administration and contractor management help ensure the following outcomes:

- The contractor and the State agency completely understand their respective roles in the contract arrangement and their relationship during contract performance
- A clear and mutual understanding of contract requirements, terms, and conditions is achieved
- Any potential or current problems are promptly identified and resolved
- The State agency and the end users are satisfied with the product or service being obtained under the contract
- Federal requirements are met

4.2.4.3 Contract Amendments



The State agency must get prior FNS approval for SNAP MIS and SNAP EBT contract amendments involving cost increases that cumulatively exceed 20% of the base contract cost. All SNAP contract amendments, regardless of cost, must be sent to FNS for recordkeeping purposes.

WIC MIS and WIC EBT sole source amendments over \$250,000 that extend a contract require formal FNS review and response. All WIC MIS and EBT contract amendments, regardless of cost, must be sent to FNS for recordkeeping purposes.

All contract amendments must be submitted to FNS. For WIC MIS and WIC EBT projects, if the governing contract for the amendment was initially reviewed by FNS and it included the required federal provisions, then the amendment does not require formal FNS review and response. An exception, however, is that sole source amendments that extend the length of a WIC MIS or WIC EBT contract and exceed \$250,000 in cost do require formal FNS review and response. Contract amendments must always be submitted to FNS for review if the base contract was not competitively procured.

Prior written approval from FNS is required for SNAP MIS and SNAP EBT contract amendments that cumulatively exceed 20 percent of the base contract costs. Base contract means the initial contractual activity for a defined period of time. The base contract includes only the base period and does not include any options or amendments. SNAP MIS and SNAP EBT contract amendments that do not cumulatively exceed 20 percent of the base contract cost do not require FNS prior approval as long as the contract was competitively procured.

Amendments exceeding a cumulative 20 percent of the base contract will be subject to prior approval by FNS. This means that the first amendment for 15% would not be subject to approval. If a subsequent amendment for 6% is submitted, it would require prior approval because the cumulative total now exceeds the 20% ($15\% + 6\% = 21\%$). When a project exceeds the 20% threshold, FNS may at its discretion review the entire scope of the changes. FNS will not disallow costs that were not subject to approval.

States must determine if amendments to a SNAP or WIC contract trigger the need for the state's submission of an IAPDU As Needed, or, a new project IAPD. In general, FNS approval prior to amendment execution is not required for amendments that do not add cost or change the contract term, or do not impact FNS programs. However,

FNS may require States to submit contract amendments for approval even if they are under the threshold amount. This could occur if the contract amendment is not adequately described and justified in an APD or APDU.

4.2.4.4 Contract Closeout

Contract closeout is the process of completing and settling the contract to ensure that all terms, conditions, and deliverables have been met. A contract is not complete and ready for closeout until the contractor complies with all the terms of the contract, such as the following closeout actions:

- Disposition of material covered by confidentiality rules
- Disposition of State agency property
- Settlement of interim or disallowed costs
- Settlement of any subcontracts by prime contractor
- Closure of warranty period and resolution of any warranty coverage items

Closeout is completed when all administrative actions have been completed, all disputes are settled, and final payment has been made.



Because most IS projects will involve competitive procurements, the remainder of this chapter will refer to these types of procurements. See section **4.8.2 Non-Competitive Procurements** for additional information.

4.2.4.5 Disposition of Government Property

When FNS pays for property using FFP, in whole or in part, it becomes the property of the State upon procurement. The State agency may use the property for program purposes, as long as it is needed.

When this need no longer exists, the State agency may use the property where needed in the administration of other programs in the following order:

1. Other federally-funded FNS programs
2. Other federally-funded USDA programs
3. Other federally-funded programs

When a need in any of these categories ceases to exist, the property may be used for the State agency's own official activities under the following conditions:¹⁴



- If the property had a total procurement cost of less than \$5,000 per unit, the State agency may use the property without reimbursement to FNS
- If the property had a total procurement cost of more than \$5,000 per unit, the State agency may retain it for its own use, provided fair compensation is made to FNS for the FNS share of the property
 - Compensation is computed by applying the percentage of FNS participation in the cost of the property to the current fair market value of the property

If the State agency has no need for the property, disposition shall be made in accordance with [7 CFR 277.13\(b\)\(3\)](#)¹⁵ and [7 CFR 277.13\(c\)](#)¹⁶ and [2 CFR 200.311\(c\)](#).¹⁷ In general, disposition of the property will be made as follows:

- If the property had a total procurement cost of less than \$5,000 per unit, the State agency may sell the property and retain the proceeds.
- If the property had a procurement cost of \$5,000 or more per unit, the State agency will:
 - Ship the property to another site. If instructed to ship the property elsewhere, the State agency will be reimbursed with an amount that is computed by applying the percentage of the State agency's participation in the cost of the property to the current fair market value of the property, including any shipping or interim storage costs incurred.
 - Otherwise, dispose of the property. If instructed to otherwise dispose of the property, the State agency shall be reimbursed by FNS for the cost incurred in such disposition.

If disposition or other instructions are not issued by FNS within 120 days of a request from the State agency, the State agency will sell the property and reimburse FNS an amount that is computed by applying the percentage of FNS participation in the cost of the property to the sales proceeds. The State agency may deduct and retain from FNS' share \$500 or 10% of the proceeds, whichever is greater, for the State agency's selling and handling expenses.

4.3 Procurement Reviews

4.3.1 Determining the Need for Review

Management information systems often have lifecycles spanning years, from initial concept to final disposal. It is the project sponsor's responsibility to ensure appropriate resources are available to support the system throughout its lifecycle. Initially, there is the planning for the system's design, development, and deployment that starts the lifecycle. This continues with implementing the system and transitioning to maintenance and operations. Over time, the system will change due to maintenance needs, operational needs, upgrades, and enhancements. The level of support and types of service required during each phase of the system's lifecycle will need to accommodate the activities for the particular phase of the system's lifecycle and the changes that occur. State agencies often decide to use contracts to procure goods and services to handle the many lifecycle events



and support needs for IS for SNAP, WIC, and related EBT systems. These activities are often separate projects over the system's lifecycle. Depending on the type of activity and amount of money required for the project, advance planning documents may be required. Much of the information associated with the APDs supports the procurement decision-making process.



See chapter **1.0 *Getting Started with the Advance Planning Document (APD) Process*** for APD Document Submission Thresholds (section **1.5.1**).

Procuring goods and services may require FNS review and approval of the various RFPs and contracts. Changes and modifications (i.e., amendments) to existing contracts may also need FNS review and approval. As with the APD, submission is based on the potential dollar value of the contract or amendment. While related to APD thresholds, the need for FNS RFP and contract review determination is separate from APD thresholds. The thresholds are different for competitive (**Table 16**) and non-competitive (**Table 17**) procurements. If at any time a contract which is below the threshold requiring prior FNS approval later increases in cost to an amount above the threshold (see **Table 16** and **Table 17**) due to a change order, contract amendment, etc., the contract and supporting documents must be submitted to FNS for approval. For example, a State has an initial base contract for SNAP eligibility system enhancement work for \$5,000,000. If an amendment for additional hours estimated at \$1,500,000 is later negotiated by the State and vendor, the base contract and any change order, amendment, etc., will need to be submitted to FNS for review and approval. For SNAP, SNAP EBT, WIC, and WIC EBT a competitive procurement may transition to a noncompetitive procurement status if the procurement exceeds its available base period, or its options included within the base contract agreement or RFP. In this scenario, the procurement will be subject to the applicable noncompetitive contract and/or contract amendment requirements. Regardless of cost, all contract amendments must be submitted for FNS' records.

Table 16: COMPETITIVE – RFP and Contract Document Submission Thresholds

Procurement Documents	Competitive Procurements			
	Program/Funding Source			
RFP	SNAP	SNAP EBT	WIC	WIC EBT
State Agency prepares and submits RFP. FNS reviews within 60 days.	Total cost of the individual procurement is ≥ \$6M	For all procurements requesting or utilizing FFP	For all procurements requesting or utilizing federal funding ≥ \$250,000	For all procurements requesting or utilizing federal funding ≥ \$250,000
Contract	SNAP	SNAP EBT	WIC	WIC EBT

**Table 16: COMPETITIVE – RFP and Contract Document Submission Thresholds**

Procurement Documents	Competitive Procurements Program/Funding Source			
State Agency prepares and submits contract. FNS reviews within 60 days.	Total cost of the individual procurement is ≥ \$6M	For all procurements requesting or utilizing FFP	For all procurements requesting or utilizing federal funding ≥ \$250,000	For all procurements requesting or utilizing federal funding ≥ \$250,000
Contract Amendment	SNAP	SNAP EBT	WIC	WIC EBT
State Agency prepares and submits amendment. FNS reviews within 60 days.	For any amendment ≥ 20% of base contract cost (cumulative)	For any amendment ≥ 20% of base contract cost (cumulative)	For any amendment that increases the cost of the contract to the \$250,000 threshold	For any amendment that increases the cost of the contract to the \$250,000 threshold

Table 17: NON-COMPETITIVE - Procurement Contract Document Submission Thresholds

Procurement Documents	Non-competitive Procurements Program /Funding Source			
SOW or PWS and Sole Source Exception Request (SSER)	SNAP	SNAP EBT	WIC	WIC EBT
State Agency prepares SOW/PWS and SSER and submits. FNS reviews within 60 days.	For all procurements with total cost ≥ \$1M	For all procurements requesting or utilizing FFP	For any acquisition ≥ \$250,000	For any acquisition ≥ \$250,000
Contract	SNAP	SNAP EBT	WIC	WIC EBT
State Agency prepares and submits contract. FNS reviews within 60 days.	For all procurements with total cost ≥ \$1M	For all procurements requesting or utilizing FFP	For any acquisition ≥ \$250,000	For any acquisition ≥ \$250,000

Table 17: NON-COMPETITIVE – Procurement Contract Document Submission Thresholds

Procurement Documents	Non-competitive Procurements Program /Funding Source			
	SNAP	SNAP EBT	WIC	WIC EBT
Contract Amendment				
State Agency prepares and submits amendment. FNS reviews within 60 days.	For any amendment > 20% of base contract cost (cumulative)	For any amendment > 20% of base contract cost (cumulative)	For any amendment that increases the cost of the contract to the \$250,000 threshold	For any amendment that increases the cost of the contract to the \$250,000 threshold

4.3.2 Overview of the FNS Review Process

All RFPs, contracts, and their subsequent amendments that exceed applicable thresholds must be submitted to FNS for review and approval before their release or execution. If a State agency proceeds without FNS approval, it may be held liable for any incurred expenditures. The State agency is responsible for submitting the RFP, contracts, and their subsequent amendments to each individual federal agency that may be participating in the federal funding of the project. In other words, separate copies must be submitted to FNS and Department of Health and Human Services (DHHS) agencies if both are contributing FFP to the project. The time required to prepare one or more RFPs, obtain FNS approval, receive and evaluate bids, and award a contract must be factored into the PAPD and IAPD schedules.



FFP may be disallowed for procurement and subsequent procurement-related actions when FNS finds the procurement fails to comply with the criteria, requirements, and other activities described in the approved or modified APD.

In general, the review process for the RFP and the contract are the same. Only the content of the documents being reviewed differs. See **Figure 38: FNS Review Process for RFPs and Contracts** (page 181). Both the RFP and the contract are reviewed using the same criteria. FNS has 60 days to review the RFP or contract document(s) and notify the State of its decision or the need for revisions or clarifications. The official review time begins upon FNS receipt of the State agency's submission for review.



See appendix **A12 RFP and Contract Review Checklist**
for review criteria for RFPs and contracts.

In general, the following steps apply (see **Figure 38: FNS Review Process for RFPs and Contracts** next page):

1. The State agency prepares and submits the RFP
 - a. Start working on the procurement, at least 30-36 months in advance of current contract end dates if continuing or replacing services in an existing contract, such as M&O or EBT processing, to assure sufficient time for a competitive process and a smooth transition to a new vendor, if selected.
 - b. Submit the procurement to FNS at least 24-30 months in advance of the current contract end date to accommodate time for FNS reviews and approvals
 - c. Submit to FNS regional office with a copy to the applicable RO and SSO
 - d. Draft RFP to be accompanied by a transmittal letter signed by an official authorized to commit State resources
2. Upon submission, FNS will
 - a. Notify the State agency of receipt of the document
 - b. Conduct a preliminary review for completeness
 - c. Notify the state of any missing or incomplete components
 - d. Evaluate whether the scope of work, requirements, and deliverables are clear and specific
 - e. Determine whether the RFP requirements and selection criteria will assure fair and open competition
 - f. Coordinate comments and requests for information among FNS reviewers as needed
 - g. Provide written comments to the State agency
 - h. Provide technical assistance as needed and meet with the State agency on any negotiable matters
3. FNS approval decision will be conveyed by the RO to the State agency
4. The State agency releases the RFP and conducts source selection.
5. The State agency submits the negotiated contract to FNS for review and approval prior to execution. If the State agency will be transitioning to a new vendor, contract submission may need to be 12-18 months prior to the end of the current contract.
6. FNS coordinates response among FNS reviewers as needed.
7. The RO conveys FNS approval decision to the State agency.
8. Upon receiving FNS approval, the State agency signs and executes the contract.
9. The State agency provides FNS a copy of the final signed executed contract.

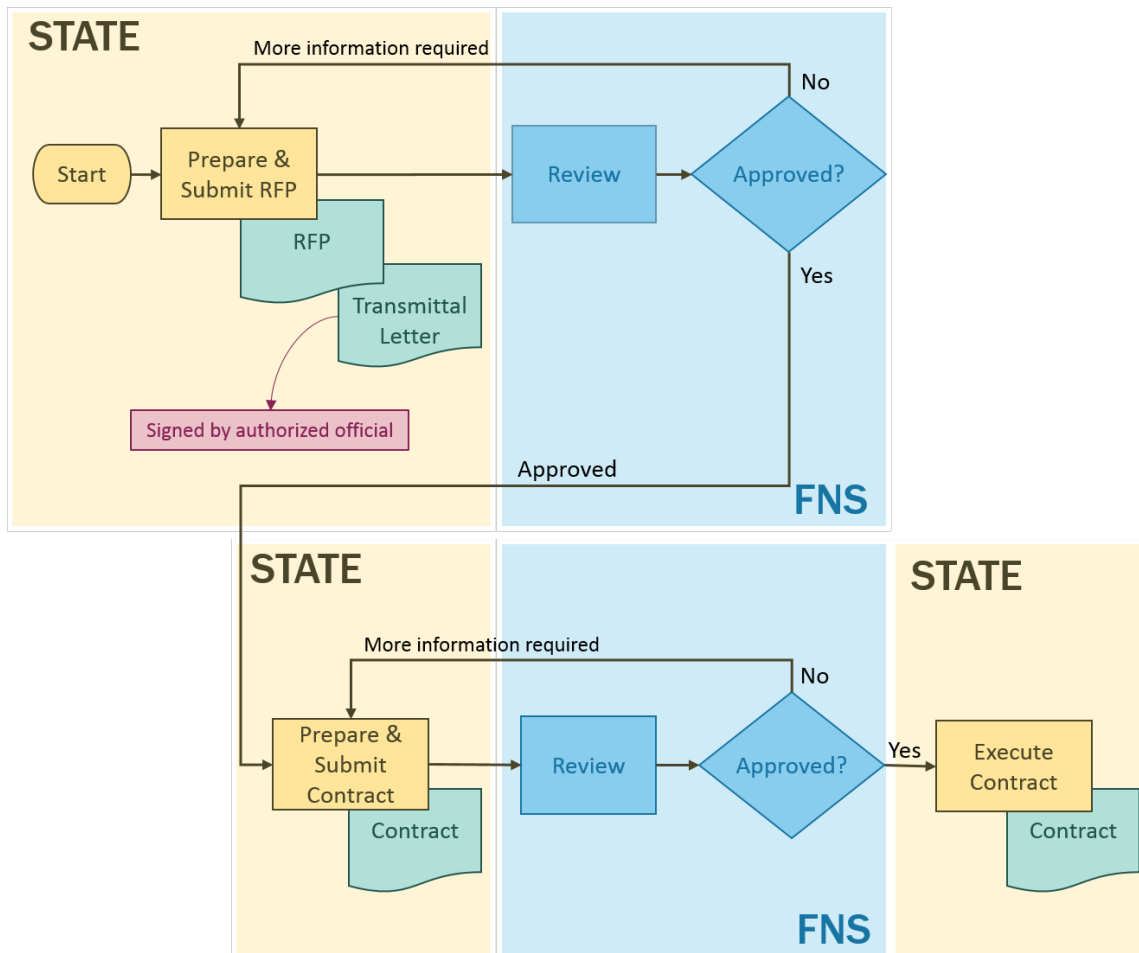


Figure 38: FNS Review Process for RFPs and Contracts

Once the RFP is published, the State agency notifies FNS of the publication date and provides a copy of the posted document to FNS. The State agency must submit any subsequent amendments that are made to the RFP. If a State makes any significant changes to the approved RFP prior to publication, these changes must be submitted to FNS for approval.



In accordance with SNAP regulations, provisional approvals are for SNAP submissions only. This occurs when FNS has not provided written approval, disapproval, or a request for additional information within 60 days of acknowledging receipt of the submission. However, provisional approval will not exempt a State from having to meet all other federal requirements that pertain to the procurement of IS equipment and services. Such requirements remain subject to FNS audit and review.

4.4 Regulations and Policies

There are two principal sources of authority for government agencies to acquire IT systems: Executive Direction and public law (legal basis). Executive Direction comes from the authority of the President and the federal government's executive agencies. These groups issue orders and regulations to enforce and facilitate the law, as well as help carry out the constitutional duties of the executive branch. Executive Direction includes the President, the Office of Management and Budget (OMB), and USDA. These offices generate Policy and Directives that impact the procurement process.

Examples of executive direction relevant to State procurements include the following:

[2 CFR 200.416](#) and [2 CFR 200.417](#)¹⁸ Cost Principles for State, Local, and Indian Tribal Governments establishes principles and standards for determining costs for federal awards carried out through grants, cost reimbursement contracts, and other agreements with State and local governments, including federally recognized Indian tribal governments (governmental units).

Regulations at [7 CFR 277.14](#) - Procurement Standards¹⁹ require State agencies to conform to the following standards for procurement using FNS funds:

- Maintain a contract administration system that ensures that contractors comply with the terms, conditions, and specifications of their contracts or purchase orders
- Maintain a written code of standards of conduct for employees involved in the award and administration of contracts to avoid conflict of interest
- Enter into State and local intergovernmental agreements for procurement or use of common goods and services for greater economy and efficiency
- Use federal excess and surplus property in lieu of purchasing new, whenever the use is feasible and reduces project costs



- Provide a review of proposed procurements to avoid duplications or unnecessary items and strive to obtain the most economical purchase
- Evaluate RFPs and make awards only to responsible contractors that possess the ability to perform successfully under the terms and conditions of a proposed procurement
- Use time and material-type contracts only after determining that no other contract is suitable and that the contract includes a ceiling price that the contractor exceeds at its own risk
- Be responsible for the settlement of all contractual and administrative issues arising out of procurements, disputes, and claims, including protests
- Establish protest procedures to handle and resolve disputes
- Maintain sufficient records to detail significant history of the contract. Include the rationale for the method of procurement, selection of contract type, contractor selection or rejection, and the basis of the contract price
- All State agency procurement transactions must be conducted in a manner that provides maximum open and free competition

State agencies use their own applicable State procurement regulations and standards to prepare procurement documents using federal funds. These regulations and standards must conform to federal standards and ensure that the procurement is conducted in the most effective and economical manner.

4.5 Roles and Responsibilities

4.5.1 FNS

FNS reviews RFPs and contracts to ensure that State agency procurements are in compliance with federal policies for procurements and with allowable use of FFP for IS projects. FNS provides guidance and technical assistance to State agencies to remain eligible for FFP and provide federal stewardship of FFP. FNS has 60 days to review and notify the State of its decision or the need for revisions or clarifications.

4.5.2 State Agency

Some roles, responsibilities, and authorities for IS procurements are specified by regulation. For example, [2 CFR 200.313 Equipment](#)²⁰ requires the State agency to use, manage, and dispose of equipment acquired under an award in accordance with State laws and procedures. Other roles and responsibilities may vary from procurement to procurement and from State to State. Regardless, a senior-level official should designate a procurement team (**Table 18**) with responsibilities for each procurement early in the process.

**Table 18: State Agency Roles and Responsibilities**

Role	Responsibilities
Project Sponsor	• Ensure appropriate representation by the Program Office • Ensure that the organization's long and short-term needs are met through the procurement process • Seek to maximize the benefits resulting from the management of multiple related projects • Provide material for inclusion in the RFP • Prepare and submit a cost estimate to the contracting officer as soon as possible in the pre-solicitation phase
Project Manager	• Represent the Project Office • Work with the contracting officer to define the contract management plan, including acceptable performance criteria • Ensure that the organization's long and short-term needs are met through the procurement process • Oversee progress of the project • Ensure that the procurement complies with federal requirements for the program
Information Systems Manager	• Provide technical expertise to the project manager and contracting officer throughout the procurement process
Contracting Officer	• Prepare the RFP package and incorporate input from the program manager • Issue the RFP when it is complete and accurate • Enter into, administer, and terminate contracts and make related determinations and findings

4.6 Technical Procurement Planning

The primary purpose for procuring goods, services, or both for an IS project focuses on the technical and functional requirements. This section describes some technical considerations when planning the procurement and the resulting RFP and contract.

4.6.1 Performance Requirements

When planning procurements, the area often getting the most attention is the technical requirements. Requirements planning is covered extensively in other HB901 chapters (e.g., chapter **5.0 System Planning**, chapter



6.0 Test Planning, chapter **9.0 Systems Security**). In addition to planning the technical requirements, the State agency must also focus on the performance requirements for the contractor or vendor. The performance requirements define HOW the contractor will deliver the technical and functional requirements. They also include HOW the contractor and the State agency will interact over the course of the period of performance.

FNS recommends that the RFP require the contractor(s) to perform the following activities:

- Use configuration management (CM) software during design, development, and testing
- Develop requirements documents (which may include use cases) that require sign-offs when accepted by the State agency
- Implement a change control process to document all requested changes to the system and to track their status to help control scope creep and to ensure that all currently implemented and future requests are documented
- Conduct an incremental system demonstration every few months during development, as appropriate
- Provide detailed system and functional requirements, system design specifications, source code with inline comments, and a complete system installation guide
- Ensure that the system under development occurs in accordance with FNS program requirements and regulations

The State agency should consider several other performance requirements arising out of the technical and functional requirements. These include the impact of plans on project timelines and schedules for data migration, testing and pilot activities, and transitioning any incumbent contractors. The State agency should request that offerors detail how they will approach all of these topics as part of their management and technical approach responses.

4.6.2 System Transfer Considerations

System transfers deserve special attention when planning procurements. There are technical considerations as well as intellectual property issues to consider (see sections **4.7.7.6 - Ownership and Licensing** and **4.7.7.7 - Intellectual Property Rights &** and appendix **A16 Ownership Rights**).

For State system transfers, the general system design or system specification may reference an existing State system as a possible transfer that contains the level of IT and functionality desired but it must be clear this is a sample and does not state a preference. The RFP must ask for the best possible system solution. However, the RFP itself cannot request transfer of a specific State system. States can identify the specific functionality and technical platform and cite examples of required functionality, but should not specify a State system by name in an RFP. Exceptions to this are discussed below.

4.6.2.1 WIC State Agency Model (SAM) Exception



An exception to specifying State systems by name for transfer would be for those WIC State agencies seeking a State Agency Model (SAM) transfer. State agencies transferring a SAM must specifically explain the nature of their intended transfer project to ensure that potential vendors fully understand the scope.

State agencies may transfer a SAM using two scenarios:

1. A State agency may choose to transfer the code “as-is” and join the SAM Users Group, submitting its desired changes after implementation using the group’s change control process
2. A State agency may transfer the code and make the desired changes as a “stand-alone” system, without the benefits of Users Group membership

These two options represent different scopes of work for the contractor. The State’s expectations must be made clear in the SOW, within the RFP, to ensure accurate pricing in the proposals.

When a State agency is transferring a SAM system and joining the User Group, details must be included in the RFP to define requirements for a contractor to only perform transfer and implementation (T&I), and perhaps maintenance and operations. (See **section 4.8.5.4**, page 220, for description of T&I contractors.) Enhancements to the SAM are generated through the User Group Change Management process and will only be performed by the SAM maintenance and enhancement contractor. Details should indicate that code modifications will not be a requirement of the contract. Enhancements will only be made to the core code of the SAM system by the SAM maintenance and enhancement contractor. In addition, any details relating to the specific User Group the State agency is joining should be included in the procurement as an indication to the bidders of the environment the T&I contract will support.

4.6.2.2 WIC Exception – (non-SAM)



Another exception to specifying State systems by name for transfer would be for those WIC State agencies seeking to transfer an existing functioning MIS/EBT system. State agencies may follow the traditional path of providing their list of Functional and Technical Requirements to the vendor community to bid the best fit solution. WIC State agencies may also conduct an in depth Feasibility Study with Alternatives Analysis to determine the best transfer solution during the planning phase.

State agencies may request the transfer of a specific existing WIC MIS/EBT system if they have completed a thorough Feasibility Study and Alternatives Analysis of available options. The results of the Feasibility Study are provided in the IAPD submission to FNS and must be approved prior to pursuing the procurement of a Transfer and Implementation or System Integrator. In this scenario, the inclusion of the selected transfer system GSD or system specification as part of the RFP is appropriate.



Enhancements or changes to the transfer MIS/EBT are identified by the State agency and included in the RFP. The extent of these changes and enhancements are based upon decisions made by the transferring State agency and constrained by the availability of federal funds.

4.6.3 EBT Conversion or Transition Planning

When transitioning to a new Electronic Benefits Transfer (EBT) support contractor, a smooth handover requires a reasonable transition period to the non-incumbent. The more complex the system, the longer the transition period needs to be to ensure success. The State agency needs to do its own planning for the conversion and transition from the previous provider to the new provider. This includes developing a transition schedule to be included in the RFP as a requirement.

A transition plan in the RFP should address at minimum the following items:

- Project initiation with the new contractor
- Project planning and management
- System documentation
- Contractor system testing
- Transfer initiation
- Transfer User Acceptance Testing
- System conversion and cycles (mock/dry/trial runs)

The RFP should include full details about the current EBT system and the eligibility or certification system with which it interfaces. This is essential for bidders to recognize and plan for all aspects of system integration and all system interfaces.

The State agency should include the following plans in the RFP:

1. A detailed conversion plan (for changing processing platforms and converting the database files)
2. A transition plan (for moving equipment, people, data, processes, operations, and so forth)

This ensures that every associated activity needed for the transition from the State's current EBT system to the new one will have minimal disruption in the event a new vendor is selected. The plan should include these items:

1. Description of the overall approach
2. Order in which the activities will occur
3. Tasks to be performed
4. Parties responsible for performing each task
5. A back-up plan should any or all of the activities be delayed
6. A preliminary project schedule including milestones and overall timeline

The State agency should specify the requirements for transition from one EBT processor to another, such as:

- Creation or migration of client, retailer, and provider databases, including account aging information, expungement dates, transaction history, recipient card and demographic data, and benefit data
- Creation or migration of transaction acquirer and retailer files
- Client notification of database conversion outage (at State's discretion, if applicable)
- Retailer notification of database conversion outage (if applicable)
- Selection of an appropriate date and time frame for database conversion, including an appropriate backup date
- EBT-only retailer transitions (including getting retailer contracts signed)
- POS device deployment and installation at retailer locations (if applicable)
- Personal identification number (PIN) pad installation
- EBT card replacement and reissuance if the State opts to change its cards
- State, client, and retailer training
- Testing procedures, verification, and validation of the migration process
- Deployment of card activation devices (if applicable)
- Customer service/help desks
- Quality Assurance (QA) checkpoints and critical paths

4.6.4 SNAP EBT Conversion or Transition Planning



For SNAP EBT, all the guidelines in the previous section apply. However, the State agency should specify additional requirements for transition from one EBT processor to another, such as requiring that processor data for Anti-Fraud Locator using Electronic Benefits Transfer Retailer Transactions (ALERT) be created for the conversion month. State agencies may also require that the vendor provide two separate files of individual transaction data for ALERT to FNS - one from the incumbent processor for transactions occurring before the conversion date and one from the new processor for transactions occurring after the conversion date - for the conversion month. Alternatively, the State agency may require the new processor to provide the ALERT data for the entire conversion month. FNS recommends securing data from the incumbent and from the new processor.



Preparing and submitting the RFP begins the FNS approval process in SNAP EBT. Procuring SNAP EBT services does not require the approval of an IAPD before the RFP is issued if no significant development efforts are involved. State agencies generally procure a “turnkey” EBT delivery method. An EBT contractor provides or subcontracts for host processing, retailer management, and call center services, usually under a single contract. The IAPD is submitted after contract award and before implementation. However, an IAPD may be required in advance of procurement should significant development be necessary or if a change in technology is proposed. The State agency should contact the RO or SSO to determine whether an IAPD is required prior to procurement planning.



Refer to the SNAP [EBT System Transition Guide](#) for further details.

See **Table 19** (also available in the SNAP [EBT System Transition Guide](#)²¹) to help plan the schedule for preparing and submitting the required documentation to FNS, and to plan other key activities before an EBT conversion or transition.

Table 19: Sample SNAP EBT Time Frame

Item	Time before database conversion	Comments
RFP Submitted to FNS	-30 months	
SNAP EBT waivers	-25 months	FNS approves, need waivers for RFP
RFP Approved by FNS	-24 months	FNS approves
Contract submitted to FNS	-12 months	
FNS Approves Contract	-10 months	
IAPD to FNS	-12 months	FNS approval of the IAPD is required before costs are incurred; otherwise may be disallowed
Transition Team	-9 months	
Detailed Transition Plan	-8 months	FNS approves
Retailer Association Contacts	-7 months	



Table 19: Sample SNAP EBT Time Frame

Item	Time before database conversion	Comments
Layouts, Data Elements, etc.	-6 months	
Telecom Hardware	-6 months	
Retailer Implementation Plan	-6 months	
Notification to TPP Contacts	-5 months	
Federal Acceptance Test Plan	-4 to -2 months	Requires FNS approval when converting to a new processor
Acceptance Test Scripts	-4 to -1 months	Requires FNS approval when converting to a new processor
Links for Trial Runs	-4 months	
Data Clean-Up	-4 months	
AT User Clean-Up	-4 months	
EBT-Only Retailer Agreement	-4 months	FNS approves
CS Phone Number Transfers	-3 months	
PIN Encryption Key Transfer	-3 months	
Retailer Notice of Outage #1	-3 months	FNS will do mailing
EBT-Only POS Replacements	-3 months	Obtain reduction in billing from incumbent if possible
Trial Run #1	-3 months	
AMA/ASAP Profile	-3 months	FNS initiates by sending profile form to the State
Voucher Decision for Outage	-3 months	
State Functional Demonstration	-3 months	
FNS Pseudo-Retailer Numbers	-2 months	FNS sends via email
Trial Run #2	-2 months	
User Acceptance Test	-2 months	FNS concurrence required for a 'GO' decision
Customer Service Messages for Outage	-2 months	

**Table 19: Sample SNAP EBT Time Frame**

Item	Time before database conversion	Comments
EBT-Only, TPP, ATM Access Evaluations	-2 months	SNAP requires 85% coverage with no sizable geographical gaps
Trial Run #3	-1 months	
Retailer Notice of Outage #2	-2 weeks	FNS will mail
Stop State Input	-1 day	
Incumbent Cut-Offs: Vouchers (settle what is at old processor) Adjustments Automatic card mailing AT profile changes Expungement sweeps POS maintenance	-1 day	
Cut-Off Incumbent Processing	0	
Database Conversion	0	
Validation/Reconciliation	Day 1	Advise FNS
Former Processor ALERT and STARS Data for their portion of last month	+1 day	
Last Monthly reports from Former Processor	+1 day	
Former Processor Last ACH	+2 days	
New Processor 1 st ACH	+2 days	
Obtain any missing Data from former processor	+2 days	

4.7 RFP and Contract Planning

While the purpose of the procurement is obtaining goods, services, or both for an IS system, there are many other elements to be planned aside from technical and functional needs. Selecting a contractor and managing the resulting contract relationship must be part of the RFP and resulting contract. This section describes many of the



main RFP and contract planning activities the State agency must perform in addition to the technical planning elements described above.

4.7.1 Preparing Criteria for Evaluating Proposals

All government agencies generally seek to award contracts on the basis of the best overall value. This means that the State agency should consider and plan for all relevant factors for deciding which proposal response best suits its needs. Preparing an RFP consists of selecting appropriate clauses and provisions, tailoring them when necessary, and finally assembling the various parts of the RFP for issuance. The RFP should clearly state the significant evaluation factors. These factors include cost or price, cost or price-related factors, past performance, and other non-cost or non-price-related factors that will be considered in making the source selection. Each factor should have its relative weight or importance documented as well. These are in addition to functional requirements and technical specifications. As part of this preparation, it is important that the State agency plan a general source selection strategy. The State agency needs to decide how it will make potential tradeoffs between cost and non-cost factors, rather than just buying from the lowest cost, technically acceptable offeror.

Most proposals include three main categories of evaluation criteria: technical evaluations, cost evaluation, and past performance evaluation. It is the State agency's decision how to rank these and weight them for evaluating proposals. A State agency may add other criteria categories. However, the number of categories should be only those the State agency deems essential so that the scoring is not diluted by having too many evaluation criteria. Regardless of whether there are three, four, or more criteria category, the order of precedence and weight for each must be planned and documented in the RFP.

Evaluation criteria should be individually tailored to each RFP. For criteria to be effective, they should have the following characteristics:

- Clear: not subject to multiple interpretations, not ambiguous
- Relative: all key elements of the project requirements must relate to the requirement definition and be covered by evaluation criteria
- Discriminating: separate best, average, and weaker proposals
- Non-discriminatory: fair and reasonable
- Realistic: given the nature or value of the contract
- Measurable: must have distinguishing importance
- Economical: use of the criteria should not consume an unreasonable amount of time or resources
- Justifiable: make sense and can be justified on common sense, technical, and legal basis; mandatory and heavily weighted criteria must be justified



4.7.1.1 Technical Evaluation Criteria

The term “technical evaluation,” as used below and throughout the document, refers to non-cost factors other than previous program experience. Often, this is the first and most important category for evaluating proposals. The purpose of technical factors is to assess the offeror’s proposed approach, as detailed in their proposal, to satisfy the State agency’s requirements. There are many aspects which may affect an offeror’s ability to meet the RFP requirements. Examples include compliance with RFP requirements, technical excellence, management capability, personnel qualifications, staffing availability, and facilities.

The evaluation criteria are based on the contents of the PWS, schedule, specific deliverables, functional requirements document, and services needed. Services might include design, development, installation, testing, implementation, training, maintenance, and technical support.

The evaluation of risk is related to the technical assessment. Evaluating technical risk assesses the degree to which the offeror’s proposed technical approach for the requirements of the RFP may cause disruption of schedule, increased costs, degradation of performance, the need for increased Government oversight, or the likelihood of unsuccessful contract performance.

Other relevant factors for evaluating proposals the State agency should plan for include the following:

- Response format as required by the RFP
- Adequacy and completeness of proposal
- Offeror’s understanding of project/statement of understanding (Offeror demonstrates understanding of the purpose and goals of the project.)
- Project experience in providing similar services (Offerors may be required to provide samples of past work experience and qualifications relevant to the RFP.)
- Project personnel (Offerors should submit resumes of the staff that will participate in the project.)
- Project management plan and methodology to accomplish tasks
- Proposed system documentation
- Technical skills (Offerors should map staff skills to the functional areas identified in the RFP.)

4.7.1.2 Proposed Cost Considerations

As part of planning proposal evaluation, the State agency must determine how it will weigh each bidder’s proposed cost in relation to other evaluation criteria. This includes paying attention not just to the actual project costs, but also to the costs of ongoing operations of the proposed system compared with the State’s current technical operations costs. For example, can the State afford the M&O costs on the proposed system once the development and implementation contractor and any special FNS funding for it are gone? Efficient and careful use of funds is crucial in managing FNS programs. State agencies should not base their decision solely on cost. To

ensure the best product and long-term value for the project, it is important that the State agency not weight the cost proposal too highly and choose the lowest bidder, regardless of other factors.

Other relevant factors for evaluating proposals that the State agency should plan for include the following:

- Other factors (e.g., current relationship with the contractor, incremental funding payment points, and Subject to Availability of Funds orders)
- Company stability (e.g., cancelled contract history, financial stability).

FNS recommends the cost proposal be weighted as 20% to 40% of the total proposal to provide a balanced evaluation between the technical and cost factors. States should test their formula before use to ensure that they are comfortable with the results.

Scenarios to be tested include the following relationships:

- High technical score, low cost score
- Low technical score, low cost score
- High technical score, high cost score
- Low technical score, high cost score

Too little weight on the cost may result in a strong technical proposal's winning, no matter how high the cost. Too much weight on the cost may result in a low bid's winning, no matter how poor the technical proposal.

The contracting officer is encouraged to research available sources to determine what the fair and reasonable price range should be for the products or services sought before requesting cost or pricing data from the contractor. Normally, competition establishes price reasonableness.



Contracting officers should not require unnecessary details in submitting cost or pricing data. Excessively detailed cost or pricing data may lead to increased proposal preparation costs. This also generally extends procurement lead-time and consumes additional contractor and State Agency resources.

4.7.1.3 Previous Program Experience

There are two aspects to the previous program experience evaluation. The first is to evaluate the offeror's previous program experience to determine how relevant a recent effort accomplished by the offeror is to the effort being procured. The criteria to establish what is recent and relevant should be unique to each procurement

and should be stated in the RFP. In establishing what is relevant for the procurement, give consideration to those aspects of an offeror's contract history that would give the greatest ability to measure whether the offeror will satisfy the current procurement. Common aspects of relevancy include similarity of service/support, complexity, dollar value, and contract type. The second aspect of the previous program experience evaluation is to determine how well the contractor performed on the contracts. Rather, the previous program experience evaluation process gathers information from customers on how well the offeror performed those past contracts. Relevant performance factors for past contract performance would include timeliness, quality, cost control, etc. References are helpful in evaluating these factors. References (Offerors should provide valid references and points of contact from other similar projects, including telephone numbers and mailing addresses.)

States should not put previous program experience in their selection criteria as a pass/fail element. Instead, an RFP may require and assign evaluation points for relevant experience. More points might be awarded for experience in large-scale eligibility or benefit management programs and for program-specific experience. Therefore, the selection criteria should not contain language such as "must have WIC experience," or "must have 5 years' experience processing public sector EBT transactions." Instead, points should be assigned on the basis of experience. States should assess the quality of the experience as well as the existence of the experience.

Another important aspect of evaluating a contractor's ability to perform the work is management approach and staffing available for the contract. These are more properly addressed in the "technical approach," or a specific criteria category for management approach and staffing. State agencies should evaluate experience on the basis of the team proposed, not just the company itself. A company as a whole may have years of experience, but if stretched thin over many projects, may assign an inexperienced team to a new project. Similarly, a new start-up company may hire experienced people away from competitors, but would not qualify if the RFP says the company itself must have a specified number of years of experience. The proposed contractor staff and their availability should be considered, not just the experience of the corporate entity as a whole.



All of the decisions resulting from planning for evaluation of proposals should become part of the RFP. They would be included in the section "Evaluation Factors for Award."

4.7.2 Terms and Conditions

States should plan to use contract terms to ensure that systems developed for federal programs are procured in the most cost-effective way. A key consideration is meeting the federal requirement for maximum practical full and open competition. States should be aware that excessive terms and conditions may limit competition. Examples include large performance bonds, unlimited liability, and large holdbacks on payments.



States undertaking IS development projects should balance these concerns with State requirements and vendor performance remedies when contemplating the inclusion of the following issues in their contracts:

- **Prescribed Payment Terms**—Payments or holdbacks are prorated according to the relative value of, and tied to acceptance of, deliverables. In many cases, this includes a final payment that is a substantial percentage of the total contract value (e.g., 20 percent). This amount is not paid until the system is accepted or certified. The preferred method of ensuring contractor performance is through prescribed payment terms, such as incremental payment points based on the schedule by deliverable and/or phase. Payment terms may be used in conjunction with liquidated damages clauses to ensure that all contract obligations, including timeliness and quality of deliverables, are met by the vendor.
- **Liquidated Damages**—Fixed amounts are assessed to contractors for compensation of damages, which may be difficult or impossible to determine precisely, as a result of contractor nonperformance. Provision for liquidated damages, in combination with prescribed payment terms, provides the level of security needed to ensure vendor performance.
- **Performance Bonds**—Bonds, from which costs for noncompliance can be assessed, are secured usually through financial or insurance firms. Performance bonds, in particular, are costly because a contractor must make a direct outlay of funds to acquire the bond and the systems initiatives being bonded are costly, which affects the cost of the bond. This increases the bid price and the cost of the project and may deter potential bidders from doing business with the State agency, ultimately inhibiting competition.

In cases in which State agencies have had problems or failures in systems projects, performance bonds would not have provided the compensation States seek. In these cases, performance problems most often stem from a lack of specificity in the SOW section of the RFP and other matters, including project management. The State agency is responsible for defining in the RFP performance expectations, prescribed remedies, and penalties that protect the State in the event of a failure in performance by the vendors. These should also become part of the contract. Most contractors are willing and expect to abide by a combination of holdbacks (i.e., payment percentage terms), liquidated damages, and software escrow^{***}. When the project is effectively managed, performance issues are kept to a minimum.

^{***} Software escrow is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.



While vendors must be held accountable for their performance, using one or a combination of the methods described above involves costs for contractors that are passed on to Federal and State agencies. State agencies should choose a combination of performance terms that are appropriate to the scope and value of the contract, applicable to the performance factors, appropriate to the risk, and enforceable.

4.7.3 Incentives and Remedies

Incentives are intended to motivate for high-performance and quality work. Incentives can be monetary, non-monetary, positive, negative, or some combination of these. They can be based on cost, schedule, or quality of performance. Incentives are often based on the buyer and the seller sharing risks for cost overruns or sharing the benefits of cost savings. The sharing formula is a negotiated formula (e.g., 60% contractor to 40% customer) between the contracting officer and the contractor. In firm fixed-price contracts with incentives, there is often a ceiling for the incentives, thus a limit to the total contract cost, as would be expected for a firm fixed-price contract. Regardless of the final composition and structure of the incentives, the goal is to encourage and motivate the best-quality performance. It is recommended that incentives be used when they will promote better quality contractor performance. They should apply to the most important aspects of the work instead of being applied to every task. Incentives should correlate with results. They are best used for high-dollar efforts or projects with a history of problems with performance or cost overruns. To achieve the greatest effect, incentives should be applied selectively to motivate contractor efforts that might not otherwise be emphasized and to discourage inefficiency. Definitions of the maximum positive and negative incentives should be clearly spelled out in the RFP. The Quality Assurance Surveillance Plan (QASP) (see section **4.7.4**) is one part of the RFP and contract used in conjunction with incentives and remedies. The QASP provides an objective means to administer incentives and remedies.

Below are useful guidelines on incentives:

- Avoid rewarding contractors for simply meeting minimum standards of contract performance
- Use incentives to create a proper balance among cost, performance, and schedule factors
- Use incentive amounts that correspond to the difficulty of the task required but do not exceed the value of the benefits the State agency receives
- Verify the effectiveness of incentives to ensure that they accomplish their intended purpose (e.g., encourage good performance and discourage unsatisfactory performance)

Remedies are used in contracts to specify procedures or reductions in price (or fee) when services are not performed or do not meet contract requirements. In a firm fixed-price contract with incentives, the negative incentive of having to take a reduced price is one remedy that does not have to wait for a failure to perform that results in a breach of contract. If the contractor fails to deliver, this may be a case of a breach of contract that may be remedied by means other than a lawsuit. Other remedies for breach of contract include award of damages, specific performance, rescission, and restitution. As part of the process for implementing remedies, the State agency must give the contractor the opportunity to correct non-conformance service at no increase in contract price. In addition, the State agency can choose to allow the contractor to re-perform the service at no additional cost to the State agency. Acceptance procedures should be clearly identified by the State agency to ensure that the contractor adequately meets requirements. The purpose of remedies is to ensure that the State agency does not pay for services that do not meet identified requirements and performance standards.

4.7.4 Quality Assurance Surveillance Plan (QASP)

The Quality Assurance Surveillance Plan is the key State agency-developed surveillance (i.e., observation and monitoring) process document. The State agency must plan for how it intends to perform quality assurance surveillance and document it in the QASP. The QASP is used to manage contractor performance assessment by ensuring that systematic quality assurance methods are utilized to validate the contractor's quality control (QC) efforts. The contractor's quality control efforts should be timely and effective and ensure delivery of the results specified in the contract. The QASP directly corresponds to the performance objectives and standards (i.e., quality, quantity, timeliness) specified in the PWS. The QASP details how, when, and by whom the State agency will survey, observe, test, sample, evaluate, and document contractor performance results to determine whether the contractor has met the required standards for each objective in the PWS. The QASP is intended to be a "living" document and is reviewed as performance warrants. Consequently, the method and degree of performance assessment may change over time depending on the level of confidence in the contractor.²² The QASP should be part of the RFP and is usually referenced in the PWS. However, in most cases, it is a separate attachment or exhibit to the RFP and contract due to its size.



The QASP is not required by FNS for RFPs and contracts. However, it is recommended as a best practice because of its importance for producing a successful project outcome.

The QASP should be prepared in conjunction with the preparation of the PWS. The QASP should specify all work requiring surveillance and the method of surveillance. It should designate the place or places where the State agency reserves the right to perform quality assurance.²³ Performance incentives, both positive and negative,



based on QASP measurements should be included in this plan. The RFP and contract should reference the QASP when defining procedures for the reduction of fee or price when services are not performed or do not meet contract requirements and rework is not feasible.

4.7.5 Required Federal Assurances

There are several required assurances the State agency must include in the contract for work funded by FNS and other cognizant federal agencies. These assurances must be part of the RFP to ensure that potential contractors understand the agreement they are entering into before they commit resources to developing a response. **Table 20** provides a summary of the major RFP and contract provisions the State agency must include.

Table 20: Basic Contract Provisions and Federal Assurances

Provision Type	Examples	
Standard Contract Provisions	• Governing laws of the State, county, and/or federal entity under whose purview the contract will be governed • Agreement duration of the start and end periods of the contract and possible extensions • Document incorporation and order of precedence (i.e., controlling order) • Scope of contract • Contract amendment provisions • Subcontracting provisions • Interpretation and disputes • Contractor hold-harmless clause • Force majeure • Record retention • Reporting requirements • Confidentiality provisions • Affirmative Action provisions	• Key personnel provision • Termination provisions • System acceptance criteria • System warranty provisions • Maintenance provisions • Payment provisions • Charges to be reported by contractors to the State agency • Liquidated damages • Notice provisions (i.e., notice to cure, notice of intent, notice to terminate) • QA provision • Risk of loss or damage provision • Specifications (SOW or PWS) • Training provisions • Out-of-scope services • Contractor bond provisions • Limitation of liability clause • Access to facilities and records



Table 20: Basic Contract Provisions and Federal Assurances

Provision Type	Examples	
Ownership, Licensing and Intellectual Property Rights	• Tangible property provisions (e.g., equipment purchased with the contract) (7 CFR 277.18(l)(2)) • Intangible property provisions (7 CFR 277.18(l)) ○ Federal Ownership License (7 CFR 277.18(l)(1)(ii)) ○ Copyright licensing (7 CFR 277.18(l)(iii)) ○ State agency ownership of intellectual property (7 CFR 277.18(l)(1)(i)) ○ Indemnification provisions of patents and copyrights • Jointly developed materials provisions	
FNS-Required Provisions (based on 2 CFR 200 Appendix II Contract Provisions for Non-Federal Entity Contracts Under Federal Awards)	• Compliance with Executive Order 11246 related to Equal Employment Opportunity • Compliance with Clean Air Act (42 U.S.C. 7401-7671q.) • Compliance with Clean Water Act (33 U.S.C. 1251-1387) • Compliance with Anti-Lobbying Act • Compliance with Americans with Disabilities Act • Compliance with Drug-Free Workplace requirements • Compliance with Suspension/Debarment requirements • FNS has royalty-free rights to use software and documentation developed	
General Provisions	• Procurement Standards (7 CFR 277.14; 7 CFR 277.18(c)(ii)); and (7 CFR 277.18(c)(iii))	
Commonly Found Provisions	• Executory clause • Non-assignment clause • Comptroller's approval • Workers' compensation benefits • Wage and hours provisions • International boycott prohibition • Conflict of interest	• Fair practices • Antitrust • Publicity • Reduction of Federal or State funding • Penalty clause • Off-set rights • Insurance provisions



Additional information regarding each of these provisions is provided in appendix **A11 Federal Procurement Clauses**.

4.7.6 Travel and Per Diem in Fixed Price Contracts

Per Diem is the allowance for lodging (excluding taxes), meals, and incidental expenses for temporary duty travel. Travel policy and per diem for contractors normally follow the specific State's travel regulations for its employees. FNS recommends, and many State agencies adhere to, GSA limits on travel costs.

State agencies should define a methodology that allows travel and per diem associated with all aspects of a project, including individual tasks, to be readily identifiable within the proposal's budget. Many times these costs are embedded in the bid as a portion of the price to complete the individual task and cannot be easily separated. FNS strongly recommends that all travel and per diem be identified as a separate budget line item, with the number of events, staff, and associated costs clearly identified. Likewise, the States need to have controls in place to ensure that meetings and events that occur sequentially at a location are not over-billed. These events may have been bid as separate occurrences, but in reality occur over a period of time at one location, thus incurring less cost for air fare and transportation than originally budgeted. Once source selection is completed, the contract should include the same provisions, as well as the selected contractor's proposed costs converted to an invoicing or billing schedule.

States should only be billed for actual costs incurred. This situation also applies to strict accounting of time sheets for hours worked, such that there should not be a 24-hour hourly rate charge when in travel status. Often, the requirements of a task change and affect the amount of travel and per diem. For example, a change in the schedule may delay a travel event such that the contractor has very little time to make travel arrangements. Consequently, the costs for airfare increases the closer to the travel date the reservations are made. These types of costs resulting from changes in the schedule should be reimbursed to the contractor.

4.7.7 FNS Procurement Standards for State Agencies

4.7.7.1 Code of Conduct

The State agency should maintain a written code of conduct that governs the performance of its officers, employees, or agents engaged in contract awards and administration funded in whole or in part by FNS program funds.²⁴



4.7.7.2 Contracting with Small and Minority Firms, Women's Business Enterprises, and Labor Surplus Firms

State agencies should be aware of the federal regulations for how contracting applies to small and minority business firms, women's business enterprises, and labor surplus area firms. State agencies must take affirmative steps to ensure that such businesses are used, when possible, as sources of supplies, equipment, and services.²⁵

4.7.7.3 Full and Open Competition

All State agency procurements must be conducted in a manner that provides for maximum full and open competition.²⁶ In this regard, States should have written selection procedures that do not unduly restrict or eliminate competition. Solicitation of offers, whether by competitive sealed bid or competitive negotiation, must accurately describe the technical requirements for the material products or services desired. These descriptions should not, in competitive procurements, contain features that unduly restrict competition. Descriptions may state the qualitative nature of the product or service desired and set forth those minimum essential characteristics and standards to which the product or service must conform. A brand name, or equal description, may be used to define the performance or requirements desired, if it is impractical or uneconomical to describe clearly and accurately the technical requirements.

4.7.7.4 Geographic Preference Prohibition

Office of Management and Budget (OMB) policy ([2 CFR 200.319](#)) prohibits grantees and sub-grantees from conducting procurements that impose geographical preferences. Geographical preferences are anything that uses statutorily or administratively imposed in-State or local geographical preferences in the evaluation of bids or proposals. The only exception is those cases in which applicable federal statutes expressly mandate or encourage geographic preferences. Nothing in this section preempts State licensing laws. Therefore, a State can require that a vendor be licensed in the State.²⁷

4.7.7.5 State Agency Procurement Records and Information Systems

The State agency must make procurement records available to FNS and provide access to all aspects of the IS project. This includes design, development, operation, and work performed by any source, including cost records of contractors and subcontractors.²⁸



Failure to provide this access to procurement records and information systems will result in suspension or termination of FFP for the costs of the system and its operation.

4.7.7.6 Ownership and Licensing

There are several policy requirements that State or local governments must include in all RFPs and contracts for any software or software modifications and associated documentation that is designed, developed, or installed with FFP. These include ownership rights and a broad federal License, among others, as provided in [7 CFR 277.18\(l\)](#).²⁹



See appendix **A16 Ownership Rights** for examples of contract language that has been used to achieve FFP eligibility requirements and proper ownership rights.

4.7.7.7 Intellectual Property Rights & Transferability

The RFP, Statement of Work (SOW), and all State contracts should include the technical language and applicable contract clauses regarding intellectual property (IP) rights for IT and IS procured using FFP. This language should also promote system transferability. There are several policy requirements that State or local governments must include in all contracts. Software, software modifications, and associated documentation designed, developed, or installed with FFP must meet these requirements. Proprietary vendor software packages and operating systems (OS) that are provided at established catalog or market prices and sold or leased to the public are not subject to these licensing and ownership provisions.

In State contracts, the responsibility and discretion to negotiate the State's minimum needs is significant. Many States may have default clauses for IP rights and rights in technical data. In the absence of State specific procurement clauses for such contracts, the parties must negotiate all that is addressed in the standard IP contract clauses. The potential rights and issues are so involved that the risks of not obtaining the necessary rights increase if you try to negotiate. State agencies should use some model as a guide that has been rigorously tested. An alternative to writing IP clauses from scratch if these clauses do not exist, rather than negotiate the rights, is for the State agency to use detailed clauses from other existing policy or regulations. In other words, "Don't make it up as you go." One such model is the FAR³⁰. States are not required or obligated to use FAR references in their RFPs and contracts. Nonetheless, the FAR clauses would be a valuable reference to use as a model for State RFP and contract IP clauses, especially given the federal awarding agencies' involvement and the use of FFP.



4.7.8 FNS Specific Procurement Requirements

FNS may stipulate certain deliverables for submission and review. To support FNS requests, the State agency needs to plan the procurement documents accordingly. The RFP and the resulting contract should stipulate that payment will occur following review and acceptance of each major deliverable by the State agency. Major deliverables may include the detailed system design, as well as system and functional requirements documents. The State agency is responsible to have performance expectations, prescribed conditions, and remedies in place that protect it in the event of a failure in performance by contracted vendors. Examples include holdbacks, regular monitoring of performance, or liquidated damages. Procurements and subsequent undertakings that fail to meet approved APD requirements may be subject to disallowance in accordance with [7 CFR 277.18 \(h\)](#).³¹

4.7.9 Order of Precedence

FNS strongly recommends, and most States' contract language specifies, that the various documents in the procurement process be ranked in order of precedence. This ensures that all parties understand which document prevails in the event of a disagreement or disparity. The State agency must determine an Order of Precedence or use Governing Documents to facilitate dispute resolution. For example, the State's own language in the RFP should outrank the contractor's language in the proposal, if the two should differ. This order of precedence should then be consulted in the investigation and resolution of a dispute. Likewise, the contract takes precedence over the RFP or the contractor's proposal. It is usually labeled "Order of Precedence" or "Governing Documents" in the RFP and the contract.

The order of precedence of the contract documents is as follows:

1. Contract
2. RFP Addendum(s) (in descending numerical order)
3. RFP
4. Best and Final Offer Documents (BAFO) (BAFO Form, Negotiation Items, Pricing Tables, Payment Terms, Functional Response Spreadsheet, Proposed Work Plan)
5. Bid dated mm-dd-yyyy

Figure 39: EXAMPLE Order of Precedence



4.7.10 Disputes

Ideally, the relationship between the State agency and the contractor will be one of collaboration and teamwork to accomplish the goals of the project. However, the State agency must plan for the possibility of disputes with the contractor. This includes deciding on steps for addressing breaches of contract and dispute resolution, including how these processes will be initiated. Additionally, the office with oversight over disputes and the procedural time limits must be determined. Once the State agency has planned this, the RFP and contract must contain appropriate documentation and requirements for resolving disputes.

4.7.10.1 Alternative Dispute Resolution

The Alternative Dispute Resolution (ADR) is an essential contract tool. It includes any procedure or combination of procedures voluntarily used to resolve issues in controversy without the need to resort to costly and time-consuming litigation. There should be multiple levels and opportunities to settle disputes before the State agency or contractor must turn to legal remedies. Failure to include such options may force the parties into costly litigation over relatively simple matters.

The following list of methods is intended to suggest options that have worked in the past. These methods are designed to supplement, but not to replace, existing extrajudicial approaches to dispute resolution:

- **Partnering**—An agreement between the parties describes how they will work together to keep issues from becoming adversarial.
- **Fact-Finding**—An impartial third party examines the issues and submits a report with a recommended settlement.
- **Mediation**—A neutral third party serves as an advisor to determine mutual interests and defines best and worst alternatives to a negotiated agreement. Mediation may also be called conciliation.
- **Mini-trials**—Each party makes presentations to a panel composed of senior executives from each side and also a neutral party. The panel attempts to work out an equitable agreement.
- **Arbitration**—A neutral third-party serves as decision maker to examine issues and render a binding opinion.

Any method that results in settlement or partial settlement of a contract dispute is a good method. The parties may select any ADR method for any claim of more than \$100,000. For claims of \$100,000 or less, an Appellant may elect consideration under the Accelerated Procedure, U.S. Civil Board of Contract Appeals Rule 5332, without agreement by the State agency. Guidelines, schedules, and requirements for implementing the ADR method selected will be by agreement of the parties and the settlement judge or neutral advisor. ADR can be used successfully at any stage of an appeal, although election should be as early as possible. Proceedings generally will be conducted within 120 days of approval.

These ADR methods are intended to shorten and simplify the ADR Board’s more formalized procedures. Parties who in good faith attempt to resolve their differences by agreement will save both time and money and be able to maintain or restore amicable relations. This tool acknowledges that unforeseen problems may occur and that no contract is perfect, allowing the State agency and contractor to engage in a collaborative process to remove obstacles and enable joint mission success.

4.7.11 Debarment and Suspensions

Debarment and suspension actions preclude companies and individuals from participating in Government contracts or subcontracts. Suspension or debarment by one federal agency is Government-wide and prohibits a company from doing business with other agencies. Suspended or debarred companies are available on the Excluded Parties List System (EPLS), an electronic web-based system. The EPLS is a part of the System for Awards Management. The EPLS identifies those parties excluded from receiving federal contracts, certain subcontracts, and certain types of federal financial and non-financial assistance and benefits. The EPLS keeps its user community aware of administrative and statutory exclusions across the entire Government and individuals barred from entering the United States. State RFPs should contain a requirement that the offeror attest it has not been debarred or suspended and will notify the State agency immediately if its status changes.



Check the suspension and debarment list “Excluded Parties List System (EPLS)” on the System for Award Management (SAM) website. (<https://www.sam.gov/>)



See appendix **A11 Federal Procurement Clauses** for specific Suspension and Debarment clauses.

4.8 Procurement Methods

Procurement planning includes deciding on the type of procurement that best suits the State agency’s needs. All of the foregoing planning activities will impact selecting the procurement method. Likewise, the selected procurement method may require returning to the procurement planning activities described above to make sure there are no disparities. This may be an iterative and somewhat repetitive process to ensure alignment of activities and methodology as well as schedule requirements. The procurement method will affect the structure of the RFP and contract, the acquisition strategy, and post-award activities. There are three common types of procurements used for procuring IS goods and services. These are competitive procurements, non-competitive procurements, and cooperative purchasing.



4.8.1 Competitive Procurements

For major procurements, competitive sealed bids and competitive negotiation are primarily used. Both require an RFP. The nature of the IS procurement often requires the competitive negotiation process, such as in circumstances involving development of software applications.

State agency procurements using FNS program funds must be made by one of the following methods:

- **Small Purchase Procedures** for services or supplies costing in aggregate not more than \$150,000
- **Competitive Sealed Bids** using formal advertising resulting in the award of a firm fixed-price contract to the bidder whose bid, conforming with the terms and conditions of the RFP, is lowest or the best value
- **Competitive Negotiation** in which the RFP is publicized, requesting proposals from several sources, and resulting in the award of either a fixed-price or cost-reimbursement type of contract
- **Cooperative Purchasing Agreements** for competitively procured State master lists for goods and services (see section **4.8.3 Cooperative Purchasing**, page **212**)

Contracts are generally grouped into two broad categories: fixed-price contracts (including firm fixed-price contracts) and cost-reimbursement contracts. Circumstances rarely arise when FNS would support use of a cost-reimbursement contract for a system project. Therefore, HB901 focuses on fixed-price RFPs and contracts.

4.8.1.1 Firm Fixed-Price Contracts

Although there are several types of fixed-price contracts, the federal government, including USDA, advocates the use of firm fixed-price contracts to acquire goods and services when feasible. Firm fixed-price contracts provide an agreed upon price for services delivered that will not change once the contract is awarded. In other words, the price is not subject to any adjustment based on the contractor's cost experience while performing the contract. This type of contract places maximum risk and full responsibility for all costs on the contractor. The contractor's risk is related to profit or loss to complete the work for the agreed upon price. There is a lower risk for the customer that the contractor may complete the work for less cost than the agreed upon price. The customer cannot recover that money. It is the contractor's profit. Firm fixed-price contracts provide maximum incentives for the contractor to control costs and perform effectively. Generally, firm fixed-price contracts impose a lower administrative burden on the contracting parties. This is because accounting, invoicing, and auditing are greatly simplified compared to cost reimbursement or time and materials contracts.



State agencies need to be careful when writing RFPs and contracts that include administrative requirements requesting the contractor perform “contract” administration. While there is a legitimate need for these, they should not be burdensome or they may add unnecessary costs.

Firm fixed-price contracts are usually implemented when the following conditions exist:

1. There is adequate price competition
2. Realistic estimates of the probable costs for goods/supplies or services may be obtained by comparison of the same or similar prior purchases made on a competitive basis, or supported by valid cost or pricing data
3. Services and quantities are known and unlikely to fluctuate
4. Processes or methods are mature
5. Requirements are stable
6. Cost control is a driving factor

4.8.1.2 Time and Materials Provisions in Contracts

A time and materials (T&M) contract provides for acquiring supplies or services on the basis of labor and materials. A labor-hour contract is a variation of the T&M contract, differing only in that materials are not supplied by the contractor. T&M contracts and labor-hour contracts are not fixed-price contracts.

Specifically, T&M contracts provide:

- Direct labor hours at specified fixed hourly rates that include wages, overhead, general and administrative expenses
- Actual cost for materials

A T&M contract may be used when it is not possible to accurately estimate the extent or duration of the work at the time the contract is established. It may also be used when it is difficult to anticipate costs with any reasonable degree of confidence. This type of contract provides no incentive to the contractor for controlling costs or labor efficiency. Therefore, appropriate State agency surveillance of contractor performance is required to give reasonable assurance that efficient methods and effective cost controls are being used.

During operations and maintenance, there may need to be modifications made to the system. This may happen because of new Federal or State requirements or to make enhancements to improve the system’s efficiency and effectiveness. If the modifications being considered do not change the scope (i.e., materially change the purpose

of the system or involve a major redesign) then it makes sense to have a provision in the M&O contract to allow the M&O vendor to do this work on a T&M basis. Using such a provision reduces the risk inherent in possibly hiring a vendor other than the M&O vendor to do the enhancement work.

For these reasons, FNS recommends this strategy be included in RFPs/contracts by:

1. Requiring labor rates for the category or categories of work being procured
2. Specifying an overall dollar limit (e.g., not to exceed 20 percent of the cost of the base contract)
3. Providing for the negotiation of the cost of task orders upfront based on the labor category and estimated number of hours required

4.8.1.3 Service Agreements

A service agreement can take many different forms, depending upon the type and scope of the service, the service arrangement, and the type of organization. State agencies should execute service agreements when IT or other project-related services are to be provided by their internal IT department or by other State and local agencies. Examples of IT services include telecommunications, network installation and maintenance, hardware installation and maintenance, a common network operations center, and IT security services. Another common use of service agreements would be for non-IT services such as project management, QA or IV&V. Performance expectations and service level thresholds should be included as part of the agreement.



Examples of service agreements include: (1) Master Service Contracts, (2) General Schedules, and (3) Blanket Purchase Agreements FNS prefers that State agencies solicit formal responses from at least three vendors from pre-established lists of contractors, to obtain the best value procurement.

Agreements for services to be provided by a contractor that were procured by another State entity should ensure that the contractor was competitively procured. Service agreements typically contain the following components:

- **Introduction** - Introduces the purpose, participants, and general service description.
- **Service Environment** - Describes the environment in which the organization will perform the service, from physical location, to hardware/software being used and the policy and procedures the service provider will need to follow.
- **Roles and Responsibilities** - Describes the roles and responsibilities of all major participants. The service provider responsibilities need to articulate the:
 - Service tasks



- Documentation of their services
- Reporting their actions
- Support functions, such as
 - When the service will initiate trouble calls
 - Who will handle trouble calls
 - How trouble calls will be handled
- **Service Level** - Identifies the specific scope and quality of covered services, as well as methodology to assess successful task completion. Organizations may choose to define service levels with a ratings range from unacceptable to minimally acceptable to satisfactory level. They may also choose to set varying levels for these ratings based on user groups or project timelines. If levels are set, each service level will need to be documented accordingly.
- **Terms and Adjustments** - Provides the costs (e.g., proposed budget and schedule of charges) and period of performance (PoP) of the service levels. It describes the roles and responsibilities documented in the previous sections. This agreement also needs to include processes for resolving service agreement disputes, remedying noncompliance, and amending the agreement to account for changing requirements.
- **Adherence to Program Regulations** – The State agency must comply with all program requirements, including those related to system performance, timeliness standards, and other technical requirements. This is particularly critical for centralized data processing services. Contracts/memorandum of Understanding or other State agreements between the program office and service provider must have provisions in place to enforce these requirements.
- **Priority of Service** – The agreement must ensure that IT-related changes that affect benefit levels or benefit issuance are given a higher priority than other maintenance services.
- **Equipment Disposition and Property Management Requirements**
 - IT equipment may have un-depreciated value remaining. Any equipment over \$5,000.00 at the time of disposition must be disposed according the federal requirements.
 - Equipment procured with FNS funds must comply with property management standards and must be physically inventoried every two years. If equipment is transferred to a new organization and has been expensed, that equipment cannot be charged to the former agency on a usage basis.
- **Administrative Fee Structure**
 - Costs included in the administrative fee must be allowable under provisions of OMB [2 CFR 200](#), Guidance Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, Subpart E – Cost Principles.
 - The administrative fee must be “reasonable, necessary, allowable and allocable” in accordance with OMB guidance, under [2 CFR 200](#). For example, costs associated with centralization should not be significantly greater than current costs.

- A uniform fee for all agencies could unfairly penalize any federal program that funded a greater proportion of the equipment that is ultimately centralized.
- Specific billing algorithms need to be spelled out in any memo of understanding or other service agreement. Costs which will be billed to the program operated by FNS grantees must be based on written cost measurements.
- Costs to FNS cannot be double charges through direct and indirect payment structures.
- **Staffing Changes** – For employees who were formerly assigned to a program 100% of the time and are now assigned to multiple programs, a method of tracking the time spent on each program must be implemented and costs allocated properly. Program offices should be careful to ensure that this change does not result in a degradation of service.



Although service agreements need not be submitted for prior approval, the State agency must have valid service agreements on file and available for FNS review. In addition, any equipment or software acquired through a service agreement relationship must have FNS prior approval if federally aided public assistance programs may be expected to be billed for more than 50 percent of the total cost. Costs for unapproved procurements or undocumented service agreements may be disallowed by FNS.

Equipment may be acquired through State schedules, assuming that such schedules have been established competitively. It is also recommended that States consider the quantities of hardware or software licenses being acquired related to guaranteed quantities under State schedules. Separate procurements for large quantities may result in significant savings over costs incurred using State schedules. A comparison of costs between the State schedule pricing and market research for a separate procurement may help ensure the State agency obtains the best value.

4.8.2 Non-Competitive Procurements

Non-competitive procurements are not allowable under most circumstances. However, there are cases when this may be the only option for a State agency. This situation often arises as an outcome of market research or initial attempts to complete a competitive procurement.

The most common situation arises during a competitive negotiation that results in one of the following conditions:

- Credible market research demonstrated
 - The lack of multiple available sources to conduct a fair and open competition



- That the item is only available from a single source
- The RFP resulted in too few qualified bidders
- A public emergency is involved

FNS may authorize an exception to competitive procurement (i.e., approval of a sole source or non-competitive procurement). When submitting an exception request, certain key information is required that demonstrates the State agency did its due diligence in promoting free and open competition. State agencies should contact either their SSO or RO contacts for this information. At the discretion of FNS, a State agency may be required to notify FNS regardless of the dollar amount, whenever a non-competitive procurement strategy is chosen.

4.8.3 Cooperative Purchasing

Cooperative purchasing involves two or more government agencies jointly identifying a common need for goods and services, which results in sharing contracts between governments. The term “cooperative purchasing” covers several different sharing arrangements among any number of governmental relationships. Groups that form cooperative purchasing arrangements are known as “purchasing cooperatives.” Several State agencies may work together and cooperate to issue a single RFP to serve joint needs that leads to a shared contract.

Most frequently, government organizations within a single State will enter into these arrangements. States may sponsor cooperative purchasing programs with local governments or participate in cooperative purchasing arrangements with other States. They may also have formalized cooperative purchasing arrangements with the federal government. Purchasing cooperatives leverage their combined purchasing power and benefit from higher volume of purchases from a group of suppliers. They obtain more favorable buying terms than would be achievable on their own. The most common method for developing a cooperative purchase through a formal agreement or contract is by using provisions from the adopted contract and adding or substituting terms and conditions. A combination of all of these methods may be used.

Cooperative purchasing is increasing as States look to procure goods and services in more efficient and cost effective ways.

Resulting benefits may include:

- Lower prices
- Higher quality goods and services
- Improved customer service
- Better maintenance and service agreements
- Stronger contract terms and conditions



FNS recommends that States participate in purchasing cooperatives in one of two ways:

1. Interested States should join purchasing cooperatives before RFPs are issued to ensure bidders are aware of the potential scope of the contracts.
2. States should make purchases or execute contracts based on existing cooperative contracts that offer an open procurement period to any additional buyers at the winning bid or price.

A common method of cooperative purchasing is using the U.S General Services Administration (GSA). An example of a State-led cooperative is the National Association of State Procurement Officials (NASPO) ValuePoint (formerly the Western States Contracting Alliance (WSCA)).

4.8.3.1 U.S. General Services Administration (GSA)

GSA's Cooperative Purchasing Program provides procurement assistance to other government agencies.³³ GSA makes its competitive negotiated schedule prices, product warranties, and other contract terms available to State, local, regional, and tribal governments through the Cooperative Purchasing Program. By allowing non-federal governments to use existing GSA contracts, all levels of government become more efficient by reducing duplication of effort and utilizing volume purchasing techniques.

GSA maintains several purchasing agreements known as "schedules." Each schedule is a compilation of pre-negotiated contracts with vendors and service providers. GSA schedule contracts are designed to streamline the federal procurement process for obtaining commonly used commercial goods and services at low prices associated with volume buying.

GSA Schedule 70 is used for purchasing a variety of IT hardware, software, supplies, support equipment, and professional services. GSA Schedule 70 contains IT special item numbers (SINs). GSA Schedule 84 includes system security.



There is an industrial funding fee (IFF) charged by GSA for using the program. The IFF reimburses GSA for the costs of operating the Federal Supply Schedule program as set forth in 40 U.S.C. 321 - Acquisition Services. For more information, see "GSA - State and Local Government Customers" (<http://www.gsa.gov/portal/category/100631>).

GSA Schedules Seek Best Value

Although volume discounts are built into the GSA Schedule contract, the schedule prices are ceiling prices and may be higher than prices obtained from other procurement processes. GSA has determined that prices under



GSA Schedule contracts are fair and reasonable. When buying services that require a statement of work, consider the proposal for a particular requirement and make a determination as to whether the total price is reasonable and represents the best value.³⁴ An established best practice is to seek additional price reductions and/or increased discounts and/or concessions when placing an order under a GSA Schedule contract. Be aware that the GSA program includes voluntary participation clauses for both the buyer and the contractor. GSA Schedule contractors are not required to offer a price reduction extended only to an individual customer for a specific order to all Schedule users. The GSA program also allows vendors a window to opt-out of honoring a purchase order submitted by the State.

GSA Schedules Integrate Contract Terms and Conditions

Several States have implemented a procedure that integrates GSA IT schedule terms and conditions into their own State-sponsored multiple-award contract schedule programs. This process is known as “piggybacking.” Piggybacking provides the State agency these benefits:

- Contract terms and conditions
- Negotiated State agency prices
- Provisions, such as those that ensure service reliability, delivery time lines, and product warranties
- Control over the contracting process

State Laws Apply

Some State procurement laws and policies are more stringent than federal regulations. Most States practice a strict procedure in soliciting bids from a certain number of contractors and conducting a formal evaluation before a contract is awarded. Some State laws establish criteria for recognizing small businesses in their incentive programs. In order to make small business awards using the cooperative purchasing programs, schedule vendors would have to meet these same criteria before a State small business award could be made.



For more information on the [U.S General Services Administration](https://www.gsa.gov) and the GSA Schedule go to www.gsa.gov.

4.8.3.2 National Association of State Procurement Officials (NASPO) ValuePoint

Several States are using procurement cooperatives operated by nonprofit organizations or fellow States to meet their needs. One example is NASPO ValuePoint (formerly the WSCA-NASPO).³⁵ NASPO ValuePoint was established to enable participating States to benefit from cooperative multi-state contracting. This approach is intended to help States achieve cost-effective and efficient procurement of products and services. NASPO ValuePoint provides



members access to a range of contracts encompassing a variety of products including computers, communications equipment, and general electronics. All NASPO members, as well as non- NASPO members, are welcome to use the approved agreements.

NASPO designates lead agencies to coordinate and conduct the RFP and award for cooperative multi-state contracts. Lead State agencies are assigned a product category and are responsible for competitively soliciting prices from vendors and establishing contracts. Lead States must abide by their State's procurement guidelines and regulations, and all contracts are to include terms allowing the other NASPO members to place orders. To participate, States must have authority (either statutory or ordinance-driven) to share the NASPO contracts with other States. Non-NASPO States are generally able to use NASPO ValuePoint contracts if they have followed their own statutory processes. Some States have the authority to utilize cooperative contracts, but lack the authority to act as a lead agency on a contract.



For more information on the National Association of State Procurement Officials and the [NASPO ValuePoint](http://www.naspovaluepoint.org/#/home/contracts) go to <http://www.naspovaluepoint.org/#/home/contracts>.

4.8.4 Contract Periods

The length of the contract period will depend on the goods and services needed, as well as the type of contract. Typical contracts have a base period, commonly three (3) to five (5) years, with several optional extension years. Option periods are typically in one-year increments but may vary depending upon State preference or project needs. State agency procurement rules may dictate a shorter timeframe with limited renewals.

FNS and State agencies should seek the best value and best service for IT projects. The optimal contract length will depend on several factors. Contract length impacts pricing/cost, quality and schedule delivery, and performance parameters. The contract period selected should help to minimize the potential need for amendments to the contract scope, terms, cost, and federal approval.

FNS recommends that the contract length be limited to 5 to 10 years, inclusive of option years. This provides a balance between State management of procurement activities and the benefits to be gained by obtaining an updated assessment of the marketplace.

- A period that is too short may limit a State's flexibility and require the use of resources from both State and vendors' staffs for frequent re-procurements. Frequent re-competition due to short timeframes and limited option periods is burdensome and costly for both the State agency and contractors. It increases project risks to manage the potential transition to a new contractor.

- A period that is too long may cause the State to miss the potential benefits of competition to the incumbent contractor and obtain fresh perspectives from other bidders. The IT industry typically undergoes relatively rapid advances in technology, innovation, and service delivery or performing services. For products or services where “generational” change is frequent or where pricing is rapidly dropping in the field, contract lengths should be kept shorter in order to allow re-competition to take advantage of these technological advancements or price trends.



The term of the contract must not deviate from the term found in the RFP. In addition, contract values and not-to-exceed amounts should be specified for both the base period and optional extension periods.

4.8.5 Contractor Types and Roles

State agencies that implement FNS programs use several types of contractors to support the different phases of the SDLC. Agencies typically use contractors for support in such areas as: planning, development and implementation, quality assurance, project management, Independent Verification and Validation (IV&V), and system maintenance and operations.

Many States choose to perform planning activities themselves. Others may wish to acquire a contractor who will not only assist in performing the feasibility and requirements analyses, but also produce the IAPD and RFP for the implementation phase. The type of contractor a State agency may need depends upon the complexity and specific intended outcomes of the project. Internal resources, expertise, and the budget allocated to the project are all factors that determine the type of contractor procured. States may have in-house resources that can carry out some functions without the need of contractor assistance.



Solutions involve the participation of several types of contractors.

- **Contractors** are those under contract to the State and from whom a delivered system is expected
- **Integrators** are those who perform the task of integrating different commercial items into a functioning system
- **Vendors** are those who sell products in the marketplace

It is possible for some or all of these roles to be combined.

The contractor always reports to the State agency for task assignment, deliverable acceptance, and payment. The roles listed below are examples of functions that may be performed by a contractor for a State agency.

Design, Development, and Implementation (DDI) is the process of defining, designing, developing, testing, and implementing a new software application or program. A DDI contractor specializes in designing, building, and implementing new IS, including complete systems, enhancements, or upgrades.

Transfer and Implementation (T&I) is the transfer of a system, component, or data, typically from one State's hardware or software environment to another State. Any planned or desired modifications to the current "core" code are usually kept to a minimum. T&I contractors are often referred to as integrators. When a State agency is transferring a system, requirements for the T&I must include any enhancements and code modifications.



State agencies must remain aware of potential conflict of interest when using multiple contractor types for a project. See **section 4.8.6** for detailed guidance regarding conflict of interest.

4.8.5.1 The Planning Contractor

The primary goal of procuring a planning contractor is for the State agency to hire professional, consultative services for planning activities during the planning and procurement phases of the project. The planning contractor may support project planning, but the State agency must retain all decision-making authority and accountability for project management.



Typical responsibilities for the planning contractor are listed below:

- Guiding the State agency in identifying system requirements to meet program needs
 - Provide functional analysis of alternatives and identify potential system solutions (upgrade, transfer, new development)
 - Arrange and set up demonstrations of potential systems
- Recommending procurement methods for acquiring alternative solutions
- Identifying risks and recommend risk mitigation strategies
- Assisting in business process review or reengineering efforts to streamline or improve business processes before the introduction of a new or updated system
- Facilitating schedule coordination by assisting in identifying and achieving planning milestones
- Developing documentation for meetings and documenting planning decisions
- Creating and maintaining a central repository to house documentation
- Guiding the State agency and assisting in development of the IAPD
- Guiding and assisting the State agency in development of the Implementation RFP
 - For either the DDI or the T&I contractor
 - Handling RFP revisions, finalization, and coordination until FNS approval
- Developing RFPs for additional contract services, such as PM and QA
- Developing a recommendation for the planning and procurement schedule
- Generating periodic status reporting for project stakeholders, including FNS and other funding agencies

4.8.5.2 Project Management Contractor

The function of the Project Management (PM) contractor is to maintain a well-managed project adhering to well-defined scope, schedule, and cost constraints. A PM contractor may be retained by the State agency to carry out project management roles and project activities instead of using State agency staff to perform these activities. The PM contractor may play a major role during the development and implementation phase of the project lifecycle when the State agency is not using its own staff to perform these duties.



While a PM contractor may assume the day-to-day PM activities, the State agency remains responsible for project management and federal reporting. The PM contractor reports to the State agency project manager or project director as defined in the contract. The State agency must retain all decision-making authority and accountability for project management. The State agency's project manager or project director is responsible for all communications with the federal funding authorities.

Typical roles and responsibilities for PM contractor support include, but are not limited to, these activities:

- Planning and coordinating additional demonstrations of systems as needed
- Providing the State agency with additional expertise and advice on management of the development and implementation processes
- Overseeing and monitoring program activities (State agency supervises system development and implementation; contractor advises State on these activities)
- Developing a user training plan
- Ensuring that testing and training are conducted properly and meet State and federal requirements
- Providing PM support by ensuring the program stays on track, meets timelines, and stays within budget
- Identifying potential solutions to correct program missteps, delays, and cost overruns
- Coordinating activities of key stakeholders and decision makers
- Facilitating coordination by performing the following duties;
 - Assisting in identifying and achieving project milestones
 - Coordinating and scheduling meetings
 - Developing documentation for meetings
 - Maintaining a central repository to house documentation
- Producing periodic status reports for State decision makers, FNS, and other stakeholders

4.8.5.3 Planning and PM Contractor Considerations

To decide the level and type of contractor support required during the initial planning phases of the project, the State agency must evaluate the options for selecting a planning and PM contractor. **Table 21** identifies some of the considerations involved in making key decisions concerning planning and PM support.

Table 21: Pros and Cons of Contractor Options

Pros	Cons
Option 1: A single contract for performance of both planning and PM Roles	
- Increases continuity of efforts - Does not require additional ramp-up time to learn issues - Has potential for increased efficiency of contractor resources; familiarity with State agency operating procedures - Can result in time savings	- Harder to define roles and responsibilities, such as those of the PM, for future project phases because the planning phase for defining roles, responsibilities, and activities covering the entire project has not yet occurred - May increase cost by resulting in higher bids from potential contractors due to unknowns
Option 2: Two Separate contracts awarded for contractor performance of planning and PM roles. In this instance: - State writes separate RFPs for planning and PM contractor functions OR - Planning Contractor writes PM contractor RFP	
- Could facilitate project movement by allowing release of the initial planning contractor RFP instead of requiring additional time to define specifications and release a single RFP - Provides the opportunity for decreased risk of conflict of interest in bidders limited to only one of the two project phases - Enables more accurate definition of tasks and requirements prior to contract award - Potentially lowers contract costs due to contractors' bidding for the PM support task after the costs have been fully defined and accurately detailed	- Requires two RFPs to retain contractors (however, both RFPs may be drafted initially, and the second RFP may be revised later) - Can lead to loss of continuity and efficiency - Can reduce the number of contractors competing if potential bidders choose not to bid on the planning role, allowing them to be eligible to bid on the longer term and greater value contract to fulfill the PM role

4.8.5.4 Development and Implementation Support Contractor

Some IS projects involve the design, development and implementation of a new system. Other options may include transferring a system from one State to another (also known as Transfer and Implementation (T&I) Contractors) and enhancing or upgrading to the existing system. Choosing the appropriate contractor for these projects requires as much consideration as choosing between a new system or a transfer system.



The development and/or implementation support contractors have these responsibilities:

- Creating a detailed design and development schedule
- Guiding the State agency through a detailed design process to verify functional and technical requirements
- Writing or adapting software code and converting the data from the old system
- Writing technical and user documentation
- Installing hardware and software to support the system
- Developing any necessary interfaces to other systems, such as Electronic Benefits Transfer (EBT)
- Designing and building enhancements to the system
- Testing and demonstrating system functionality or enhancements
- Developing test plans and scenarios for users of system enhancements
- Correcting defects discovered during testing before implementing the system and during warranty periods
- Implementing rollout of the new or enhanced system
- Training users on the new system
- Implementing enhanced system rollout
- Providing preliminary Help Desk support

4.8.5.5 Maintenance, Operations, and Enhancements Contractor Support

State agencies may provide their own staff or procure contractor services for maintenance, operations, and enhancements, or a combination of State and contracted support services for the IS after implementation. The contracted services may be a separate competitive procurement from the initial implementation RFP.

The following descriptions differentiate among these support services.

- **Maintenance** - Process of modifying a system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment with the purpose of maintaining the value of the existing system. This includes ensuring that current software upgrades are installed for commercial products (e.g., operating systems, database systems) and verifying that other software applications are not adversely affected by the upgrades.
- **Operations** - The operating of the IS and networks. It may include the day-to-day procedures for operating the system, performing routine housekeeping procedures on the system, reviewing error logs, responding to any issues, and running end of period reports (e.g. daily, monthly), and performing procedures to include creating backup of key data files.

- **Enhancement** – A modification that will change the functions of software and hardware beyond their original purposes. Enhancements correct errors or deficiencies in the software or hardware or improve operational performance of the software or hardware. A major enhancement is a software change that significantly increases risk, cost, or functionality of the system.

In addition, during M&O, the State agency should provide for QA or Independent Verification and Validation (IV&V) services for system enhancements. These types of contracts must be with a separate contractor than the M&O contractor to avoid a conflict of interest. QA and IV&V contracts serve the same purpose as when utilized during system design, development, testing, and implementation.



Refer to chapter **6.0**, section **6.9 Test Lifecycle Support**, for more information on QA and IV&V and section **4.2 Procurement Process Summary** for thresholds.

FNS recognizes the risk of competitively procuring enhancement work for an operational system. There is the potential for hiring a different contractor to modify a system other than the contractor currently maintaining the system. FNS recommends a T&M contract for these situations when the RFP includes provisions for:

- Time and materials work should include hourly labor rates
- An overall dollar limit specified in the contract (e.g., not to exceed 20 percent of the cost of the base contract)
- Rates for such work should be required as part of the bidder's cost proposal and considered in the overall evaluation of the bids.

4.8.6 Conflicts of Interest

Conflicts of interest may arise when procuring contractors for IS procurement efforts, particularly related to planning and implementation activities. A conflict of interest is any situation that may have or may appear to have one of the following ramifications:

- Impair a contractor's ability to provide objective and impartial information, advice, or counsel
- Create an unfair competitive advantage for the contractor or its subcontractors

A conflict of interest can have serious consequences for the contractor and the State agency. The contractor runs the risk of being precluded from bidding or performing future work due to a perceived unfair competitive advantage; of damaging its professional reputation; or of being debarred. The State agency may suffer injury due to real or perceived bias or lack of objectivity in its work. Employees, officers, or agents of the State agency are prohibited from participating in the selection, award, or administration of a contract if a conflict of interest, real or apparent, would be involved. Such conflicts may arise when an employee, officer, agent, or any member of his

or her immediate family, his or her partner, or an organization that employs or is about to employ any of the above has a financial or other interest in the procurement.

To avoid conflict of interest, contractors that assist States with procurement activities may not bid on the work to be procured. For instance, planning contractors are not allowed to bid on the implementation phase of the project.

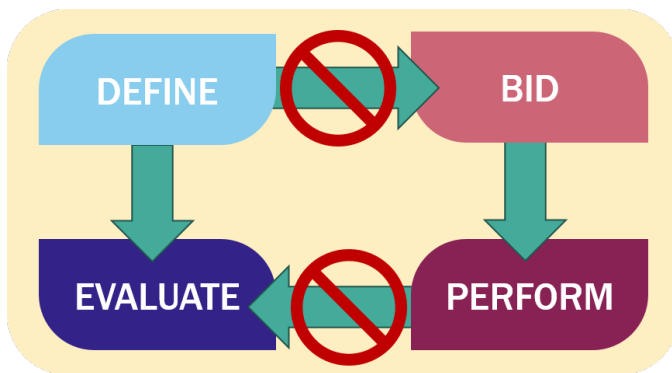


Figure 40: Conflicts of Interest

Conflict of Interest among contractors consists of two simple conflict scenarios.

The same contractor must never:

- Define the work and then bid on it, or
- Perform the work and then evaluate it.

FNS strongly discourages States from pursuing combination contracts, such as Planning and Quality Assurance. Although these areas are closely related, State agencies should strive to promote full and open competition and avail themselves of expertise in all areas to avoid any conflict of interest. States should carefully weigh the roles and responsibilities of each area in making this decision.

For example, no contractor is allowed to define the requirements, tasks, or skills for another contracted function and then bid on that function. As shown in **Figure 40** and **Table 22**, this would occur if a planning contractor wrote the requirements or RFP for the QA contractor and then bid on the work, or if a project management contractor also served as a QA contractor by evaluating the project. They would, in essence, be evaluating how well they are managing the project.

Contractors potentially enter a conflict of interest when asked to take any of the following actions:

- Analyze or evaluate the performance of components of an agency with which they have ongoing or future expectations of business
- Review products or deliverables they have helped develop
- Develop specifications or SOWs that they may wish to respond to or that will be responded to by organizations with which they have business relationships
- Provide procurement support to an agency and also seek to be a product or system supplier to that agency



- Have access to budgetary, source selection, or other nonpublic information on future procurement programs for which they expect to compete
- Have access to sensitive third-party information that gives insight into competitor approaches to future procurements
- Define performance parameters during planning against which they will be evaluated, or measure their own performance as implementers
- Perform systems planning and implementation activities

Table 22: Conflict of Interest Examples

Activity A	Activity B	Conflict	Rationale
Planning	Development/ Maintenance & Operations	Yes	This violates the rule against defining the work and then bidding on it. Planning contractor would have unfair advantage in bidding process based on knowledge of the development requirements.
Project Management	Development	Yes	This violates the rule against performing the work and evaluating it. Project manager cannot provide objective management/oversight of its own work.
Project Management	Maintenance & Operations	Yes	If the PM helped define the M&O responsibilities and deliverables, it would have an advantage over other bidders. If filling both roles, the PM cannot provide objective management/oversight of its own work.
Development	Quality Assurance	Yes	This violates the rule against performing the work and evaluating it. The contractor cannot provide objective QA of its own work.
Planning	Project Management	Possibly	If the planner helped define the roles and responsibilities of the PM, it would have an unfair advantage in bidding based on inside knowledge of those requirements. This would not be a conflict of interest if the State defined both roles up front in the same RFP (so no contractor helped define either role). However, it may be difficult to accurately define the PM responsibilities and expectations before the planning process even begins.

Table 22: Conflict of Interest Examples

Activity A	Activity B	Conflict	Rationale
Planning	Quality Assurance	Possibly	There would be a conflict of interest between these two roles if the planning vendor helped define the responsibilities of the QA and had “inside knowledge” of those requirements, creating an unfair advantage in bidding. A contractor who helped define the project requirements in the planning phase may be well-suited to help evaluate whether the deliverables meet them, as the QA, as long as no conflict of interest occurred in securing both roles. However, the State agency may prefer the greater impartiality of a third party.
Project Management	Quality Assurance	Possibly	This potentially violates the second rule against performing the work and then evaluating it, because the QA role may include evaluation of the effectiveness of the project management process.
Quality Assurance (or any other function)	Independent Verification & Validation	Yes	IV&V is a review process performed by an organizational entity that is independent of the QA contractor or any other project role. Independence increases the success of system testing and implementation.

4.9 Procurement Documents

4.9.1 Request for Proposals

An RFP is a solicitation document used by organizations to elicit bids from potential vendors to procure a product or service based on responsive business proposals. The RFP process is meant to bring structure and transparency to the procurement decision, while reducing risk through open requirements and discussion.



The State agency may choose to hire a planning contractor to write the RFP for development and implementation services. However, State agency staff should strive to gain the confidence and expertise to drive the RFP process and manage the contractor appropriately. Not doing so may result in a system that does not meet State agency requirements.



As part of RFP preparation, it is important that the State agency have a general procurement and source selection strategy. Previous sections of this chapter describe many of the required planning activities for developing the procurement and source selection strategies.

It is important that RFPs released to the vendor community clearly outline State agency requirements and expectations. The following actions are recommendations for releasing a clear RFP:

- Ensuring that RFPs contain enough detail to clearly define requirements and the process by which detailed requirements may be added later, depending upon the development methodology being used
- Describing requirements and timeline expectations in specific terms to provide the contractor with adequate information to develop a responsive bid
- Describing acceptable levels and measures of performance for products and/or deliverables
- Ensuring that the State agency employs an RFP review process by individuals having sufficient technical expertise and knowledge so that the support requested in the RFP is what the State agency desires

The RFP should clearly describe the evaluation factors that will be considered in making the source selection. Factors such as cost or price, cost or price-related factors, past performance, and other non-cost or non-price-related factors should be assigned a relative weight or importance. Once the RFP is finalized and approved by the State procurement office and FNS, it is released to the contracting community.

4.9.2 Contracts

A contract is a legally enforceable agreement between two or more competent parties, is mutually binding, and obligates one party to furnish something of value and the other party to provide payment.

Writing Contracts

State agency procurements should reflect the federal requirements and ensure that the procurement is conducted in the most effective and economical manner while ensuring fair and open competition. The State agency is responsible for settling all contractual and administrative issues resulting from procurements. Contract terms should include holdbacks, liquidated damages, and other penalties described as incentives and remedies in performance-based contracting.

Additional contract requirements related to federal procurement standards³⁶ include the following:

- Effective Date and Term—Identifies when the project starts and ends
- Performance Standards—Describes the subject matter of the contract, why the contractor has been selected, and expectations for contractor performance

- **Priority of Documents**—States that the conditions, provisions, and terms of the RFP which the contractor’s proposal must meet under this contract
- **Quality of Work and Warranty**—States the requirements concerning contractor expert knowledge and skills needed to accomplish the tasking in a manner acceptable to the State
- **Modifications to the RFP**—Describes all modifications, if any, to the RFP
- **Duties and Obligations of the Contractor**—Describes the scope of work
- **State Duties and Obligations**—States the project management process, time limit for acceptance of deliverables, compensation requirements, contract renewal or extension requirements, and other contract modifications
- **Breach Procedure**—Describes the procedures for notice of breach, the right to cure, and available remedies
- **General Provisions**—Describes in detail the legal conditions and issues regarding the relationship between the contractor and the client, including insurance policies and compliance with federal requirements and regulations
- **Special Provisions**—Lists other special conditions, such as funds availability, software piracy prohibition, and employee financial interest conflicts

4.9.3 RFP and Contract Components

The RFP is not a legally binding document for procuring goods and services in the same way as a contract. It does not obligate either the State agency or the respondents to complete the proposed project. However, the contents of the RFP should reflect what the intended contract will bind both parties to once it is signed. In this sense, the composition, content, and layout of the RFP should be almost identical to that of the subsequent contract.



“Shall” and “will” are not interchangeable in terms of being contractually binding. When you need the contractor to perform a task, you must use the word “SHALL” for that tasking to be legally binding.

4.9.3.1 RFP and Contract Format

FNS does not prescribe a specific format for State agencies. Each State has its own procurement policies, regulations, and forms. However, FNS does have expectations of what must and should be included in RFPs and contracts.



For both the RFP and the resulting contract, each typically has the same format and contains the same relative information. However, the contract will not contain three sections: 1) Representations, Certifications, and Other Statements of Offerors; 2) Instructions, Conditions, and Notices to Offerors; and 3) Evaluation Factors for Award. These sections are only found in the RFP because they give directions to the offerors on how to respond to the State agency's RFP. Once a contract is awarded, these directions are no longer relevant for the purposes of executing the contract.

4.9.3.2 Guidance for RFP and Contract Descriptions

During the system's lifecycle, the State agency will need to develop and release several RFPs for acquiring various contracted goods and services. RFPs will likely be released to procure planning, QA, development and implementation, and M&O contractor support. The following is general guidance on the content for various parts of RFPs.

- **Introduction and Overview** – Includes details such as background information about the effort; agencies and programs that will use the system, including any placeholders for potential future partners; major objectives of the proposed system; type of contract anticipated; and procurement schedule.
 - **Current Processing Environment**—Describes existing methods, procedures, systems, applications, hardware configurations, and components that the system will support
 - **Workload Data**—Describes statistics of online transactions, volumes of regular and peak loads, and incremental growth forecast for various workload data, etc.
 - **New System Environment**—Describes improvements that the agency expects to gain, performance requirements, database management requirements, associated constraints, and so on.
- **Statement of Work (SOW) or Performance Work Statement (PWS)** – Depending on the procurement, this section may be a Performance Work Statement (PWS) or a Statement of Work (SOW). In either case, the document may contain a Work Breakdown Structure (WBS). The WBS provides a way to align the requirements, desired schedule, and deliverables, to the price proposals, staffing, performance standards, and delivery standards. The WBS provides a framework for the offeror's technical and management approach. This section contains the description of the products to be delivered or the work to be performed under the contract. This section typically includes the State agency's preliminary system performance specification.
 - **Performance Work Statement (PWS)**. A PWS identifies what the State agency's objectives or desired outcomes are but does not specify how to do the work (unlike the SOW). It also contains the standards of performance for determining if the requirements have been met. The PWS gives contractors flexibility to propose alternate solutions to meet requirements. It is most often used for the procurement of services.

- **Statement of Work (SOW).** A SOW defines the efforts to be accomplished by the contractor. It describes requirements in detail, establishes non-specification tasks, and identifies the scope of the contractor's effort. The SOW can be provided in full text or incorporated by reference, then included as an attachment. Both the State agency and the contractor look to the SOW as a key document defining the responsibilities of both parties. After contract award, SOW requirements and associated specifications constitute the standard for the contractor's effort, providing the baseline against which progress and subsequent contractual changes are measured. The SOW can be used for procurements ranging from a small research study to the development of a complex management information system.



Whether the State agency or a contractor writes the SOW or PWS, it is important that the work statement be clear, concise, and complete. The more elaborate the wording, the greater the possibility of miscommunication between the State agency and the contractor about the State agency's requirements or objectives.

The SOW lists the tasks and other potential activities, mandatory requirements, deliverables, and staffing, including the following items:

- **Desired Schedule**—Provides realistic schedules, including time for State review and approval of each deliverable (as well as federal, if applicable)
- **Contract Deliverables**—Describes the products and services that the State expects the contractor to deliver (This should also include acceptable performance criteria or measurements for each deliverable.)
- **Installation, Conversion, Maintenance, and Personnel Requirements**—Lists specific requirements for installation and onsite maintenance as well as staffing requirements
- **Functional Requirements Document (FRD)**—Defines the proposed system and documents system goals, objectives, and programmatic requirements and describes what the new system and/or hardware should do
- **Management Plan** – Identifies management requirements, such as the State agency project manager/lead State agency to whom the contractor will report, the type and frequency of project status reports, and the review and approval process for work performed.
- **Contract Clauses** – Because the acquisition of rights to computer software and computer software documentation is a special interest for use of FFP, Contract Clause language should include relevant clauses for acquiring ownership rights for software being procured using FFP. Contract Clauses typically incorporate the clauses by reference to appropriate State or Federal policies and regulations

with the same force and effect as if they were given in full text. However, in the absence of references, the clauses need to be clearly and properly written.

- **Solicitation Instructions and Conditions** – List the issuing office and agency manager responsible for procurement, submission requirements, limitations/stipulations imposed on all bidders, standards, and subcontractors and so forth. This section instructs the offerors on how to structure their proposal and what should be included in each proposal section. It needs to clearly identify the structure and composition of each volume and section of the proposal and should track to the evaluation factors in Evaluation Factors for Award. The technical definition of the computer software architecture and data meta-model, estimated sizing, throughput timing, and growth migration strategy also need to be defined as a condition of award criteria in the “Instructions, conditions, and notices to offerors” section and in the offeror’s proposal. FNS requires that all solicitations remain open for a minimum of 90 days to allow vendors sufficient time to respond and to promote fair and open competition.
- **Proposal Structure and Content** – Describes expectations for the general appearance and organization of the proposal (e.g., separation of information into volumes), attachments, supplements, and other supporting documentation as listed below.
 - The technical approach in a separate volume from the pricing and costing proposal. The technical volume should not include any costing or pricing information.
 - A statement, including personnel background and experience, of the contractor’s staff resources planned for assignment to the project
 - A statement of corporate financial resources, history of prior involvement in similar projects, and information regarding pending litigation, debarment, and suspension
 - Pricing and Cost proposals presented in a separate volume from the technical response because pricing is evaluated separately. Line-item cost statement, covering both developmental and operational costs, for the expected life of the system
- **Evaluation of Proposals and Contract Award** – Identifies proposal controls, such as the methods that States will use to evaluate proposals, requirements for benchmarks and system demonstrations, evaluation criteria, and State appeals process. This section should be carefully structured to address only those elements determined to be discriminators in the source selection to select the best proposal with acceptable program risk. The most effective evaluation factors are measurable, relevant to the program, traceable, with expected differentiation among the offers, and under the offeror’s control.



Refer to appendix **A10 Request for Proposal Template** for additional information and guidance. Also see appendix **A12 RFP and Contract Review Checklist**.



When creating the RFP, it is important to consider Instructions to Offerors and Evaluation Factors for Award first. Evaluation Factors should be defined before attempting to complete the Instructions to Offerors. This establishes the conditions so that Evaluation Factors directly elicit responsive information and should only contain factors for which there is a corresponding request for proposal information in Instructions to Offerors. In preparing Evaluation Factors and Instructions to Offerors, be aware of the proposal preparation time and page limitations by which offerors are constrained. Ask only for information that should be readily available to offerors and that is necessary to accomplish the source selection evaluation.

4.10 Procurement Summary

The major objective for the State agency in any procurement process is to identify the best solution to meet the State's specific information system needs for supporting SNAP, WIC, and related EBT systems. FNS recommends that State agencies conduct the procurement and contracting process in accordance with their State-defined processes.

- Procuring goods and services may require FNS review and approval of the various RFPs and contracts
 - Changes and modifications (i.e., amendments) to existing contracts may need FNS review and approval
 - The requirement for FNS reviews of procurement documents are based on the potential dollar value of the contract or amendment
 - The thresholds used for determining the need for FNS reviews are different for competitive (**Table 16**) and non-competitive (**Table 17**) procurements
- Procurements using Federal financial Participation are governed by State agency and federal policies, which include:
 - [2 CFR 200.416](#) and [2 CFR 200.417](#) "Cost Principles for State, Local, and Indian Tribal Governments"
 - Regulations at [7 CFR 277.14](#) – "Procurement Standards"
- Key federal procurement requirements include:
 - State agency procurements must be conducted in a manner that provides for maximum full and open competition
 - The RFP and contract must include ownership rights and a broad federal License as provided in [7 CFR 277.18\(l\)](#)
- State agencies must include several required assurances in contracts for work funded by FNS and other cognizant federal agencies.
 - These assurances must be part of the RFP to ensure that potential contractors understand the agreement they are entering into before they commit resources to developing a response
 - **Table 21: Basic Contract Provisions and Federal Assurances** provides a summary of the major RFP and contract provisions the State agency must include



- State agencies that implement FNS programs may use several types of contractors to support the different phases of the SDLC to include contractors for the following processes:
 - Planning
 - Development and implementation
 - Quality assurance
 - Project management
 - Independent Verification and Validation (IV&V)
- Procurements have three overall phases: Pre-Award, Award, and Post-Award
- Pre-Award Phase - when the majority of procurement planning occurs
 - State agency's acquisition strategy developed during procurement planning results in requirements
 - Procurement planning produces information to prepare the RFP
 - The RFP must include:
 - Terms and conditions
 - Required federal procurement clauses
 - Federal assurances
 - Conflict of interest statements
 - Other legalities developed during procurement planning
- Award Phase - when the source selection is performed
 - Evaluation of proposals based on price, technical response, past performance, and other criteria are the key events during the award phase
 - Evaluating proposals is based on the information provided in the RFP developed during procurement planning
- Post-Award Phase - begins when award notifications are made
 - Once approved, the contract is awarded, award notifications are made. Any protests are resolved during the notification process.
 - Award is finalized after FNS approval of the contract
- A key component of the RFP and contract are the system functional and technical requirements developed during System Planning (see Chapter 5.0)



Endnotes

-
- ¹³ “Procurement Requirements”, 7 CFR 277.18(c)(2)(iii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_118
- ¹⁴ “Disposition”, 7 CFR 277.13(b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_113
- ¹⁵ “Disposition”, 7 CFR 277.13(b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.277&rgn=div5#se7.4.277_113
- ¹⁶ “Transfer of title to certain property”, 7 CFR 277.13(c), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.277&rgn=div5#se7.4.277_113
- ¹⁷ “Disposition”, 2 CFR 200.311(c), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=ff484db18414dbfbb43d5af191d986c3&mc=true&node=sg2.1.200_1309.sg2&rgn=div7
- ¹⁸ “Special Considerations for States, Local Governments and Indian Tribes”, 2 CFR 200.416 through 200.417, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=869b161f2b2d06ad4ad5bd520d3e756f&mc=true&node=sg2.1.200_1415.sg14&rgn=div7
- ¹⁹ “Procurement Standards”, 7 CFR 277.14, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_114
- ²⁰ “Equipment”, 2 CFR 200.313, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=f219d0e0a6b141b3d986a96fb84993eb&mc=true&node=se2.1.200_1313&rgn=div8
- ²¹ “Electronic Benefits Transfer (EBT) System Transition Guide”, Version 2.0, U.S. Government, June 6, 2005, http://www.fns.usda.gov/sites/default/files/FSP_EBT_Transition_guide_6-05%5B1%5D.pdf
- ²² “Quality Assurance Surveillance Plan”, AcquiPedia, June 27 2016, <https://www.dau.edu/acquipedial/pages/articledetails.aspx#!354>
- ²³ “Government Contract Quality Assurance General”, Federal Acquisition Register Subpart 46.401 (a), U.S. Government, <https://www.acquisition.gov/?q=/browse/far/46>
- ²⁴ “Code of Conduct”, 7 CFR 277.14(c), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_114
- ²⁵ “Contracting with small and minority firms, women’s business enterprises and labor surplus area firms” 7 CFR 277.14(e), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_114



-
- ²⁶ “Procurement Requirements”, 7 CFR 277.18(c)(2)(iii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6a761d62f7ce6055cfad4e5088ec004a&mc=true&node=se7.4.277_118&rgn=div8
- ²⁷ “Competition”, 2 CFR 200.319 (b), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=0cd7382a06e57361da4a63e47b58ae37&mc=true&node=se2.1.200_1319&rgn=div8
- ²⁸ “State agency procurement records”, 7 CFR 277.14.(i), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_114
- ²⁹ “Ownership Rights, Software”, 7 CFR 277.18 (l)(1)(ii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6a761d62f7ce6055cfad4e5088ec004a&mc=true&node=se7.4.277_118&rgn=div8
- ³⁰ “Rights in Data—General”, FAR 52.227-14; also “Rights in Data—Special Works”, FAR 52.227-17; also “Rights in Data—Existing Works”, FAR 52.227-18; also “Commercial Computer Software License”, FAR 52.227-19, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?mc=true&node=pt48.2.52&rgn=div5#se48.2.52_1227_614
- ³¹ “Disallowance of Federal financial participation (FFP)”, 7 CFR 277.18 (h), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ³² “Accelerated Procedure”, Civil Board of Contract Appeals Part II Rule 53, U.S. Government, <https://www.cbca.gov/howto/rules/procedure.html#rule53>
- ³³ “Cooperative Purchasing”, General Services Administration, U.S. Government, <http://www.gsa.gov/portal/content/202285>
- ³⁴ “Price Reductions”, General Services Administration, U.S. Government, <http://www.gsa.gov/portal/content/200397%20>
- ³⁵ NASPO ValuePoint, Cooperative Purchasing, (February 2015), <http://www.naspovaluepoint.org/#/home/contracts>
- ³⁶ “Procurement Standards”, 7 CFR 277.14, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%23se7.4.277_114%20#se7.4.277_114



5.0 System Planning

Key Points

The information in this section should allow you to understand the following:

- What is the relationship of system planning to the APD process?
- What is the purpose of completing a needs assessment?
- What are the important activities for doing a needs assessment?
- What system planning activities are necessary after completing the needs assessment?
- What are the important activities for doing a feasibility study?
- What are the key considerations in system planning?

Chapter Contents

5.1	State Planning for Information Systems.....	237
5.1.1	System Planning and the APD Process.....	237
5.1.2	Recognizing the Need or Opportunity	237
5.1.3	Acting on the Need or Opportunity	238
5.2	Needs Assessment	239
5.2.1	Business Analysis	240
5.2.2	Business Needs Assessment	241
5.2.3	Business Capability Definition	245
5.2.4	SNAP Program Waivers	247
5.2.5	The Business Case.....	247
5.2.6	From Business Case to APD	248
5.3	Feasibility Study	248
5.3.1	Requirements Analysis	253
5.3.2	Alternative Analysis	257



5.3.3	Cost Benefit Analysis	264
5.4	Technical Planning	268
5.4.1	Data Conversion & Migration	268
5.4.2	Capacity Planning Study	270
5.4.3	Technical Approach	272
5.5	Considerations	273
5.5.1	FNS Priority for Transferability and/or Reusability	273
5.5.2	Technology and System Capabilities.....	278
5.5.3	Implementing New Systems	281
5.6	Summary.....	284

Chapter Acronyms

BCD	Business Capability Definition
BPA	Business Process Analysis
BPR/I	Business Process Reengineering/Improvement
CIO	Chief Information Office or Chief Information Officer
FFP	Federal financial participation
POAM	Plan of Actions and Milestones
RFI	Request for Information
RFP	Request for Proposal
ROM	Rough Order of Magnitude
SIRT	System Integrity Review Tool
SOA	Service Oriented Architecture



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.

5.1 State Planning for Information Systems

5.1.1 System Planning and the APD Process

The principle focus of the Advance Planning Document (APD) process is “planning.” In very simplistic terms, the PAPD explains the State agency’s project objectives and the IAPD explains the results of the activities described in the PAPD, as well as future actions based on the results. The SDLC is the foundation of all of the State agency’s project-related activities. The contents of the PAPD and the IAPD encompass the SDLC activities from initiation through deployment. System development decisions impact data management strategies, including licensing and copyright provisions. These, along with technical planning activities for the system, affect acquisition management decisions, testing requirements, project management, and security management. State agencies are required to provide information on all of the project decisions using the APD. All of the initial activities for preparing APDs begin with systems planning, as depicted in **Figure 41: Planning Activities for Preparing APDs**, which tends to be focused on technical development and supplemented by funding, procurement, and project management.

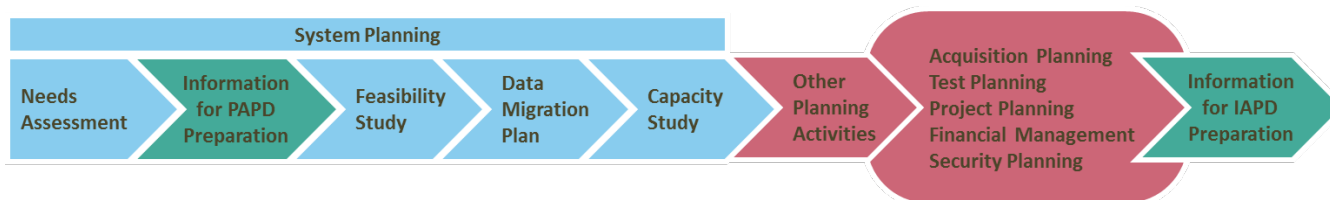


Figure 41: Planning Activities for Preparing APDs

5.1.2 Recognizing the Need or Opportunity

System planning does not necessarily mean that a completely new system is being implemented to replace a legacy system. It may be for a significant enhancement or upgrade during the Maintenance and Operations (M&O) phase of the SDLC. Policy updates for the SNAP or WIC programs may create a need for an enhancement or upgrade. New technology may be an opportunity to enhance existing capabilities, or be required to keep the system current. Malfunctions and errors may require changes so significant that the costs trigger the APD process. The need may be for changes to a recently implemented system or a legacy system. Regardless of whether the State agency is planning a full-scale system implementation, a major enhancement, or a significant upgrade, the planning activities are the same. Only the scope and scale vary. It all starts when a need or opportunity is identified.

5.1.3 Acting on the Need or Opportunity

Once the State agency identifies a need or opportunity, they must do a needs assessment in preparation for the FNS advance planning document process. A needs assessment is a systematic process for determining and addressing needs or “gaps” between current conditions and desired conditions or “wants.” The difference between the current condition (i.e., “as-is”) and wanted condition (i.e., “to-be”) must be measured to appropriately identify the need. The needs assessment, and applicable cost thresholds, are the basis for determining whether a Planning APD must be submitted.



See chapter **1.0 Getting Started with the Advance Planning Document (APD) Process**, section **1.5.1 Thresholds**.

If a PAPD is required, submitted and approved, initial planning activities begin using the results of the needs assessment to continue system planning. This includes doing a feasibility study with alternatives analysis. Together, the needs assessment and the feasibility study make up the initial system planning activities upon which all other planning activities are built. **Figure 42** illustrates the relationships among the initial system planning activities.



This chapter discusses the activities for Needs Assessment and Feasibility Study, which are depicted in **Figure 42**. Refer to **Figure 42** as you read this chapter to understand the process and how each activity relates to the others.

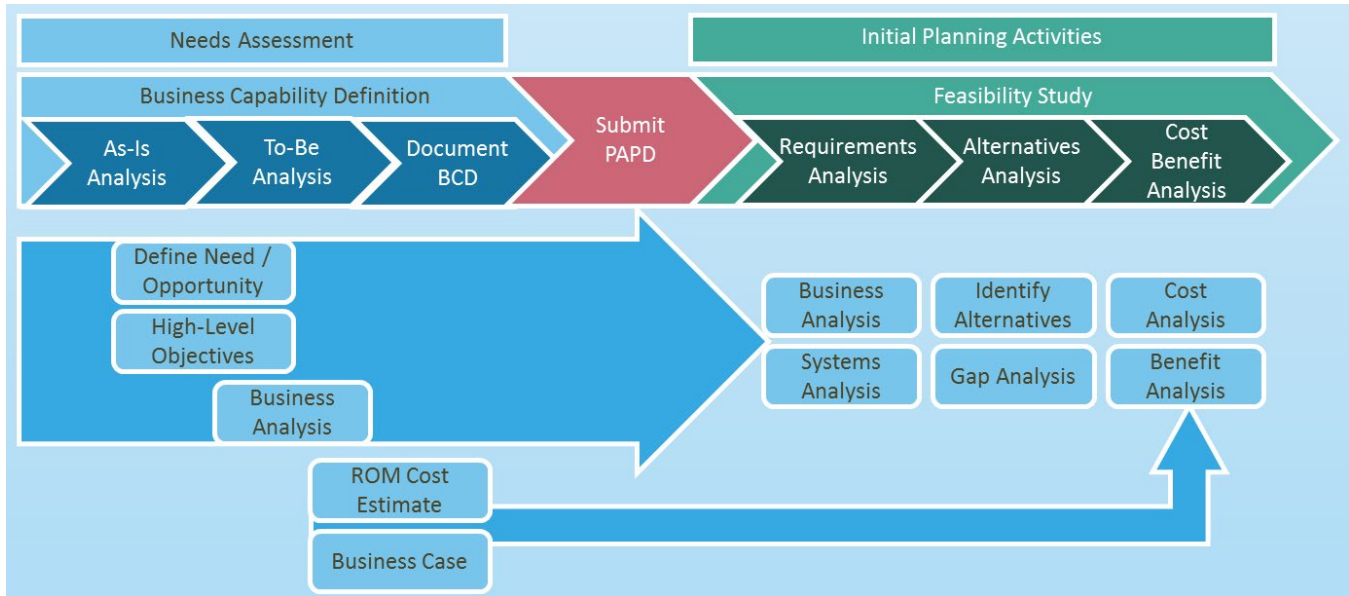


Figure 42: Overview of Initial System Planning

5.2 Needs Assessment

The purpose of the needs assessment is to determine the extent and urgency of the identified need or opportunity and whether the time is right to address it. The needs assessment is not a formal part of the APD process, but an essential preparatory activity leading to the APD process.

The State agency uses the needs assessment activities to build a business case for whether or not to proceed with planning the project. If the business case supports proceeding, the needs assessment activities provide the essential information for the PAPD. A good needs assessment provides the scope of planning activities, funding and resource needs, budget, initial schedule, and cost allocation which must be included in the PAPD.

Whatever the scope of the problem or need, a major responsibility of the State agency is to know whether it is ready to take on the task, willing to commit the resources needed, and able to use FNS funds effectively and efficiently to engage in the SDLC.

The following are some questions the State agency should ask to make this determination:

- Are there sufficient resources available to dedicate to the task?
- Is there a project sponsor, such as a Department head, Program Manager, Commissioner, or State Chief Information Officer (CIO)?



- Is access available to people with the necessary knowledge, skills, and abilities?
- Are technical and management abilities in place? If not, how will the State get them?
- How will knowledge needed to complete the project be developed or accessed?
- What are the State's strengths and weaknesses and how will gaps be filled?
- Will the new system or system changes;
 - Improve program effectiveness?
 - Strengthen controls and accountability?
 - Increase operational efficiency?
 - Meet federal reporting requirements?
 - Better serve program participants?
- Has long-term funding for maintenance and operations been considered?

If the State can positively answer these questions, it is probably ready to begin an IS project, but must be able to obtain buy-in from its key stakeholders.

5.2.1 Business Analysis

During needs assessment, the business analysis is very high-level. A more thorough and comprehensive business analysis must be completed after the PAPD is approved, to support requirements analysis and definition as part of the feasibility study and alternatives analysis.

Business analysis involves assessing the business **needs** of the organization, which are the basis for determining and arriving at a technical solution. Business analysis is the set of tasks and techniques used to facilitate stakeholders' understanding of the structure, policies, and operations of an organization, and to recommend solutions that enable the organization to achieve its goals. It involves understanding how organizations function to accomplish their purposes, and defining the capabilities an organization requires to provide products and services to external stakeholders. In most cases, however, business analysis is performed to define and validate solutions.

It includes:

- The definition of organizational goals; how those goals connect to specific objectives
- Determining the courses of action that an organization has to undertake to achieve those goals and objectives
- Defining how the various organizational units and stakeholders within and outside of that organization interact

All of these focus on understanding the business in order to identify needs, problems, or issues.



Business analysis is performed by business analysts who must analyze and synthesize information provided by a large number of people that interact with the business such as customers, staff, IT professionals, and executives. The business analyst is responsible for eliciting the actual needs of stakeholders, not simply their expressed desires. In many cases, the business analyst will also work to facilitate communication between organizational units. In particular, business analysts often play a central role in aligning the needs of business units with the capabilities delivered by information technology, and may serve as a “translator” between those groups. Business analysis includes Business Needs Assessment, Business Process Analysis (BPA) and Business Process Reengineering and/or Improvements (BPR/I).

These three activities are tools used by business analysts to achieve the overarching purposes of business analysis:

- **Business Needs Assessment** evaluates doctrine⁺⁺⁺, policies, organization, leadership, personnel, training, materiel⁺⁺⁺, leadership, personnel, and facilities within an organization to assess how each of these constrains, supports, or promotes the needed capability for both the “as-is” and the “to-be” conditions.
- **Business Process Analysis** captures various business operations classified into processes, or series of related tasks, where observation revolves around the specific ways in which these processes happen along a lifecycle from beginning to end. It determines how a business process works and how individuals from different groups work together to achieve a business goal.
- **Business Process Reengineering and Improvement** involves the redesign of core business processes to achieve dramatic improvements in productivity, time to complete activities, and quality. It is ideally about improving business processes by making them more effective, efficient, and economical.

Completing business analysis prior to requirements analysis and definition ensures the system design is not based on outdated, inefficient, ineffective, or inappropriate business processes. Optimizing business processes first reduces the need for customization of IS solutions, whether COTS or system transfers. Minimal customization supports the system design goals of portability, interoperability, and compatibility.

5.2.2 Business Needs Assessment

Business needs assessment is based on an analytical approach and method for defining the operational context of a perceived problem. There are eight areas that should be considered in assessing needs.

⁺⁺⁺ Doctrine is different than policy. It includes strategic plans and objectives for an organization and official objectives for programs such as SNAP, WIC, CNP. Mission statements are one example of doctrine.

⁺⁺⁺ Materiel includes all items necessary to execute policy and operate systems supporting SNAP and WIC programs.



Doctrine

Doctrine is different than policy. It includes strategic plans and objectives for an organization and official objectives for programs such as SNAP, WIC, and CNP. Mission statements are one example of doctrine. Doctrines are the fundamental principles that guide FNS and the State in coordinated action toward a common objective. Though neither policy nor strategy, joint doctrine serves to make policy and strategy effective in achieving a common objective. Doctrine is authoritative guidance and will be followed except when, in the judgment of the federal agency, exceptional circumstances dictate otherwise.

- Is there existing doctrine that addresses or relates to the business need? Is it federal? State? Local?
- Are there operating procedures in place that are NOT being followed which contribute to the identified need?
- If no doctrine is in place which pertains to the defined need, does new doctrine need to be developed and implemented that will provide a total or partial solution to the need?

Organization

The organization is a hierarchal arrangement of a department or division with varied functions enabled by a structure that may include joint departments or divisions. These organizational units are the basis through which individuals cooperate systematically to accomplish a common mission and directly provide, or support, capabilities. Subordinate organizations coordinate with other departments or divisions and, as a whole, enable the higher-level organization to accomplish its mission. This includes the State staffing required to plan, operate, sustain, and support SNAP and WIC program capabilities.

- Where is the need or problem occurring? What organizations are the needs or problems occurring in?
- What is the primary and secondary mission / management focus of those organizations?
- What are the organizational values and priorities?
- Is the organization properly staffed and funded to deal with the need or problem?
- Is senior management aware of the need or problem?
- Is the issue already on some type of organizational issue list?
- If so, why isn't the issue being resolved?
- Who exactly is aware of the need or problem, or who is being impacted by the need or problem?

Training

Training includes techniques and procedures to prepare State agency staff to respond to strategic, operational, or performance requirements considered necessary to execute policy and operate systems supporting SNAP and WIC programs.



- Is the need or problem caused, at least in part, by a complete lack of or inadequate training?
- Does training exist which addresses the need or problem?
- Is the training being delivered effectively?
- How are training results being measured and monitored?
- Is the need or problem caused by a lack of competency or proficiency on existing systems and equipment?
- When was the need or problem discovered? During maintenance, operations, or training?
- Do personnel affected by the need or problem have access to training?
- Is the training effort supported by leadership?
- Is training properly staffed and funded?

Materiel

This includes all items necessary to execute policy and operate systems supporting SNAP and WIC programs (e.g., information technology, information systems, telecommunications, hardware, and software; related spares, repair parts, and support equipment, but excluding real property, facilities, and utilities). FNS advocates the reuse and/or transfer of existing materiel when feasible more than the development or acquisition of new materiel. FNS recognizes the age and capabilities of materiel may be a contributing factor in some cases.

- Is the need or problem caused, at least in part, by inadequate systems or equipment?
- What legacy systems exist where the problem is occurring?
- What functionality would a new system provide that currently does not exist?
- What increases in operational performance are needed to resolve the need or problem?
- Is the need or problem caused by a lack of competency or proficiency on existing systems and equipment?
- Can increases in performance be achieved without development of a new system?
- Who would be the primary and secondary users of the proposed systems or equipment?
- Is interoperability either a driver or barrier to the need, or a problem resolution?

Leadership and education

Professional development of all leadership is the product of a learning continuum that comprises training, experience, education, and self-improvement. The role of professional education is to provide the education needed to complement training, experience, and self-improvement to produce the most professionally competent individuals possible.

- Is the need or problem caused, at least in part, by inability or decreased ability to cooperate, coordinate, or communicate with external organizations?



- Does leadership understand the scope of the need or problem?
- Does leadership have resources at its disposal to correct the need or problem?
- Has leadership been trained on effective change management principles?
- Has leadership properly assessed the level of criticality, threat, urgency, risk, etc. of the operational impact(s) of the need or problem?
- Is leadership aware of the drivers and barriers to resolving the need or problem within the organization?
- Has leadership identified cultural drivers and barriers between the Federal, State, and local agencies which hinder need or problem resolution?

Personnel

The personnel component primarily ensures that qualified personnel exist to support executing policy and operating systems supporting SNAP and WIC program requirements. This is accomplished through synchronized efforts of State agencies to optimize personnel support at the State and local levels to ensure success of policy and systems supporting SNAP and WIC programs.

- Is the need or problem caused, at least in part, by inability or decreased ability to place qualified and trained personnel in the correct occupational specialties?
- If need or problem resolution is likely to involve new materiel, systems, or equipment, are different occupational specialty codes needed to properly staff new systems?
- Do new personnel have support to onboard to their jobs?
- Are the right personnel in the right positions (skill set match)?

Facilities

Defined as real property consisting of one or more of the following: buildings, structures, utility systems, associated roads and other pavements, and underlying land. Key facilities are defined as headquarters installations and facilities of primary importance to the support of SNAP and WIC programs.

- Is the need or problem caused, at least in part, by inadequate infrastructure?
- Is physical distance of equipment, etc. leading to other problems?
- Are there proper environmental controls?
- Is there a lack of operations and maintenance?



Policy

Policy from any Federal or State agency related to certification, eligibility, benefits, administration, funding, auditing, accountability, security, technology implementation, contracting, acquisitions, or SNAP and WIC program management.

- Is there existing policy that addresses or relates to the business need? Is it Federal? State? Local?
- If no policy exists which pertains to the defined need, does new policy need be developed and implemented that will provide a total or partial solution to the need?
- Can policy be developed and signed at the State agency level? Will policy require USDA-level sponsorship, coordination and / or signature?

When doing the “as-is” needs assessment, doctrine, organization, training, materiel, leadership, personnel, facilities, and policy are assessed for how they constrain the existing processes. During the “to-be” needs assessment, doctrine, organization, training, materiel, leadership, personnel, facilities, and policy are assessed for their impact on the new processes.

5.2.3 Business Capability Definition

The needs assessment begins with defining the needed business capability using business analysis methodologies. (See **Figure 43: Business Capability Definition and the Needs Assessment**, next page) The capability may be necessary to resolve a business or technology problem, fill a gap in supporting SNAP or WIC, respond to policy changes, or take advantage of an opportunity. This means doing a simple root cause analysis. Defining the capability requires establishing the “as-is” state and identifying the desired “to-be” state. Gap analysis determines what is needed and how to make the necessary change to go from the “as-is” to the “to-be.” It involves doing a business needs assessment by evaluating doctrine^{§§§}, organization, training, materiel, leadership, personnel, facilities, and policy. The State agency needs to assess how each of these constrains, supports or promotes the needed capability for both the “as-is” and the “to-be” conditions. This is the basis for establishing high-level outcomes and how the outcomes will be measured for success.

^{§§§} Doctrine is different than policy. It includes strategic plans and objectives for an organization and official objectives for programs such as SNAP, WIC, CNP. Mission statements are one example of doctrine.

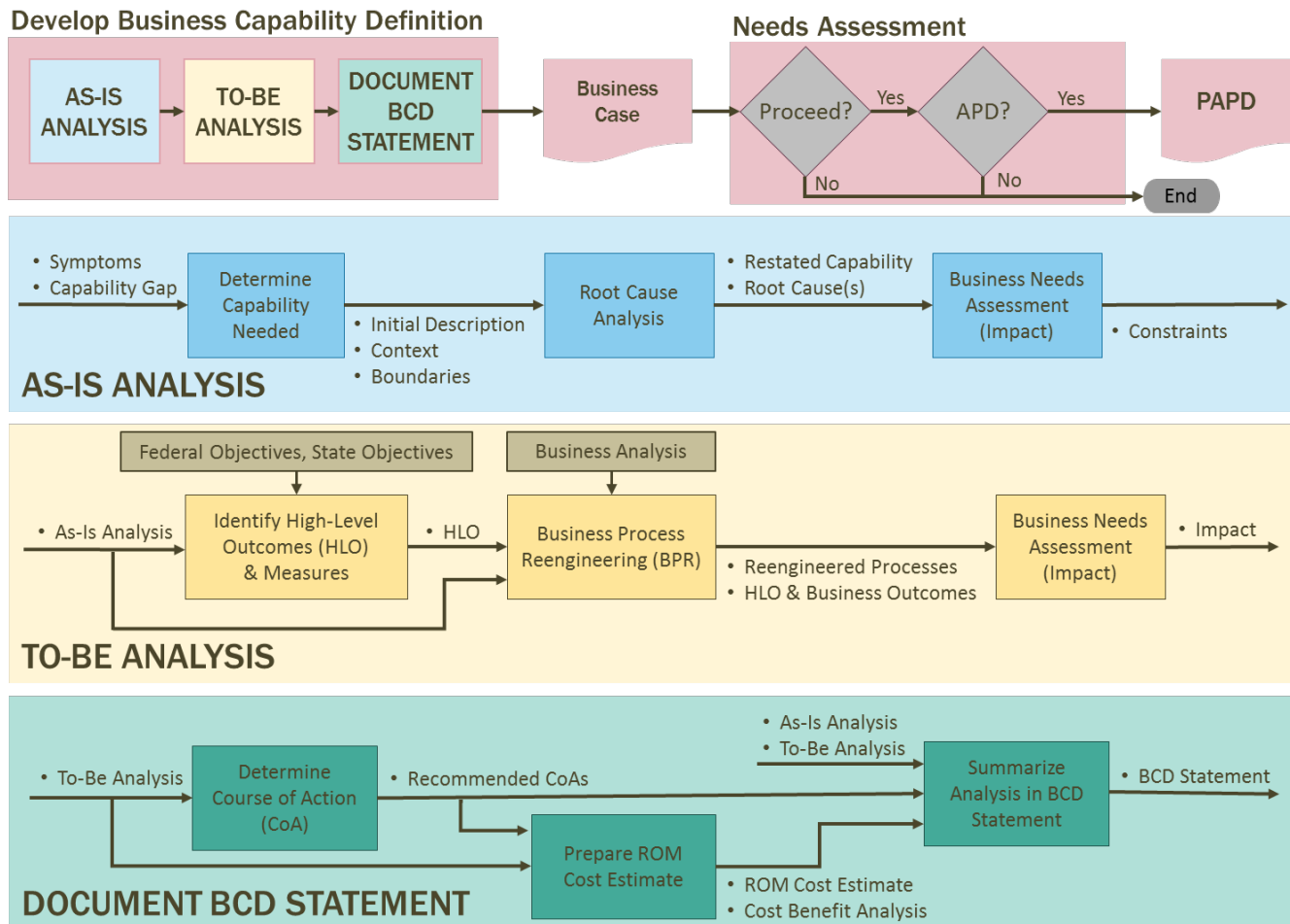


Figure 43: Business Capability Definition and the Needs Assessment

The solution to go from the “as-is” to the “to-be” may or may not require an IT solution. It may be possible to achieve the desired outcomes in other ways. Determining this is based on business analysis. Business analysis should not only validate the high-level outcomes, but provide opportunities for BPR/I. These BPR/I opportunities may become their own courses of action, or be combined with other courses of action to include an IT solution. Each course of action requires its own rough order of magnitude cost estimate. The BCD ends with a summary of the outcomes; in other words, a report commonly known as the business case. Once the BPA process has been completed, the State agency will have defined the “to-be” environment around which all future business should be conducted.

The appropriate State agency authority uses the business case as the basis for making the decision to proceed with the project, or not. If the decision is to proceed, the State agency compares the scope and cost of the proposed project to the FNS thresholds requiring approval, to determine if the APD process applies.



See chapter **1.0 Getting Started with the Advance Planning Document (APD) Process**, section **1.5.1 Thresholds**.

5.2.4 SNAP Program Waivers



Some SNAP IS projects may trigger the need for a program waiver. Where technology is used to supplant or supplement the duties of merit staff, or where communication with applicants or participants changes the way applications are processed, changes are reported, or notices to participants are delivered, States should notify their FNS regional offices to ensure that the new processes are in compliance with SNAP policy or identify what waiver requests might be necessary.

See the SNAP website for information on waivers of rules.^{****} State agencies should keep in mind that tasks involving client contact are restricted to State merit system personnel unless FNS approves use of non-merit or vendor staff to perform certain tasks. This guidance may be found on the SNAP website.^{****}

5.2.5 The Business Case

A well-developed business case provides most of the information needed for the PAPD. The business case is built on the information from the business capabilities definition. It is used by the State agency as the basis for deciding to proceed with the project. It summarizes the key elements for the needs assessment and is a tool for the decision maker to select a course of action based on credible and objective information derived from systematic analysis. The complexity of a business case is driven by the level of confidence the decision maker needs to choose a course of action that will most reliably, and cost effectively, produce the desired outcome. The contents of the business case describe the full range of resources and actions required to reach the stated objectives.

The business case development process should ensure:

- The Business Case concerns the business capabilities and impact, rather than focusing on technical aspects
- An executive with the capability and authority to deliver the benefits, sponsors, and commits to the investment

^{****} <http://www.fns.usda.gov/snap/rules/Waivers/default.htm>

^{****} <http://www.fns.usda.gov/snap/rules/Memo/2010/012210.pdf>

- Thorough consideration and documentation of the required issues
- Clarity of both the value and risks inherent in the proposed solution
- The delivery of the outcomes and benefits can be traced and measured
- Inclusion of all factors relevant to a complete evaluation
- Clearly relevant and logical contents which are simple to evaluate
- Direct justification of key elements in a transparent manner
- Clear accountability and commitment for the delivery of benefits and management of costs

Later, the business case will be used as a starting point to develop more detailed information for the feasibility study that supports the IAPD.

5.2.6 From Business Case to APD

The need for an APD relies on the needs assessment, based on the relationship to dollar thresholds established in law and regulations, types of action/approval sought, program funding source, or type of funding sought. The appropriate State agency decision maker will use the business case from the needs assessment to determine the need for an APD. If the decision is to proceed with the project and request Federal financial participation (FFP), the State agency begins preparing the APD, using information from the business case.



See chapter **3.0 The Advance Planning Document Process** for details on preparing the APD.

5.3 Feasibility Study

Given the complex nature of system development and the interdependence of technical, program, fiscal, and operational considerations, a team approach is recommended. The team may consist of a variety of individuals with different skills and backgrounds (e.g., accounting, budget, program, or IT). Managers, business analysts, system analysts, programmers, and program analysts may also play a role. If the proposed system is integrated with other programs, specialists from those programs may either be included formally or be used on a consultant basis for the team. The size and composition of the team may also depend on the type and complexity of the proposed project. The important factor in the formation of the team is that its size and composition is sufficient to allow a comprehensive, well-coordinated project.

The feasibility study is a tool to help the State agency analyze, compare, and make sound decisions. It is a preliminary study that determines whether the project being considered is technically, financially, and operationally viable. The feasibility study occurs after approval of the PAPD. It builds on the needs assessment,

the initial business case, and the PAPD. It is an integral part of building the IAPD. See **Figure 42** (page 239) for a depiction of the relationship between the Needs Assessment and the Feasibility Study.



For SNAP, the alternatives analysis should assist the State agency to identify any possible need to request a waiver of program requirements.

The feasibility study uses the current system as a baseline to begin the comparative analysis of alternatives. A feasibility study includes three major activities: requirements analysis, alternatives analysis, and cost benefit analysis. Before considering alternatives, the State agency must know what capabilities and functions it needs the alternatives to provide; in other words, the functional requirements of the ideal solution. Alternatives analysis identifies the most likely candidates that can satisfy the scope and requirements for the project. Once a list of alternatives has been established that meet the functional requirements, they must be evaluated for technical, operational, and functional suitability. Alternatives that don't satisfy these needs are eliminated. Finally, the remaining alternatives are compared based on cost to decide which alternatives provide the most benefits. Each of these activities needs to include risk analysis.



The Feasibility Study is a required component of the Implementation Advance Planning Document (IAPD) for SNAP and WIC projects.

The feasibility study identifies the approaches that can be used to meet the program objectives of improved effectiveness and efficiency of operation and administration. The purpose of the feasibility study is not to determine whether it is feasible to build a new system, because the answer can always be "yes." Rather, it needs to determine whether it is feasible to build a State's future system based on the specific State agency's circumstances such as budget and schedule.

The outcome of the feasibility study should identify what system(s) might be functionally, technically, and operationally feasible for the State based on current circumstances and needs. Based on the analysis, there may be more than one feasible system. It may also be possible that none of the options are feasible resulting in a go/no-go point at which the State agency should halt the process and reevaluate the project's direction. **Table 23** provides an overarching synopsis of feasibility study guidelines and related documentation requirements for the IAPD.



See section **3.3.2.3** for related *IAPD Documentation Requirements*.

Table 23: Feasibility Study Guidelines

Content/Issues	Information to be Addressed
General Information	• Provide a brief description of the present system: ○ Is the present system integrated with another public assistance or health system? ○ What is the age of the current system? Does it meet the functional requirements of the program(s)? ○ What Federal, State, and local programs will the new system service? ○ What are the roles of other offices that will be involved (e.g., IT finance, Attorney General's office, other health or human service programs)?
Management Summary	Objectives: • Compliance with regulations • Increased processing speed • Increased productivity and streamlined business processes • Improved IT services • Improved implementation of program policies and decision making Requirements: • Increased capacity (e.g. number of users that may be supported, number of offices, number of mobile sites) • New technical requirements (e.g., a statewide standard) • Improved privacy and security (e.g., must be HIPAA compliant or meet state-specific security standards) • Improvements in management controls Assumptions and Constraints: • Operational life of the proposed system • Availability of information and resources • Financial constraints (e.g., a specific program function was mandated to be completed within a given time frame) • Legislative and policy constraints



Table 23: Feasibility Study Guidelines

Content/Issues	Information to be Addressed
	• Technical constraints (e.g., changing hardware/software/operating environment, new equipment must be compatible with existing) • Operational constraints (e.g., constraints imposed by an outside agency if the proposed system will be integrated with other public assistance programs)
Alternatives Analysis	Methodology: • Identify how the analysis was accomplished and how the alternative system(s) were evaluated • Summarize the general method or strategy employed; such as surveying, weighing, modeling, benchmarking, or simulating Evaluation Criteria: • Identify the criteria to be used to determine the viable system(s); including the relative technical, fiscal, and operational advantages and the ability to meet the system requirements specified in the functional requirements document Alternatives: • Describe each alternative system in terms of methodology and the degree to which it meets the established objectives and evaluation criteria within the framework of the aforementioned constraints • Include alternative systems deemed to be infeasible and specify the reasons for this conclusion (include the alternative analysis elements described in section 5.3.2.1 Minimum Alternatives)
Proposed System(s)	Technical Maturity - Describe the level of technical maturity for the potential solution. The description may address questions such as: • Is the potential solution technically proven or a recent innovation? • Has the proposed technology solution fully matured? • Is it nearing obsolescence? • Are services and expertise required to support the potential technical solution readily available? • What is the estimated lifecycle and longevity of the solution? Equipment Effects: • Describe how new equipment requirements and changes to currently available equipment will be met; for example, do current hardware, telecommunications, and/or network services have the capacity to meet new system requirements



Table 23: Feasibility Study Guidelines

Content/Issues	Information to be Addressed
	Software Effects: • Describe any required additions or modifications needed to existing applications and support software to adapt them to the proposed system(s) and explain how such needs will be met • Describe any data conversion activities that will be necessitated by adoption of the proposed system Organizational Effects: • Describe any organizational, personnel, and skill requirements that will change and how the change will be handled • Program Effects • Describe any conflicts or need to request a waiver (SNAP only) from program requirements • Resource Effects • Management, programmatic, and technical resource requirements • Computer processing resources required to develop, convert, implement, and test the new system(s) • Continued support for current system operations Operational Impacts- How the development process will take into account the effects on operations: • User operating procedures • Operating center procedures • Operating center and user relationships • Telecommunications impacts on the operating center and user sites • Source data processing • Data retention requirements and information storage and retrieval procedures • Output reporting procedures, media, and schedules • System failure consequences and recovery procedures • Plans for system support throughout the system's life Site/Facility Effects: • Describe building modification requirements and how they will be met

Table 23: Feasibility Study Guidelines

Content/Issues	Information to be Addressed
	Fiscal Impacts: - Describe cost factors that may influence the development, design, and continued operation of the proposed system(s) - Identify the estimated total developmental cost and estimated annual operating costs and who will pay for these expenses Justification: - State the reasoning that supports the selection of the proposed system(s) based on the aforementioned evaluation criteria and elimination of other alternatives
Proposed Schedule	- For any alternative still being considered after the alternatives analysis, outline a proposed schedule for all implementation activities; such as systems design, development, testing, quality assurance, data conversion, and deployment and address the following components: - Specific activities to be performed by the user in support of development of the proposed system(s) - Major milestones and management decision points

5.3.1 Requirements Analysis

The feasibility study begins with requirements analysis; State agencies should carefully define their criteria for the new system prior to performing the alternatives analysis. Requirements establish the scope of the technical capabilities needed. High-level objectives identified during the needs assessment are further expanded to include primary requirement needs. The focus is to satisfy the defined business capabilities needed, not build an exhaustive list of every detail of performance and capability. Requirements analysis uses the Functional Requirements Document (FRD) as a baseline to assess the ability of various alternative approaches to meet defined requirements. Requirements need to be of sufficient detail to assess what alternatives are available and capable of meeting the business needs.

Policy Related System Requirements

During systems analysis, the State agency needs to consult applicable FNS policies related to system technical requirements.

- SNAP – Requirements in [7 CFR 272.10\(b\)\(1\), \(b\)\(2\)\(vii\) through \(xiii\), and \(b\)\(3\)](#)
- SNAP – System Integrity Review Tool

- SNAP EBT – “Issuance System Approval Standards” in <https://www.ecfr.gov/current/title-7/subtitle-B/chapter-II/subchapter-C/part-274>
- WIC – Functional Requirements Document (FReD) for a Model WIC Information System^{***}
- WIC EBT – “Food Delivery Systems” in [7 CFR 246.12](https://www.ecfr.gov/current/title-7/subtitle-B/chapter-II/subchapter-C/part-274)



See chapter **9.0 Systems Security** for additional technical requirements based on federal policy.

Requirements analysis involves business analysis, business needs assessment, and systems analysis.

5.3.1.1 Business Analysis

Business analysis is a key activity during requirements analysis. (For more information on business analysis see section **5.2.1**). Inefficient processes should be improved, or reengineered, before requirements are defined. This is especially true if the State agency intends to automate business processes that have been manual prior to the proposed project. BPR/I at this stage will minimize the need for technology customizations in alternative solutions. Customization is expensive. While systems analysis is important during requirements analysis, business analysis should take priority.



Business analysis includes Business Needs Assessment, Business Process Analysis (BPA) and Business Process Reengineering and/or Improvements (BPR/I).

5.3.1.2 Business Needs Assessment

Business needs are initially explored, in a more general way, during needs assessment as part of the business capability definition and related business analysis activities. (See section **5.2**). During the requirements analysis phase of the feasibility study, business needs should be more thoroughly analyzed as part of business needs assessment. The analysis of business needs during the feasibility study is more detailed than during the needs assessment. This is so that the level of detail is sufficient for producing fully defined requirements. This effort will

^{***} <https://www.fns.usda.gov/sites/default/files/apd/FReD-v2.0-Final.pdf>

contribute significantly to fully defining what requires a technology solution versus what can be resolved with BPR/I prior to undertaking a technology solution.

5.3.1.3 Systems Analysis

Systems analysis is more technically oriented than business analysis, and should be performed for the existing system. It is focused on breaking a system down into its component parts and functions; in this case an IT system or database system. The purpose is to establish how all of the component parts interact with each other. Systems analysis activities help define technical interfaces within the system as well as to external systems. Data structures for storing information and exchanging information are analyzed for interoperability. These are all important elements for requirements analysis. System analysis will lead to the generation of accurate technical requirements which ensures that the new system is compatible with the existing system and any additional systems that it must interface with. During systems analysis, State agencies need to refer to FNS requirements for SNAP, WIC, and EBT systems.

5.3.1.4 System Integrity Review Tool Analysis for SNAP



The objective of systems development is to design a system that meets the needs of the user, not just the system specifications. Confirming that the developed system meets all user requirements is the function of user acceptance testing.³⁷ However, the system design requirements are the first step in development; understanding the criteria for testing begins during requirements analysis. If a requirement is not testable, or a required regulatory capability is not part of the design, testing will fail to accomplish its purpose. State agencies are required to develop sufficient automation and to adhere to multiple policies in order to receive federal funding for automation projects. Sufficient automation levels are those that result in effective programs or in cost-effective reductions in errors and improvements in management efficiency.³⁸ FNS has developed a [SNAP System Integrity Review Tool](#)³⁹ to be completed by State staff for review by FNS Regional Office staff, to ensure automation projects adhere to all policy requirements.

The SNAP APD process described at [7 CFR 277.18](#)⁴⁰ states that FNS may conduct reviews of the system either prior to pilot, once it is fully operational statewide, or both. The review may include regulatory and policy requirements, system controls and performance, and system security, among other topics, as its foundation. Although the System Integrity Review Tool is intended to be used prior to User Acceptance Testing, and again after statewide implementation to validate functionality, it is also useful during requirements analysis. State agencies should use this tool as part of their requirements analysis to understand what system capabilities must be considered in the design. FNS will use this same tool for UAT, pilot, and possibly post-implementation reviews.

5.3.1.5 WIC Functional Requirements Document (FReD)



The WIC FReD for a Model WIC IS addresses systems that support a number of WIC program operations and management functions such as certifying applicants, monitoring food vendors, tracking participation and expenditures, and managing appointments. This document also incorporates basic functions for an EBT system. The document is intended to help State agencies prepare the FRD for the IAPD, as well as RFPs for IS services, and to serve as guidance to in-house IT staff developing a WIC IS.



Refer to the [WIC Functional Requirements Document \(FReD\)](#) for details.

5.3.1.6 System Integrity Review Tool Analysis for WIC



The WIC program is subject to the same reviews of the system either prior to UAT, once it is fully operational statewide, or both.⁴¹ FNS has developed two tools for the WIC program for System Integrity Reviews: the [WIC MIS System Integrity Review Tool](#)⁴² and a [Functional Area Spreadsheet](#). The review tool is intended to be used by the State agency during their planning and design stages as a list of data elements and system functions desirable for a WIC MIS. As with SNAP, it is intended to conduct State agency pre- and post-implementation reviews.⁴³

5.3.1.7 Functional Requirements Document

The results of the requirements analysis are documented in a “Functional Requirements Document (FRD)” that is required for the IAPD. Specifications must be based upon a clear and accurate description of the functional requirements for the project. The FRD identifies the requirements analysis and desired system functionality for all aspects of program operations. This is a primary document needed for the alternatives analysis, as well as later SDLC system design activities.

The FRD should include:

- Mandatory – absolute – functionality encompassing Federal and State requirements. This list should not take short-cuts, but be realistic about what is mandatory.
- A list of “nice to have” functionality that may be used as trade-offs when it comes to selecting a best fit alternative. Or, they can become the enhancement list for future projects.

This document serves as a touchstone for the project when defining specifications, providing developers (whether contracted or in-house) with the “what” of the system or enhancement. It serves as guidance to program and IT staff in developing an IS. State agencies are urged to ensure this document is kept up to date as the project progresses, noting decisions or changes to requirements. The FRD is also a reference for testing. When the project is complete, the FRD provides a historical view of the requirements and how they were met with changes noted. The FRD serves as a reference document during operations and maintenance as well.



In competitive procurements, the FRD must not lead to requirements that unduly restrict competition. The FRD assists State agencies in preparing an RFP for development contractors and associated implementation services.

5.3.2 Alternative Analysis

Unless the State agency is introducing new technology or architecture, the primary focus of the feasibility study for FNS systems is the alternatives analysis. A State agency must perform an analysis of representative alternatives for hardware, software, and program functionality to determine the type of system that best meets its needs. The alternatives analysis involves identifying viable candidates to meet the requirements identified in the high-level objectives and technical scope; in other words, the results of the requirements analysis activities. What are alternatives? They can be almost anything the State agency believes is practical for meeting their needs. Alternatives range from modifying current systems to transferring and modifying another State’s system, incorporating off-the-shelf solutions, or initiating custom development when more cost-effective and timely solutions do not exist.

5.3.2.1 Minimum Alternatives

Typically, States use the following four alternatives in their analysis:

- Upgrading or enhancing the existing State system
- Transferring a system or components from another State
- Developing a new system from the ground up
- Cloud computing options ranging from a hosted environment to subscriptions for online products

FNS recommends including a minimum of three alternatives in the analysis, to be sure that the best solution is found. Below are some examples:

Table 24: Minimum Alternatives

Alternatives	Considerations
System Upgrade or Enhancement	State agencies should consider this alternative. If it is not an available option, an explanation of why it is not must be included with the alternative analysis.
Transfer of another State system This may include the entire system, or only some components (best of breed). It is usually appropriate to include systems from more than one other state in the analysis, as they represent different approaches to meeting similar requirements.	Some things to remember when considering a transfer system are: • State agencies need to analyze obstacles to the transfer and modification of an existing system. • Compare the costs of overcoming the problem(s) in transferring an operational system to the costs of developing a new system. • Pay attention to what the cumulative cost of “tweaking” a transfer system may be. State agencies sometimes start with a transfer when they really want a new build. In some cases, transfers can end up costing the same, if not more, than an original build or the original cost of the transfer system. • Is it possible or in the best interest of the program to change/update existing business processes? This may reduce the number of changes required to a transfer system.
Developing or Implementing a new system	Depending on the age of the legacy system, and the technology it is built upon, there may come a point where it cannot be upgraded or enhanced enough to meet new technical standards. Building a new system, or implanting a COTS solution, allows the State agency to consider new innovations, and brings it up-to-date with technology that is sustainable into the future.

All potentially viable alternatives should be included in the analysis. FNS will not accept the results of an alternatives analysis which compares only a pre-selected favorite to clearly non-viable “straw man” options.



Appendix **A4** includes a ***System Type and Acquisition Selection Tool*** to assist State agencies in narrowing down their alternatives.

Alternatives must also include the analysis of technical and programmatic merits of possible system transfers:

- Will existing equipment be usable or will new PCs and/or servers need to be purchased? What about the communications infrastructure - will it support the alternative?
- Are there trade-offs that can be made between technology and business processes? If the business process is changed, will it minimize the potential changes to a system?



WIC must consider a State Agency Model (SAM) system transfer with as little change in functionality as possible, among the alternatives under consideration. (See section **5.3.2.3** for more on SAMs).

In many cases, the most cost-effective alternative is a transfer with minimal changes. Modifying software code is where the biggest development costs occur. This is why complete new builds are rare. However, underestimating the amount of work and/or the number of changes needed to make a transfer system fit the State agency's needs, are some of the major reasons why system transfers have sometimes struggled. It's important to do a thorough and honest assessment of all options and be realistic about the State's needs, constraints, and resources.

FNS will assist State agencies that request assistance in identifying other States with systems that should be considered for possible transfer. State agencies should contact those States with systems in which they are interested, to arrange for the sharing of available software and system documentation within a reasonable timeframe. State agencies need to analyze obstacles to the transfer or modification of an existing system and compare the cumulative costs of overcoming the problem in transferring an operational system, to the costs of developing a new system.

5.3.2.2 Other Alternative Considerations

Platform (or architecture) alternatives range from stand-alone solutions to mainframes, distributed networks, or web-based systems. Requirements for capacity may affect platforms as well as other options.

**Table 25: Alternative Platforms/Capacity Enhancement**

• Architecture • Client/server LAN and micros • Distributed • Web-based • Mainframe • Capacity of current hardware, telecommunications, and network components • Outsourcing (contracting out) • Acquire services (other than equipment) • From other State agencies (central IT) • Commercially • Reconfigure existing resources • Use of non-automated alternatives • Reallocating or re-training personnel • Revising business processes and/or operational flow

Table 26: Labor Alternatives

	Labor Source				
Acquisition Type	Using in-house services	Using contract services	Using combination	Using shared system	Using shared services
Transferring/Modifying Another State's System	•	•	•		
Modifying or Redesigning Current System	•	•	•		
Custom Development	•	•	•		
System Hosting by Another State	•	•	•	•	•

Services include teleprocessing, computer time, electronic mail, voice mail, cellular telephone, and web services. Alternatives include both in-house and contractual solutions, as well as sharing and borrowing resources. Support services include source data entry, training, custom software development, business analysis, systems analysis

and design, software conversion, facilities management, maintenance, equipment operation, network management, studies, and evaluation.

Table 27: Alternatives for Acquiring Services

- Increase or utilize In-House Resources
- In-House Development of Service Capability
- Resource Sharing with Other State Agencies
- Contractual Commercial Services
- Temporary Commercial Services
- Manpower-based
- Project-based
- Full Service, Per Call, On Call
- Temporary Commercial Services

5.3.2.3 WIC State Agency Model Systems (SAM) Alternatives



Regardless of whether a State agency's business case calls for transfer of a SAM, or development or acquisition of a non-SAM WIC IS, approval of a WIC system is accomplished using the APD process. FNS initiated the SAM project to promote the development of model IS for WIC State agencies. Specifically, the SAM initiative supports multi-State consortium efforts to plan, design, and develop model systems and to deploy the models in multiple State agencies. The goals of the project are to increase efficiency and eliminate or significantly reduce cost and duplicative efforts across WIC State agency systems, as well as to ensure that systems meet WIC policy and regulatory requirements.

To optimize its investment, FNS requires SAM systems be considered in the Feasibility Study/Alternatives Analysis. The benefits of transferring a SAM are the following:

- Model system software is already developed
- SAMs are fully functional and EBT-ready
- State agencies may receive priority funding for model system transfer and implementation, as well as some ongoing support costs for SAM Users Groups.

State agencies transferring a model system will maximize their Nutrition Services and Administration (NSA) funds. This is because the cost of software maintenance will be incurred only once and distributed to all States within the model's User Group.



REMEMBER, especially for a WIC SAM transfer using SAM grant funding, FNS anticipates minimal changes to the functionality upon initial transfer.

Under some circumstances, a SAM model may not meet State agency needs. If, after initial evaluation, it is determined that a SAM system is not viable, the State agency may exclude that alternative from further detailed comparison in the Feasibility Study/Alternatives Analysis, as long as valid justification is provided. The justification must demonstrate a good effort on the part of the State agency to consider a SAM system and not dismiss a SAM merely for an unexamined preference.

Examples of acceptable justification include the following:

- All SAMs are inconsistent with State's mandated software/hardware requirements
- A SAM is not compatible with State's needs for an integrated system

If a SAM is selected, the State agency must list and explain in the IAPD any planned or desired modifications to the current "core" code shared by other users of the same system. The extent of the desired modifications is important to demonstrating that the system is a "good fit" as required by the Alternatives Analysis. State agencies transferring a SAM are required to keep enhancements and modifications to a minimum. The State agency's intentions must be made clear in the IAPD.

Changes to the "core" code may be made under only two scenarios:

1. A State agency may choose to transfer the code "as-is" and join the SAM Users Group; submitting its desired changes using the group's change control process after implementation, or
2. A State agency may transfer the code and make the desired changes as a "stand alone" system, without the benefits of Users' Group membership or priority funding considerations.

The WIC program expects that SAM transfers can be done at a minimal or reduced cost. State agencies can implement the system themselves or prepare competitive procurements to hire implementation contractors. Consult with FNS for details on each SAM system.



5.3.2.4 Performing Alternatives Analysis

Gap analysis is the central activity of completing the comparison of alternatives. Each alternative needs to have a gap analysis performed to compare its existing functionality with the State's required functionality. Viable alternatives should be those that best fit the scope and requirements of the project. Cost control is always a key objective. When considering COTS or a system transfer, minimizing the number of changes or customizations will reduce costs. This can dictate the best fit for the State, the budget, and the schedule. The gap analysis is extremely helpful to determine missing or weak functionality in any systems being considered. This also goes for technical requirements of the system. Gap analysis may reveal the need to return to requirements analysis.

The gap analysis answers two critical questions required when selecting the most appropriate system for the State agency's needs:

- How big is the gap between the future vision (the "to-be" scenario) and each of the available options?
- How big is the gap between the starting point (the "as-is" scenario, available budget, and resources) and each of the available options?

The answers to these questions provide these constraints: how much can be spent to complete the system, and the maximum period of time the system must be completed in.

Once the gap analysis is performed for each alternative, then the alternatives may be measured against one another. The best fit solution should become clear. If not, then the alternatives selected and the mandatory and optional requirements may need to be revisited.

The FRD developed for the project during requirements analysis should be used to measure the alternatives. How well do they fit the State's need? If a system transfer is one alternative, get a working version if possible, and the documentation. Perform the analysis to make sure the system will meet the needs. Perform a gap analysis of program functional and technical requirements. It is important to be sure to apply the exact same analysis methodology for each alternative examined. When performing a gap analysis of functionality, include subject matter experts in the discussions and review. Based on the FRD, do all mandatory requirements exist in the alternative? Is the State willing to pay to have them added? Analyze how many changes would be needed for each alternative to meet the needs. Minimal changes are the goal.

The alternatives analysis is a comparison that focuses on **the technical, operational, and functional differences between the alternatives and the requirements.**

Table 28: Gap Analysis

Functional Area	Gap Analysis Considerations
System interfaces (Technical)	• What impacts will the alternative have on any existing systems or interfaces needed to conduct business? • Information verification processes? • Data sharing/exchange capability? • Integration with other State Health Care or Human Services systems?
Personnel and Training (Operational)	• What effect will the alternative have on existing personnel and the skills required? • Will there be an impact on the number of staff required? • Will there be a big learning curve for staff? • Will new staff need to be hired with different skill sets? • How much training will be required to bring current staff up to speed? • Will this system adapt to the State agency's business processes, or can the business processes be adapted to this system?
Data Migration & Conversion (Functional)	• Will data conversion activities add cost to the project? • What about data cleansing? • How much time will it take to reformat the data, add missing elements, etc., both before and after conversion? • How much staff time and cost will be required? • Has sufficient planning been done?

Conducting a thorough gap analysis of all alternatives is vital in assisting the State to determine which alternative is the most viable given the State's needs, schedule, constraints, and assumptions. Once alternatives analysis results are known, the State agency can compare the cost effectiveness and long-term benefits from upgrading its existing system, transferring an existing system from another State, or developing a new system.

5.3.3 Cost Benefit Analysis

Because more than one system may be functionally, technically, and operationally feasible, the State agency needs another tool to help it select the best system. The Cost Benefit Analysis (CBA) is used to estimate the costs for the existing system and each system alternative. It will estimate costs for the nonrecurring (design, development, and implementation) and recurring (operations and maintenance) components of each alternative. This decision-



making tool helps to further narrow the possibilities and arrive at the best system for the State's needs, budget, and circumstances.

The CBA determines which alternative will provide the greatest benefits relative to its costs. The analysis provides, by funding source, the estimated cost of developing and operating each alternative found to be viable through the feasibility study. The analysis identifies the tangible and intangible benefits related to each funding source. The IAPD must show that a meaningful CBA was performed as a part of comparing alternatives. However, it does not require calculating a number of years to the break-even point or tracking and reporting the CBA beyond initial approval of the IAPD. It should:

- Describe cost factors that may influence the development, design, and continued operation of the proposed system(s)
- Identify the estimated total developmental cost and estimated annual operating costs
- Identify funding sources for these expenses
- Determine which alternative will provide the greatest benefits relative to costs

A CBA is required for large-scale software development. It is not required for routine equipment replacement and upgrades. FNS may refuse additional project funding until a State submits a satisfactory CBA that provides the needed justification for proceeding with project implementation.

If the feasibility study includes the system alternative of transferring (usually with modifications) an existing system from another State or jurisdiction, and it is determined feasible, the costs and benefits of transfer must be carefully considered in the analysis. Moreover, if retention of the current system is found to be a feasible alternative, it must also be included in the CBA. **Table 29: CBA Guidelines** provides an overarching synopsis of CBA guidelines and related documentation requirements for the IAPD. A reassessment of a selected alternative or adjustments to requirements, may be triggered by the results of cost analysis.



See section **3.3.2.3** for related ***IAPD Documentation Requirements***.



Appendix **A6** provides a ***Cost Benefit Analysis Worksheet*** to help the State agency document the CBA before preparing the detailed narrative for each system.

Table 29: CBA Guidelines

Content/Issues	Information to be Addressed
General Information	• Identify and define the alternatives



Table 29: CBA Guidelines

Content/Issues	Information to be Addressed
	• State the methodology used for comparing alternative systems as described in the alternatives analysis section of the feasibility study • Document assumptions concerning the alternative systems
Developmental Costs for Each Alternative System	Personnel Costs: • IT Personnel (e.g., programmers; analysts; project leaders; and testing, implementation, and conversion personnel) • Salary plus overhead, including fringe benefits • Training • Database and data preparation, control, and conversion • Software conversion, including all necessary reprogramming • Projected maintenance (during implementation) • Office space requirements • Travel for visits to other States (include airfare, per diem, etc.) • Special one-time expenditures for areas such as conversion and testing • User Personnel (e.g., staff who are directly responsible for the new system and cannot be charged to the IT Personnel category) • Meeting time • Procurement planning and benchmarking • Reviews of the processing system • System testing, evaluation training, and manual preparation • New personnel required; technical or non-technical (permanent or temporary) Equipment and Software Costs: • Communications equipment • Hardware • Physical storage devices • New office space and supplies • Equipment maintenance costs and contracts • Special-purpose software, including system testing tools • Telecommunications equipment and services (e.g., operating center and user sites)



Table 29: CBA Guidelines

Content/Issues	Information to be Addressed
	Other Costs: • Power • Maintenance (e.g., raised floors, additional wiring, air conditioning, etc.) • Supplies (e.g., CDs, paper, ink cartridges, etc.)
Maintenance and Operations Costs	• Personnel (e.g., operations, support, and customer service) • Overhead • Space and off-line equipment • Security and privacy • Supplies and utilities • Processing requirements • Training and education • Travel • Software licenses and maintenance agreements • Maintenance agreements on the new hardware, apportioned to the department as required • Contractual and interagency services; such as IT services, data communications; technical and other support • Additional peripherals needed, such as monitors and storage units • Projected normal maintenance or revisions to the new system (not including correcting initial errors or bugs imbedded in the new system) • Additional operational manuals and offsite training for line and staff personnel • Other current operational costs that will not change with the introduction of the new system, but must be added as part of the total picture
Benefits of the Alternative Systems	Quantifiable: • Describe how the tangible benefits (e.g., cost reduction, value enhancement, leases, rentals, and maintenance) can be measured directly in monetary terms, including benefits that are measured in non-monetary terms (e.g., staff salaries and fringe benefits, travel and training, space occupancy, and direct support services) for which monetary values can be estimated. Place a monetary value on tangible benefits when possible. Express items such as cost reduction, value enhancement, leases, rentals, and maintenance, in dollar terms. Place a dollar estimate on items such as



Table 29: CBA Guidelines

Content/Issues	Information to be Addressed
	staff salaries and fringe benefits, travel and training, space occupancy, and direct support services. Non-quantifiable: Describe the benefits that cannot be quantified in terms of direct dollar values (e.g., improved customer services, faster service, improved office organization and flow, reduced error rates, improved data quality, less demands on retailers, and more accurate reporting). When applicable, include the following components: boundary areas (i.e., analysis of best-case and worst-case estimates to justify the proposed alternative), and/or tradeoffs with tangible benefits (i.e., cases in which an intangible benefit is gained at the expense of a reduced potential tangible benefit).
Comparative Cost/Benefit Summary	Display the costs and benefits of each alternative presented during the expected life of the system (e.g., recurring, non-recurring, system life, residual value, and adjusted costs)
Selected Information System	Document the final decision on the best alternative, considering all costs and benefits

5.4 Technical Planning

5.4.1 Data Conversion & Migration

When implementing a new system, data migration is a significant activity in the SDLC. Planning for data migration should be included in the IAPD. The final test plan must include test cases and scripts demonstrating that data migration was accomplished successfully.

There are two key data management activities during system implementation; data conversion and data migration.

- Data conversion is the **transformation** of computer data from one format to another. Throughout a computer environment, data is encoded in a variety of ways.
- Data migration is the process of **transferring** data between storage types, formats, or computer systems. It is a key consideration for any system implementation, upgrade, or consolidation.

Both of these activities are important when implementing a new system to replace another system. Data conversion is not restricted to situations where the system being replaced is a legacy system. The system's database design and architecture is often the primary reason for converting data, even between modern systems.



Data conversion and migration are a vital part of systems planning. Often this activity is not given the attention it needs, leading to an oversimplified and underfunded approach. Likewise, many new systems fail to meet expectations due to flaws in the conversion and migration processes, because the data was not adequately validated for the intended task. Data conversion and migration should be planned with the same diligence as other systems, planning activities like requirements definition and system testing. Understanding the hidden challenges during systems planning is more likely to deliver accurate data for supporting business needs. It also mitigates risks of delays, budget overruns, and poor data integrity.

Accurate data is essential for getting the most out of enterprise applications. Data conversion and data migration function together to produce useful data. When transferring data to a newly implemented system, data errors and flaws in the data are likely to appear immediately. Data conversion partly solves this problem because the data from the old system is not necessarily in a format compatible with the format in the new system. Additionally, the data in the old system may be adequate for the old system, but not necessarily the new system. The data being migrated needs to be converted to match the structure, content, and intended use in the new system. This requires understanding both the source and target systems data structures and purposes for the data. Without proper analysis, transferring data from a legacy system into a more sophisticated system will magnify the negative impact of any incorrect or irrelevant data. It will also increase risks by perpetuating hidden legacy problems.

Data conversion and migration objectives should include deciding which data is relevant and which is not. Data needed in the older system may not be needed in the new system. Data in the old system also needs to be validated for accuracy before converting and migrating it. Otherwise, inaccuracies will continue to persist and introduce potential risks in data integrity in the new system.

Data Migration Planning must account for several essential activities. State agencies must determine many details when planning data migration. By no means an exhaustive list, but a few considerations include:

- What data needs to be migrated?
- How must the data be prepared for the target system?
- What is the migration strategy; incremental or all at once?
- Are there risks to disrupting source systems and the availability of data during transition to the target system?
- Is there a concurrent period of operation where data will be maintained in both the source system and the target system?
- How will data be synchronized during concurrent operations?
- Which system contains the official record during concurrent operations?

There are many approaches to accomplishing data conversion and migration. Data migration phases include design, extraction, cleansing, load, and verification. Most often it is done using software to achieve an automated migration. Data conversion and migration commonly involves many iterations. Each iteration converts and moves

specific information groups until all of the data is converted and transferred to the new system. Each iteration follows a minimal approach.

1. Design a method for mapping the data on the old system to the new system, and relating the old data formats to the new system's formats and requirements (i.e., conversion)
2. Perform data cleaning to improve data quality, eliminate redundant or obsolete information, and match the requirements of the new system
3. Determine which data must be converted and migrated, and verify the accuracy of the data in the old system
4. Develop a data extraction and data loading procedure to transfer the mapped data from the old system to the new system
5. Load the data into the new system (i.e., migration)
6. Verify and validate the accuracy of the data conversion, completeness, and support for the new system's processes
7. During verification, there may be a need for a parallel run of both systems to identify areas of disparity and forestall erroneous data loss. Verification through parallel processing does not occur during pilot testing, but does occur in earlier project phases.



See chapter **6.0 Test Planning** for additional requirements for data conversion verification and validation.

Data migration requires serious attention and consideration in implementing, upgrading, or enhancing an IS. After all, the purpose of the information system is information management, retrieval, and use to accomplish SNAP and WIC program objectives. If the data is not accurate and correct, negatively impacting certification, eligibility, and issuance of benefits, the system has failed to meet program objectives.

5.4.2 Capacity Planning Study

Capacity studies are of particular importance when a State agency is contemplating making a significant change or upgrade to its major operating platform, network infrastructure, data/telecommunications services, or database management system. Examples include replacing or upgrading the current mainframe and storage hardware, replacing the networking architecture, moving to web services, or changing to a different database management software or structure.

The scope of a capacity study or plan varies depending on the breadth of the project the State agency is undertaking. A software upgrade would not entail a formal study and plan. A new system development would need to include a study of current hardware and telecommunications capacity in order to determine if the current



hardware can meet the requirements of the new system being developed. It is wise to conduct this analysis to realistically evaluate other transfer systems, a bidder's proposal, or project costs (e.g., development, operational, processing, and telecommunications). A new system may often involve significantly more data collection and much more complex storage, use, sharing, and movement of the data than the old system did. Merely looking at the capacity needs of current amount and structure of data is not sufficient. The study provides information that specifies the size and expansion capabilities of the new system or the scope of enhancement to an existing system.

Capacity planning determines the overall size, performance, and resilience of an information system. It relates organizational needs to the system's configurations, to establish a computer installation that adequately meets the organization's projections for growth. Because there are so many variables and intangibles, and because needs change so rapidly, capacity planning is not an exact science. However, various methodologies can be applied to help determine the workload, performance, and costs of the system. A workload model captures the resource demands and workload intensity characteristics of the load brought to the system by the different types of transactions and requests. A performance model is used to predict response times, utilizations, and throughputs as a function of the system description and workload parameters. A cost model accounts for software, hardware, telecommunications, and support expenditures.

The detailed components of the study will vary, depending on the intended usage of the system, but the following factors should be considered:

- Expected storage capacity of the system and the amount of data retrieved, created, and stored within a given cycle
- Number of on-line processes and the estimated likely contention
- Required performance and response required from both the system and the network
- Level of resilience required and the planned cycle of usage (i.e., peaks, troughs, and average)
- Impact of security measures (e.g., encryption and decryption of data)
- Need for 24/7 operations and the acceptability of taking the system down for maintenance and other remedial work

Conducting this task can be very difficult, particularly in predicting the volume of traffic or load conditions. Therefore, many State agencies use contractor support if their staff is not experienced in doing this type of analysis, and specify the capacity study as a requirement in the RFPs when procuring a development contractor. For this scenario, the capacity study is linked to the current processing environment, workload data, and new system environment sections that are commonly part of a statement of work (SOW) for an RFP.

5.4.3 Technical Approach

The State agency should decide on a technical approach for the IS project and conduct appropriate technical planning. The technical approach should consider which system development methodology it prefers or uses as a State agency standard (e.g., waterfall, iterative, spiral, agile, etc.). This decision might be based on vendor proposals if the IS project is going to be contracted, or it may be based on other factors. Technical approach planning is primarily a decision-making process based on the information accumulated during the needs assessment and the feasibility study. This decision will in-turn affect the Plan of Actions and Milestones (POAM) and the initial development schedule. Market research and identification of alternatives will likewise affect these decisions.



A Plan of Action and Milestones (POAM) is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.

From market research, the State agency may have narrowed the alternatives down to a particular methodology that will become a request for proposal requirement. For example, if the State agency determines through its feasibility study that an Agile approach is the preferred development methodology, and that they want a COTS-based solution, these should be stated in the RFP. On the other hand, if the State agency wants to procure a COTS-based solution regardless of development methodology, the schedule may be simply a POAM. Depending on the successful bidder, the specific schedule will be dictated by the selected vendor, based on the vendor's chosen development methodology. This is particularly important over the lifecycle of the system. If the initial implementation of the new system was delivered using a traditional waterfall methodology, the State agency needs to consider the impact that will have on future enhancements and upgrades.

Considerations should include:

- Is an Agile approach to an enhancement compatible with the waterfall methodology being used to manage the systems lifecycle?
- Is a waterfall methodology for an upgrade compatible with a system implemented and managed using Agile?

Although this decision may be long after the IAPD submission, it does not preclude the State agency from preparing a technical approach. Other considerations in the State agency's technical approach include the State's own security standards, governance process, business processes, and resources. By planning for these as part of



the State agency's own technical approach, there is a greater likelihood that the State agency's technical approach will be more effective and compatible with the contractor's proposed approach.

5.5 Considerations

If the project is to upgrade or enhance an existing system, the team should understand the technology capabilities of the existing system at a high-level. This provides the foundation for realistically developing the feasibility study. For example, if the system is built on Service Oriented Architecture (SOA), adding an enhancement or capability might be easier than a system built on a client-server architecture.

If implementing a new IT solution to completely replace a legacy system, understanding current architectures, technologies, and solution models will directly impact design decisions to include requirements. If the new system will be a transfer system, understanding the candidate system's technical design will impact requirements development differently than a COTS or custom built system. The same is true if a Software as a Service (SaaS) or cloud-based system is being considered. Furthermore, understanding FNS priorities for system development related to its FFP stewardship role will most probably provide alternative systems to COTS or custom built systems.

5.5.1 FNS Priority for Transferability and/or Reusability

FNS' primary focus in its support of acquisition and oversight of State systems is to exercise good stewardship of federal funds used to carry out the mission of increasing food security through its domestic nutrition assistance programs. A major objective of FNS' financial stewardship responsibility is to assure that Federal and State Governments do not pay repeatedly for the re-development of desirable systems already implemented with public funds. Transferability and/or reusability of desirable systems between States already produced using public funds is an economical, efficient, effective, and responsible use of financial resources. The responsibility for administering FNS programs and ensuring compliance with federal rules and regulations resides with State agency partners, including Indian Tribal Organizations.

The APD process requires a feasibility study be conducted, including an alternatives analysis that evaluates options for transferring an existing system from another State or jurisdiction. Federal and State participants in the APD process commonly view transferability and/or reusability as a matter of ownership more so than licensing. Transfers and/or the reuse of technology typically pertain to intangible property; for example, software, databases and digital information. They are rendered tangible through the use of computer hardware and electronic devices that enable presentation by outputting to monitors or printed reports. The "right to transfer" and the "ability to transfer" are two major considerations affecting transferability. The ability to transfer is contingent on the right to transfer. The right to transfer is based on technical data rights, covered in chapter **4.0** and appendix **A16**. The ability to transfer, assuming the right to transfer exists, is based on the technology and design of the candidate



system such as the implementation of the principals of modularity through SOA. We focus on the ability to transfer in this section.

5.5.1.1 Technological Transferability and/or Reusability Considerations

Form, fit, and function describes the format characteristics, the functional criteria, and the performance requirements of an IS solution. Function is typically the first factor evaluated in determining the desirability of transferring a component from one State to another. Form and fit parameters are the most common factors affecting the ability to transfer/reuse. Although the functions of the candidate component for transfer/reuse may meet the needs of the requesting State, the technicalities of integrating the component, the format, and the performance characteristics may require modifications to achieve integration in the receiving State's infrastructure.

The ability to transfer/reuse is a technological compatibility issue first and foremost. Implementation of IS supporting SNAP and WIC is typically a combination of numerous integrated component software applications, database systems, information technologies, and system hardware. Implementation is funded using a mixture of State and federal funds, depending on the Program. These systems may include a mixture of COTS and custom components. Assuming that the right to transfer is satisfied, and that the ability to transfer/reuse is possible because the technologies are compatible, isolating a component from a highly integrated infrastructure and system may result in its failure to function in the receiving system. Thus, either new solutions have to be implemented to restore operation, the transferred components have to be significantly altered and customized to make them functional again, or the required components also have to be transferred. Each variant has to be evaluated separately from the original donor solution for feasibility for transfer/reuse and the right to transfer. This impacts the practicality and feasibility assessment, as well as costs.

Traditionally, systems considered for transfer/reuse between States are customized for each State, making them proprietary from a technology standpoint. This customization complicates transfers/reuse because future recipient States may also be required to customize to achieve compatibility with their IT infrastructures. Each customization reduces the degree of technological standardization that would facilitate adopting and implementing the system. State agencies should strive to acquire systems better suited to transferability. The systems are largely self-contained, even when based on commercial enterprise database architectures and commercial programming technologies. The emergence of COTS solutions and their integration into traditional transfer systems has changed the dynamics of transferring these systems to other States and jurisdictions. Whether developing requirements for a new system, or considering a system transfer/ reuse, consider the following technological design principles:

- **Interoperability** – Are the predominant technological architectures of the recipient system or environment compatible with those of the donor system? For example, there may be technological



hurdles to overcome if the donor system is built on .Net Framework & SQL Server whereas the recipient system or environment is based on Java and Oracle.

- **Portability** – Are proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software used in the donor system clearly identifiable and cataloged to facilitate a thorough system analysis and evaluation for interoperability?
- **Supportability** – Are supportability, interoperability, and growth for future modifications easily discernible in the system integration design and operational approach? Do systems components facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems? Does the overall design preclude long-term dependence on closed or proprietary interface standards, technologies, products, or architectures?
- **Scalability** – Is there a detailed description of the donor system addressing a system architecture that incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability?

5.5.1.2 Other Transfer Considerations

FNS expects that all State agencies will help maximize limited funding by supporting system transfers and/or reuse and providing assistance to help others achieve success. The successful transfer/reuse of a system depends upon the ability of the “adopter” State agency to get the software and documentation necessary to fully install, adapt, utilize, and maintain the system. The “donor” State agency may never have anticipated that its system would become a candidate for transfer/reuse and so did not prepare, or ask its contractor to prepare, a defined set of technical resources to support a transfer/reuse.

FNS is aware that State agencies, both “donor” and “adopter”, have struggled with what materiel, exactly, can or should be provided to best support a successful transfer/reuse. Different things are needed at three different points in the process. Initially, a State agency needs access to one set of information in order to conduct a valid alternatives analysis and choose the system that best fits their needs. Having done that, the State agency then needs a different set of materiel to include in their bidders’ library, to provide that level playing field and ensure robust competition. Finally, when a contractor is selected, the State agency needs to provide a complete package of software and materiel to facilitate the transfer and implementation of the system. The following is a recommended list of items that can support all of these activities. State agencies should consult their IT subject matter experts when building this request.

- All the web files and a backup of a database shell
 - with basic lookups
 - security roles



- at least one user with admin access
- Alternatively, a series of database scripts which creates the shell database
 - applicable seed data could be substituted for a database back
 - Instructions for installing
- Detailed Functional Design Document (DFDD)
- Detailed Technical Specifications Document (DTSD)
- Source code
- All forms/ letters/ report templates
- Executable code
- Database schema
- Data Model
- Entity Relational Diagram (ERD)
- Application Architecture Diagrams (AAD)
- Application Server Package
 - installation procedures
 - configuration procedures
 - maintenance and operations support procedures
- Database Server Package
 - installation procedures
 - configuration procedures
 - maintenance and operations support procedures
- Web Server Package
 - installation procedures
 - configuration procedures
 - maintenance and operations support procedures
- Client Installation Package
 - installation procedures
 - configuration procedures
 - maintenance and operations support procedures
- Transfer Package Testing
 - test procedures for transfer
 - test cases/scenarios/scripts for transfer
 - maintenance and operations support procedures
- Database and Conversion Documentation
- Implementation Checklist



- Operations Manual
- Security Features and Configuration Plan
- Software image plan
- Software release notes
- Copies of user manuals
- Copies of training materiel

Ensuring that a State agency owns the software and materiel it has paid for, that it has a useful transfer/reuse package, and that it is able and prepared to share it when needed, begins with the procurement. It is important to put the right language into the Request for Proposals (RFP) or similar document for each of these areas. See chapter **4.0 Procurement** and appendix **A16 Ownership Rights** for detailed guidance on the required and recommended clauses that should be in any RFP, including language to assure State ownership, and the mandatory federal licensing clauses. The State agency should include a specific task and deliverable requiring its contractor to prepare a transfer/reuse package containing the elements listed above. When procuring maintenance and operations services, the State agency should include maintenance and updating of the transfer package as modifications are made to the software or documentation over time. This need not be an extensive effort. The State agency will want system documentation to be kept updated for its own purposes, and will want a current copy of the software always securely backed up. So keeping additional copies for transfer/reuse purposes is only a small extra step.

Finally, a State agency requesting a transfer/reuse package from another has responsibilities too. It's important to remember that it may take time for a "donor" state to pull together the requested materiel, or that all the materiel in the list above may not be readily available for older legacy systems. While FNS expects all State agencies to prepare to share these materiel, the requesting State should take the age and availability of the transfer/reuse package into account when considering and selecting alternatives. A requesting State agency should make its request to the donor state with as much advance notice as possible. Finally, the requesting agency should not assume that a transfer/reuse package comes with technical assistance.

While FNS expects that transfer/reuse materiel will be sound and fully functional, and that all State agencies will support each other and provide assistance whenever possible, some aspects of a transfer/reuse may require technical expertise that the "donor" state does not have, especially if they are no longer supported by a contractor themselves. In its own RFP, an "adopter" state should make it clear that the responsibility is on the winning bidder to ensure successful transfer and implementation. If only the incumbent contractor has the expertise to facilitate a transfer, due to accessibility of the code or other materiel, the State should seriously question the selection of that system for transfer.

5.5.2 Technology and System Capabilities

5.5.2.1 Open Systems Architecture

An Open Systems Architecture (OSA) is both a business and technical strategy for developing a new system or modernizing an existing one. It requires a different mindset than the traditional systems engineering process. One of the key benefits of OSA is that it enables an open and competitive business model. This is possible because OSA allows components to be added, modified, replaced, removed, or supported by different vendors throughout the lifecycle – driving opportunities to enhance competition and innovation.



Open Systems Architecture IS NOT the same as Agile development. OSA is a design principle and is compatible with all development methodologies (i.e., Waterfall, Spiral, Incremental, Agile, etc.). See chapter **2.0 Lifecycle Management** for more information on development methodologies.

OSA is executed during the design of a system and then repeated throughout the life-cycle of that system. It is a means to assess and implement, when feasible, widely supported commercial interface standards in developing systems using modular design concepts.

OSA is an enabler that supports:

- Design for affordable change
- Employment of evolutionary development
- Development and integration of a roadmap for system design and development

Basing design strategies on widely supported open standards increases the chance that future changes will be able to be integrated in a cost effective manner. Designing a system for affordable change requires modularity. Modular design means that functionality is contained in cohesive, well-focused, and well-defined units. Each module is encapsulated, meaning that the internal workings of a module's behavior and its data is "hidden." The modules do not constrain other modules and interact through the use of published interface standards. An evolutionary strategy provides a foundation that meets existing needs while providing the capability to meet evolving requirements. Evolutionary development employs an integrated roadmap as a tool for detailing the strategy to deliver a system that is capable, upgradeable, affordable, and supportable throughout its planned lifecycle. OSA supports achieving the following:



- Reduced acquisition cycle time and overall lifecycle cost
- Ability to insert cutting edge technology as it evolves
- Commonality and reuse of components among systems
- Increased ability to leverage commercial investment

As with any other approach, OSA implementation should be based on upfront planning. To be most effective, the preparations for applying OSA must be initiated early in the program and acquisition planning.

During system planning OSA should be considered, especially when new systems are being implemented. OSA as part of acquisitions is covered in chapter **4.0**, appendix **A10**, and appendix **A16**. OSA is often a key design principle for system adaptability, most frequently seen in systems oriented architectures.

5.5.2.2 System Adaptability

Service Oriented Architectures (SOA) has emerged as the primary enabling approach for system adaptability. SOA provides the means to support legacy applications, to interface with disparate programming technologies, and to support multiple platforms. SOA is neither a system architecture nor a complete system. SOA is a flexible set of design principles used during the phases of systems development and integration, regardless of whether confined to an organization's internal enterprise architecture or for sharing resources and services among organizations. It addresses other distributed capabilities like enterprise architectures, web applications, web services, and mobile applications. The emergence of the Internet and the need for greater portability, scalability, and interoperability fostered the emergence of SOA as a software engineering discipline. SOA is not cloud computing. Cloud computing is frequently developed by applying SOA and the two share many overlapping characteristics. In simplest terms, SOA emphasizes enterprise applications while the cloud computing emphasizes Internet-based services. SOA underlies most modern IT solutions, whether self-contained enterprise solutions, web-based enterprise solutions, or cloud computing.

SOA is often visualized as a collection of services. Services have self-contained functionalities that communicate with each other. When one service needs a function from another service, it sends a request for the service along with the information associated with the request. The target service performs acts on the information and service request and returns the information to the requesting service. Multiple services across all tiers may have to interact in complex ways to deliver the requested service. For example, the service responding to the request may have to call on other services to complete its task. These secondary services may also have to call on other services.

There are shared services such as the presentation of information. There are core functions such as client or customer management. There are specialized services particular to the user community such as retailer management for WIC that does not have a SNAP equivalent. Finally, there are customized services unique to a

particular program. These are all supported by governance services (i.e., business rules) security services, and data management services.

See **Figure 44: Conceptual SNAP or WIC SOA** for a simplified conceptual model of a SOA for certification and eligibility systems such as SNAP or WIC. This figure also illustrates how there may be services other than, for example, SNAP included in one large enterprise system. It is not meant to represent actual systems.

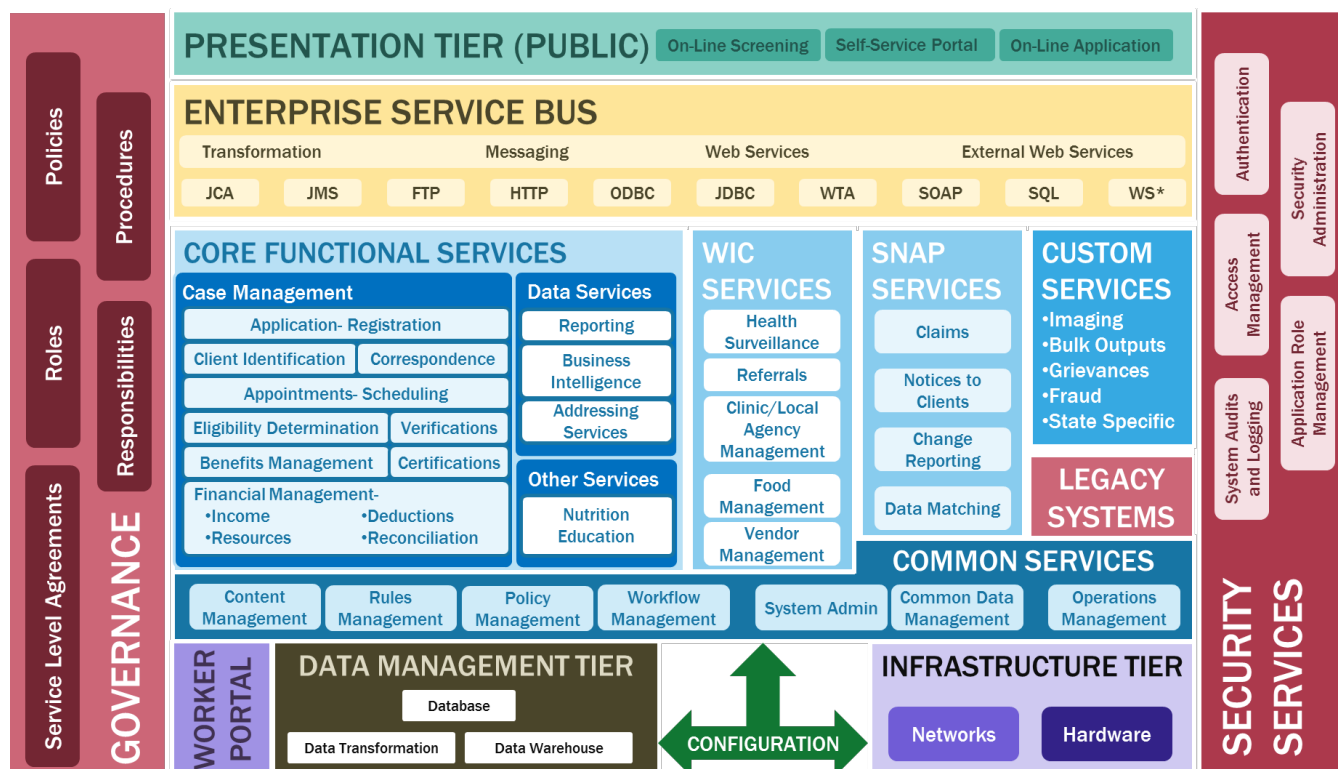


Figure 44: Conceptual SNAP or WIC SOA

5.5.3 Interconnectivity and Legacy Systems

Interfacing and interconnecting legacy systems with modern IT solutions is achieved through a combination of technologies and design principles. The use of data exchanges is becoming more prevalent. The advantage of a data exchange is that several systems with unique data formats connect to the exchange service or application. The data exchange functions as a “translator” for all of the systems so they can communicate with each other rather than having to build a multitude of custom interfaces. The idea of a data exchange is based on a data standard that does not require the interfacing systems to be reengineered or redesigned. It is simply a matter of



conforming to the data standard rather than building a multitude of unique interface adapters. As the premise of data exchanges becomes more prevalent, the cost for interconnecting systems will decline.

SOAs also greatly facilitate interconnectivity with legacy systems. SOA provides a means to integrate systems across organizations, and between organizations, with disparate technologies and services. Central to the SOA concept are services that are available for use within the system. More often than not, engineers start with a business problem and then abstract out the services which can be re-used by other applications in the future. The services are then requested for use by other services within the system. Thus, a legacy system can be “wrapped” as a service that can be called upon by other systems, which are also services. Again, the need for custom interfaces is greatly diminished.

5.5.4 Implementing New Systems

When considering a new system, rather than a transfer, State agencies should be fully aware of the solutions available to them. The best way to accomplish this is to include market research as part of the feasibility study. Market research could be conducted in a number of ways such as researching systems on the Internet, reading product literature, contacting vendors for additional information, and/or issuing Requests for Information (RFI). Using an RFI, though not as effective, is a way to interact with industry, without committing to a solution. Like the other mentioned methods, it is a way to “shop” for what solutions are available. Market research affects how requirements will be organized, expressed, and prioritized. The requirements definition may narrow the list of alternatives from all possible solutions to only those systems based on one of the design models above. Alternatively, it is a way for the State agency to consider all of the models and analyze each for its pros and cons; its risks and benefits; and its scalability and interoperability. However, there are certain solution models that are common among all enterprise-level IT solutions.

5.5.4.1 Considerations for Build vs. Buy

The build versus buy decision is simply about custom development, versus purchasing a solution based on COTS. One of the most significant attributes assigned to COTS-based solutions is the appeal that these can satisfy an organization’s business objectives while at the same time reducing total cost of ownership when applying IT solutions to meet an organization’s business objectives. In theory, COTS should reduce investment, operation, and maintenance costs while at the same time providing necessary functionality to meet an organizations’ needs.

The ease of use, familiarity, and technical servicing of IT solutions should all be improved through the use of COTS products because economies of scale are at work. A widely available product should cost less to obtain, maintain, support, deploy, and adapt to the organization’s needs than a custom solution. However, a COTS product with such broad appeal carries with it certain limitations and risks. At one end of the spectrum (i.e., COTS) is paying for functionality that will never be used. At the other end of the spectrum (i.e., custom built) is paying to have



specialized functionality added to a product to meet the organization's needs. Ideally, enterprise-level COTS tries to balance these two extremes. COTS for enterprise-level solutions often provides a variety of functions and capabilities used by the majority of consumers. To meet an organization's needs to "customize," to satisfy unique requirements, most enterprise-level COTS include configurable functionality. This provides significant capabilities to tailor an enterprise-level COTS solution to an organization's needs without expensive custom programming.

Because COTS encapsulates functionality in a standard, stable, relatively unchanging set of capabilities, the approach to acquiring COTS is different than acquiring a new build or custom system based on a defined set of functional requirements. The approach for acquiring COTS has more emphasis on the functional requirements as a "shopping list" of capabilities for a COTS product, rather than a definition of needs to be provided by the vendor. Using a market research to determine what is available is a good way to build a "shopping list" set of requirements to include in the request for proposal (RFP).

COTS acquisition is no less complex than the process for a new build or a custom solution. Both require business analysis, system engineering, and a detailed process of identifying a suitable provider and solution to meet requirements, whether new build or COTS. Both require planning for the acquisition, selecting and funding it, deploying it, and managing its lifecycle. The difference is the perspective on how to approach and execute the acquisition.

5.5.4.2 Solution Options

Whether a solution is a system transfer, custom built solution, a COTS solution, or a cloud service, there are certain underlying models that enable these solutions. The three primary models are content management systems, business process management systems, and case management frameworks. The leading model for enterprise IT solutions supporting SNAP and WIC systems is Case Management Framework (CMF).

A **Case Management Framework (CMF)** manages the relationships between documents, records, people, and the processes by which they interact using one of several "case" abstractions that best applies to that organization's business. A case management approach is often called for when the application involves processing issues that require a broad range of information, and are handled by a number of different people, and/or take a significant amount of time to complete. As a rule, case management is generally content-driven in the sense that the outcomes of the processes are largely driven by the content associated with the case. These systems include Business Intelligence (Data Analysis and Reporting), Business Logic & Rules Engines, Workflow Management, Data Services, Electronic Records Management, and Security Services.

5.5.4.3 Technology Choices



Cloud or SaaS vs. In-House Hosting

Generally speaking, cloud computing is a broad term used to describe the delivery of computing needs and data storage capacity to a heterogeneous community of end-users, primarily delivered through networked systems. There are three fundamental, high-level services available from cloud computing providers; infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Because cloud computing entrusts services with a user's data, software, and computation over a network, there is a considerable overlap with SaaS. However, SaaS is only one element of cloud computing, even though SaaS is often used interchangeably with cloud computing.



Appendix **A4** includes a ***System Type and Acquisition Selection Tool*** that provides guidance for cloud computing and SaaS options.

Technically speaking, SaaS as a component of cloud computing is most often considered a service provided by a commercial vendor. There are circumstances when SaaS is provided by other government agencies, such as when one State agency operates an eligibility system used by other State agencies. Practical IT solutions are a composite of options that form an overall IT system serving a multitude of interested parties to perform a variety of tasks. This has led to an increasing need for interoperability, scalability, and flexibility for newer computing technologies and software engineering approaches.

In-house hosting carries additional costs and commitment compared to cloud computing provided by a commercial provider. In essence, a State agency may be its own service provider. It must acquire the computer equipment, facilities, hosting software (i.e., server software), and application software (i.e., COTS or custom software). It must also provide for staffing; either with government employees, contractors, or a mix of both. The benefit is greater control of information in the system and flexibility in coping with system outages or service interruption. An additional benefit may be that a State agency could recoup some costs by offering hosting services to other State agencies.

Buying COTS or SaaS

One of the key elements when deciding between SaaS versus COTS is that SaaS is governed by the service agreement. Acquisition strategies for SaaS will focus on acquiring the service whereas procuring COTS is about requirements definition and product delivery. EBT systems are an example of where service agreements are common. In broadest terms, cloud computing is a technology solution where an application or data, which is being utilized by an end user, is not resident on the computing device they are using. It is actually physically stored in a remote location and is accessed as a service via the Internet. SaaS is not the same as a web-based application either, although there are commonalities. A COTS product can be web-enabled, but not be SaaS.



When a SaaS application is provided by a commercial vendor as a commercial product, it inherently shares most of the attributes of traditional COTS software programs. Because the code itself is the same for all users (i.e., the code-base), it is not truly customizable for any individual customer. However, COTS systems are often highly configurable, providing built-in functional options for each customer. SaaS shares many characteristics of traditional COTS software applications, including intellectual property rights.

Characteristics of COTS and Commercial SaaS:

- Encapsulates functionality in a standard, stable, relatively unchanging set of capabilities
- Inherently means that as a product, there is a mass-market product designed for broad user appeal
- Products are developed with functions designed to meet the broadest number of needs for the greatest number of potential users
- Means an acceptance of available features as “good-enough” to satisfy the organization’s business objectives, or adapting business processes to conform to the capabilities of the product
- Protected by intellectual property rights, specifically copyright
- Provide potential cost savings compared to custom-built solutions

5.6 System Planning Summary

System Planning is the primary focus of the activities described in the PAPD. The outcome of the system planning activities is documented as the implementation plan and submitted to FNS in the IAPD.

There are several key points to remember about system planning:

- The State agency must perform a needs assessment as a precursor to submitting the PAPD
 - The needs assessment results in a business case that provides information for whether to proceed with the project or not
 - Determining the need for a Planning APD is based on information generated by the needs assessment and documented in the business case
- The State agency project team should have a basic understanding of several technical considerations before beginning initial system planning
- The Feasibility Study is a required component of the Implementation Advance Planning Document (IAPD) for SNAP and WIC projects
 - A feasibility study includes three major activities: requirements analysis, alternatives analysis, and cost benefit analysis
 - The Alternatives Analysis involves identifying viable candidates to meet the requirements identified in the high-level objectives and technical scope



- Because more than one system may be functionally, technically, and operationally feasible, the State agency needs to do a Cost Benefit Analysis (CBA) to estimate and compare the costs for the existing system and each system alternative
- System planning activities include developing a plan for data conversion and migration, performing a capacity study, and planning the State agency's technical approach
 - Accurate data is essential for getting the most out of enterprise applications. Data conversion and data migration function together to produce useful data. The data being migrated needs to be converted to match the structure, content, and intended use in the new system.
 - Capacity planning determines the overall size, performance, and resilience of an information system. It relates organizational needs to the system's configuration to establish a computer installation that adequately meets the organization's projections for growth.
 - The State agency's technical approach should consider which system development methodology it prefers, which is particularly important over the lifecycle of the system. The State agency needs to consider the impact the technical approach will have on future enhancements and upgrades.
- See **Test Planning (chapter 6.0)** for additional information related to system planning.
 - Requirements analysis during system planning impacts test planning by establishing how each requirement will be tested
 - To be testable, requirements should be clear, precise, and unambiguous
 - This is where requirements analysis and test planning intersect
 - Feedback from test planning should produce better defined requirements that are testable by identifying vague, imprecise, or ambiguous requirement definitions
- See **Systems Security (chapter 9.0)** for additional information related to system planning.
 - System planning for security means developing requirements to protect sensitive information; such as participant data held in eligibility, case management, and benefit delivery systems by State agencies



Endnotes

-
- ³⁷ "SNAP System Integrity Review Tool", U.S. Government, http://www.fns.usda.gov/sites/default/files/apd/SNAP_System_Integrity_Review_Tool.pdf
- ³⁸ "SNAP APD Requirements – General APD Requirements", U.S. Government, <https://www.fns.usda.gov/sso>
- ³⁹ "SNAP System Integrity Review Tool", U.S. Government, http://www.fns.usda.gov/sites/default/files/apd/SNAP_System_Integrity_Review_Tool.pdf
- ⁴⁰ "Basis for continued Federal financial participation", 7 CFR 277.18(g)(2)(i); 7 CFR 277.18(g)(2)(ii); and 7 CFR 277.18(g)(2)(iii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=d832d408500ee17c4fdc9746e9728d4f&mc=true&node=pt7.4.277&rgn=div5#se7.4.277_118
- ⁴¹ "Management evaluation and monitoring reviews", 7 CFR 246.19, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=b6c23b6047c96a32c3f9d2adf4e74f97&mc=true&node=pt7.4.246&rgn=div5#se7.4.246_119
- ⁴² "WIC MIS Integrity Review Tool", U.S. Government, <http://www.fns.usda.gov/apd/wic-mis-integrity-review-tool>
- ⁴³ "WIC MIS System Integrity Review Tool – Introduction – WIC Management Information System (MIS) Integrity Review Tool", U.S. Government, http://www.fns.usda.gov/sites/default/files/apd/WIC_MIS_Integrity_Review_Tool.pdf



6.0 Test Planning

Key Points

The information in this section should allow you to understand the following:

- What are FNS’ minimum requirements for the “Complete and Final Test Plan”?
- What is the relationship between requirements analysis and testing?
- What activities support development of a test plan for SNAP and WIC?
- What are the major contents of a test plan required by FNS?
- How mature must the test plan be for inclusion as part of the IAPD submission?
- When is a “Complete and Final Test Plan” required for delivery to FNS?
- Does FNS require test results be submitted during User Acceptance Testing (UAT) and Pilot testing?
- What is the Go/No-Go document required after UAT and after Pilot?

Chapter Contents

6.1	Introduction.....	290
6.1.1	Test Plan - A General Description	290
6.1.2	FNS Requirements for Testing	291
6.1.3	Required Testing Activities	293
6.1.4	The Complete and Final Test Plan.....	295
6.2	Software Test Lifecycle	298
6.3	Requirements Analysis Phase	299
6.3.1	Planning Requirements Testing	300
6.3.2	Requirements Testability.....	301
6.3.3	Use Cases.....	302
6.3.4	Data Conversion and Migration.....	303
6.4	Test Planning Phase	303
6.4.1	Testing Approach.....	304



6.4.2	Issue and Defect Tracking	307
6.4.3	Resource Determination.....	308
6.4.4	Test Schedule Planning and Milestones	311
6.4.5	Test Risks/Issues.....	313
6.4.6	Test Constraints	314
6.4.7	Go/No-Go Decision Process.....	315
6.5	Test Case Development Phase	317
6.5.1	Items to be Tested	317
6.5.2	Test Cases	318
6.5.3	Test Scenarios / Test Conditions.....	319
6.5.4	Test Scripts	320
6.5.5	Test Data	320
6.5.6	Test Criteria	323
6.5.7	Expected Results.....	323
6.5.8	Error Handling	324
6.5.9	Test Procedures and Progression	324
6.6	Environment Setup Phase.....	324
6.7	Test Execution Phase	325
6.7.1	The Systems Test	326
6.7.2	User Acceptance Test	327
6.7.3	Pilot	328
6.8	Test Cycle Closure Phase.....	329
6.9	Test Lifecycle Support.....	330
6.9.1	Roll Back Contingency Plan.....	330
6.9.2	Quality Assurance.....	330
6.9.3	Independent Verification & Validation	331



6.10	Beyond Rollout	333
6.11	Summary.....	333

Chapter Acronyms

DBMS	Database Management System
EBT	Electronic Benefits Transfer
GCD	Gold Copy Database
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IV&V	Independent Verification and Validation
OS	Operating System
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
QA	Quality Assurance
QC	Quality Control
RTM	Requirements Traceability Matrix
SIRT	System Integrity Review Tool
STLC	Software Testing Lifecycle
UAT	User Acceptance Test or User Acceptance Testing
URL	Uniform Resource Locator
V&V	Verification and Validation



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.

6.1 Introduction

FNS is required to ensure system testing is accomplished when Federal financial participation (FFP) is requested for systems development.⁴⁴ Further, FNS must ensure that all eligibility systems are adequately reviewed and tested. Key objectives are to provide accurate eligibility determinations in accordance with federal regulations and approved State policies and to ensure that system functionality meets requirements. To comply with this regulation, a series of test plan documents is required. These include a preliminary test plan, a “Complete and Final Test Plan,” and Go/No-Go Documents after completing both the User Acceptance Test (UAT) and the Pilot. Throughout this chapter and HB 901 the term “pilot” refers to pilot operations in a live production environment in accordance with FNS regulations.

An important part of the Implementation Advance Planning Document (IAPD) submission is the test plan. This chapter presents the relationship between the IAPD and system testing. It explains the basic concepts for the testing FNS expects State agencies to accomplish in addition to developing the required “Complete and Final Test Plan” for submission prior to proceeding with UAT. It describes the test plan information required in the initial IAPD submission and the “Complete and Final Test Plan” document. Additional sections and components of a good test plan are also described based on best practices.



This chapter uses the term “Complete and Final Test Plan” to distinguish it from the use of “test plan,” which is a general term or refers to the State agency’s comprehensive test plan.

6.1.1 Test Plan - A General Description

In general, a test plan describes what to test, how to test it, and what is needed to verify that the system complies with all program requirements, design specifications, performance standards, usability, capacity, and security. The resources needed for testing should be included in the test plan as a discussion, list, or table. The test plan should address topics such as schedules, hardware, tools, personnel, testing environments, and training needed to support testing.

The State agency should have a comprehensive test plan to cover all FNS requirements for testing. The comprehensive test plan is very detailed and includes more information than is needed for the “Complete and Final Test Plan” to be submitted to FNS. The “Final and Complete Test Plan” is a summary of the comprehensive test plan that demonstrates all requirements will be met. FNS may request additional information when reviewing

the “Complete and Final Test Plan” which should be available from the State agency’s comprehensive test plan. See section 6.1.4 for details on the contents of the “Complete and Final Test Plan.”



This chapter discusses the processes necessary to support developing a comprehensive test plan that can be used to produce the “Complete and Final Test Plan” for FNS review.

6.1.2 FNS Requirements for Testing

Section 4121 of the Food, Conservation, and Energy Act of 2008 reflects Congress’ concern that USDA use the federal approval process to more deliberately review and monitor State agencies’ plans for major system implementations.⁴⁵ State agencies are required to ensure that certification and eligibility systems, and their related EBT systems, are adequately reviewed and tested. Testing is used to confirm that the information system is making accurate eligibility and benefit issuance determinations in accordance with federal regulations and approved State policies. Testing can also help a State agency confirm that the system is compliant with the required functional specifications. To meet this requirement, a State agency must provide a preliminary test plan in its initial IAPD submission and a “Complete and Final Test Plan” prior to the start of the UAT. FNS evaluates the information to determine if the State agency’s plans, methodology, results tracking, and analysis approach are adequate and whether additional information is needed.

The State agency must provide a “Complete and Final Test Plan” to FNS prior to the start of the UAT. Preliminary plans may be submitted based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project. The “Complete and Final Test Plan” itself does not require approval. FNS’ ability to assess the validity of the test results will be dependent upon its earlier review of the “Complete and Final Test Plan.” Failure to submit a “Complete and Final Test Plan” in advance of UAT may result in delays in FNS review and approval of test results. In addition, the State agency must submit the results of completing the System Integrity Review Tool (SIRT) prior to completing the UAT to support the Go/No-Go request. The State agency must assess the results of the UAT and prepare a formal recommendation for a Go/No-Go decision to FNS. FNS’ concurrence is required for continued system development and funding for the Pilot. A similar assessment of results and Go/No-Go recommendation must be submitted to FNS after the Pilot to secure FNS’ approval to proceed to system implementation (i.e., rollout). **Figure 45** depicts these major testing milestones.

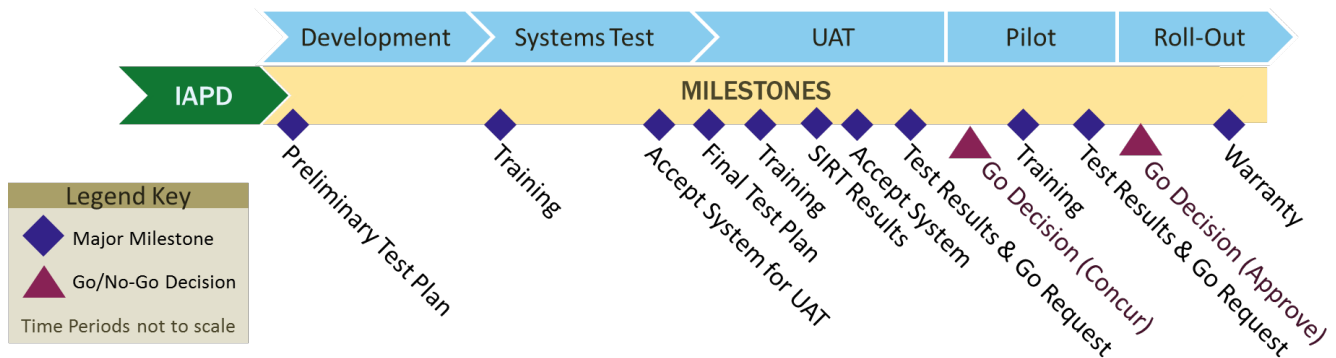


Figure 45: “Complete and Final Test Plan” Milestones

Required IAPD documentation for testing includes:

- Preliminary test plan
 - Is due with the IAPD submission and should address:
 - The State agency’s commitment to conduct the full scope of testing required for a system
 - Assurance that the State agency has enough resources for testing
 - Acknowledgement that the “Complete and Final Test Plan” will include required components and phases specified in [7 CFR 277.18\(g\)\(2\)\(i\)](#) – “Testing” and [7 CFR 277.18\(g\)\(2\)\(ii\)](#) – “Pilot”
 - Preliminary Test schedule for testing, pilot, and decision points appropriate to anticipated methodology
 - High-level overview of State agency’s testing standards or requirements, if they exist
- “Complete and Final Test Plan”
 - Is due prior to User Acceptance Testing
 - Describes the State agency’s plans for testing to accept the system from the developer
 - The organization of the test team and associated responsibilities
 - Test database generation
 - Test schedule
 - Acceptance testing
 - Documentation of test results
 - Go/No-Go criteria
 - Results of System Integrity Review Tool review
 - Contingency planning

See section **6.1.4** for required content.

- A Go/No-Go decision document to advance to Pilot
 - Is due after UAT is complete and prior to Pilot
 - Must provide UAT results and evidence that the State agency’s “go” criteria have been met

See section **6.4.7 Go/No-Go Decision Process** for a list of required contents.

- A Go/No-Go decision document to advance to Implementation (i.e., Rollout)
 - Is due after Pilot is complete and prior to Rollout
 - Must provide pilot evaluation results and evidence that the State agency’s “go” criteria have been met

See section **6.4.7 Go/No-Go Decision Process** for a list of required contents.



A State agency may be required to submit additional results and evidence if performing an incremental statewide implementation. The purpose is to inform FNS and ensure that proper testing continues throughout implementation and that major or critical issues are not exacerbated by continuing to implement prior to resolution.

6.1.3 Required Testing Activities

Testing includes, but is not limited to, unit testing, integration testing, performance testing, end-to-end testing, user acceptance testing, and regression testing. Basic descriptions of each type of required testing⁴⁶ follow:

- **Unit testing** is essentially for verification of the code (or hardware component) produced by individual programmers and is typically done by the programmer of the module. Generally, a module is offered by a programmer for integration and used by other programmers only after it has been successfully unit tested. The unit testing process should be documented in the test plan. Multiple units of code must be completed prior to any integration testing.
- **Integration testing** is the combination of many modules after being unit tested. Multiple modules are combined together into different subsystems, and the subsystems are then tested. The goal here is to see if the modules can be integrated properly. Hence, the emphasis is on testing interfaces between modules. This testing activity can be considered testing the design. An integration test activity is usually on the program schedule as a test milestone.
- **Regression testing** is not a hierarchical-level testing type, but must be planned. Newer systems are often developed in increments or builds. As defects are discovered and repaired, there is a risk that any modification to the software might impact software already developed and tested. To minimize



this risk, regression testing is performed for new builds and when a change or fix has been introduced to the software or environment to verify and validate that previously tested functions and features are still performing correctly. The regression test scripts/cases should be documented and recorded in the test plan and the test schedule should include appropriate flexibility for regression testing. Results of each regression test should be recorded to produce an audit trail demonstrating confidence in the system's performance integrity for the duration of development, implementation, and maintenance.

The next types of testing either require or assume that a full system or prototype is available for the test:

- **End-to-end testing** is more of a configuration task than a test level. A fully functional system or prototype system with all components will be interfaced and tested to ensure that data and communication interfaces work correctly. This is usually done during the final build of the System Test in preparation for the UAT, and prior to the Pilot. End-to-end setup configuration, procedures, and expected results should be incorporated into the "Complete and Final Test Plan" delivered to FNS prior to beginning the UAT.
- A **Performance Test** is used to simulate operations to test limits, ranges, and project whether the system will meet the criteria for sizing, performance, and capacity. This is usually accomplished during the Systems Test and checked again during UAT and the Pilot. Planning for performance testing should be included in the "Complete and Final Test Plan" delivered to FNS prior to beginning the UAT. Common types of performance testing include:
 - Load testing – Checks the application's ability to perform under normal and peak load conditions to verify the application can handle the anticipated number of users.
 - Stress testing – Tests an application under extreme workloads to see how it handles high traffic or data processing. The objective is to push the application beyond normal or peak load conditions to identify its breaking point.
 - Endurance testing – Ensures the software can handle the expected load over a long period of time.
 - Spike testing – Tests the software's reaction to sudden large spikes in the load generated by users.
 - Capacity testing – Determines how many users and/or transactions a given system will support and still meet performance goals.
 - Configuration testing – Tests how running an application in different configuration environments affects the system's performance.
 - Volume testing – Used to check the software system's performance under varying database volumes.
 - Scalability testing – Used to determine the software application's effectiveness in "scaling up" to support an increase in user load.
 - Response time – The time it takes from when a user inputs data into the application until the application outputs a response to that input.



- Bottlenecking – Obstructions in a system caused by faulty code or hardware issues, which create a decrease in throughput (data delivery) that can degrade overall system performance under certain loads.
- The **Systems Test** is when the entire system is tested to ensure that each component of the system, as delivered by the contractor or State agency, operates in accordance with the specifications. This is often a “dry-run” of the system to make sure the system is ready for UAT. All instances of a Systems Test should be planned, documented, and recorded in the State agency’s comprehensive test plan, but is not part of the “Complete and Final Test Plan” submission.
- The **User Acceptance Test (UAT)** is when the system is tested by the State agency as a formal acceptance of the delivered system from the contractor. FNS recommends that business users and State and local users conduct the user acceptance test. UAT is the opportunity for end users to test scenarios specific to day-to-day business operations. The goal of UAT is to assess if the system can support day-to-day business while meeting specified requirements.
- The **Pilot** follows a successful UAT and is a required milestone⁴⁷ in developing an IS supporting SNAP, WIC, and related EBT systems. The duration of the Pilot must be for a sufficient period of time to thoroughly evaluate the system (usually a minimum of three months). State agencies must operate the Pilot until a state of routine operation is reached with a full caseload in the Pilot area. The Pilot reduces the risk to the majority of Program recipients and users until all defects and processes are correct and validated as needed.

Testing should also include Security Testing and Data Conversion Testing.

- **Security Testing** verifies and validates that security requirements⁴⁸ are implemented and effective. The system must have safeguards to prevent unauthorized use (e.g., user identification and authentication), software and data security, and telecommunications security.
- **Data Conversion Testing** verifies and validates that data converted and migrated from the legacy system is accurate and correct. It also verifies and validates data is both transmitted and received correctly when interfacing with external systems. Data conversion testing is a required element of the Pilot⁴⁹, but should be performed much earlier, usually before the Systems Test.

6.1.4 The Complete and Final Test Plan

FNS requires a “Complete and Final Test Plan” prior to proceeding with UAT. This chapter describes the activities required for preparing an effective comprehensive test plan based on FNS testing requirements and industry best practices. The “Complete and Final Test Plan” has very specific content requirements that are based on the details found in the State agency’s comprehensive test plan.



This chapter uses the term “Complete and Final Test Plan” to distinguish it from the use of “test plan,” which is a general term or refers to the State agency’s comprehensive test plan.

The intent of the “Complete and Final Test Plan” requirement is to ensure that the project has a process in place that thoroughly tests all functionality of the new system to mitigate the risks associated with implementation. The “Complete and Final Test Plan” should cover the period that begins when the system is delivered in whole or in part (e.g., builds when using Agile) for testing and ends when the system is fully implemented. This is known as the “testing phase.” Though formal approval is not required, FNS will evaluate the “Complete and Final Test Plan,” may request additional information, and will determine the level and type of FNS oversight based on the project risk factors and the plan itself.

The “Complete and Final Test Plan” should contain, at a minimum, these components:

- Timeline/Milestones – The following milestones need to be scheduled: (See section **6.4.4**)
 - Pre-testing Validation of Functional Requirements (System Integrity Review Tool)
 - System accepted for UAT
 - Training on system and on test procedures
 - User Acceptance Testing
 - UAT Evaluation (FNS concurrence required)
 - Pilot
 - Pilot Evaluation (FNS approval required)
 - Statewide Rollout



The timeline will need to have multiple functional iterations if an Agile development process is being used.

- Testing Resources (see section **6.4.3**)
 - Staffing – The plan should specify the number and skill sets of the staff involved in testing, including:
 - Program/Business Area Staff
 - Development/Integrator Staff
 - Quality Assurance/IV&V Staff

- Test Environment and Equipment – Itemized list to include: (see section **6.4.3.2**)
 - Testing facility(s)
 - Testing tools (software)
 - Equipment (workstations, printers, etc.)
- Roles and Responsibilities – It should specify the what, who, and how for: (see section **6.4.3.2**)
 - Testing management/oversight
 - Testing environment(s) and test database generation
 - Selection of scenarios to test
 - Scripting of scenarios
 - Testing documentation
 - Issue/defect tracking and prioritization (see section **6.4.2**)
 - Defect resolution process (see section **6.4.2**)
 - Regression Testing process (see section **6.1.3**)
 - Evaluation of Test Progression (see section **6.4.1**)
 - Go/No-Go Decisions (see section **6.4.7**)
- Test Approach (see section **6.4.1**)
- Items to be Tested (See section **6.5.1**)
- Roll Back Contingency Plan (see section **6.9.1**)
- Risk Management (see section **6.4.5**)
- System Security (see section **6.1.3**)
- Stress/Load Testing (see section **6.1.3**)
- Data Conversion (if required) (see sections **6.1.3** and **6.3.4**)



Appendix **A15 Final Test Plan Template** provides a template for the “Complete and Final Test Plan.”

FNS’ review of the “Complete and Final Test Plan” will focus on the following information:

- The “Complete and Final Test Plan” should explain how the State agency will test:
 - Support Functionality – It should be clear from the plan that State agency staff in all functional areas /roles within the system will be involved in testing.
 - Data conversion – The plan should indicate multiple test runs to see how the data converts, note data cleanup steps, and specify how success will be measured. This step will provide a realistic idea of the amount of data cleanup required post-conversion.



- System Interfaces - All interfaces should be identified and assessed for their impact. Of utmost importance is the interface to the issuance system. The involvement of the interface partners in the testing process should be addressed.
- Security – The testing of system security is of such great importance that it should be detailed separately in the plan.
- The “Complete and Final Test Plan” should also answer the following questions.
 - Is the test methodology sound?
 - Are testers well trained?
 - Are scripts vetted by the State agency, not just the contractor(s)?
 - Are tests repeatable?
 - Would two people be able to execute the test in the exact same way based on the script?
 - Would two people interpret the script differently, and thus get different results?
 - Are pass/fail criteria for each test clear and unambiguous for the tester?
 - Are test result documentation processes detailed, clear, and specific?
 - Does regression testing allow the failed test scenario or test script to be re-tested using the exact same circumstances?
 - Are testing timelines realistic and include time for FNS review where needed?
 - Are the criteria for the Go/No-go decision specific and measurable?

The remainder of this chapter explains the relevant activities necessary to produce this information based on the Software Test Lifecycle, industry best practices, and FNS testing requirements.

6.2 Software Test Lifecycle

The Software Testing Lifecycle (STLC) is an essential element of the System Development Lifecycle (SDLC). The STLC is critical to achieving software accuracy and reliability through verification and validation (V&V). Software V&V is an extension of sound project management, systems engineering, and system development. SNAP, WIC, and EBT test plans should employ a rigorous methodology to produce objective data and conclusions. This is the basis for providing feedback to the development organization about software quality and performance in terms of system requirements. Within this context, the common objective is to assess and address defects, performance improvements, and quality issues. This applies not only to expected operating conditions, but also across the full spectrum of the system and its interfaces.

Producing reliable software requires rigorous Quality Assurance (QA) during software development. QA is a key software process initiative that prevents the introduction of flaws by ensuring testing procedures are being properly applied and followed by Project staff. Software QA involves the entire software development process: monitoring and improving the process, making sure that any agreed-upon standards and procedures are followed, and ensuring that problems are found and dealt with during development.

The terms “process” and “lifecycle” are often misunderstood and sometimes misapplied. A lifecycle identifies the steps or phases from start to finish of a project, while a process describes the work that happens within each phase of the lifecycle. For example, a testing lifecycle contains phases of Requirements Analysis, Test Planning, Test Case Development, Test Environment setup, Test Execution, and Test Closure. **Figure 46** provides an example of a typical test lifecycle, which will be used in this chapter to explain test planning in detail (sections **6.3 through 6.8**).

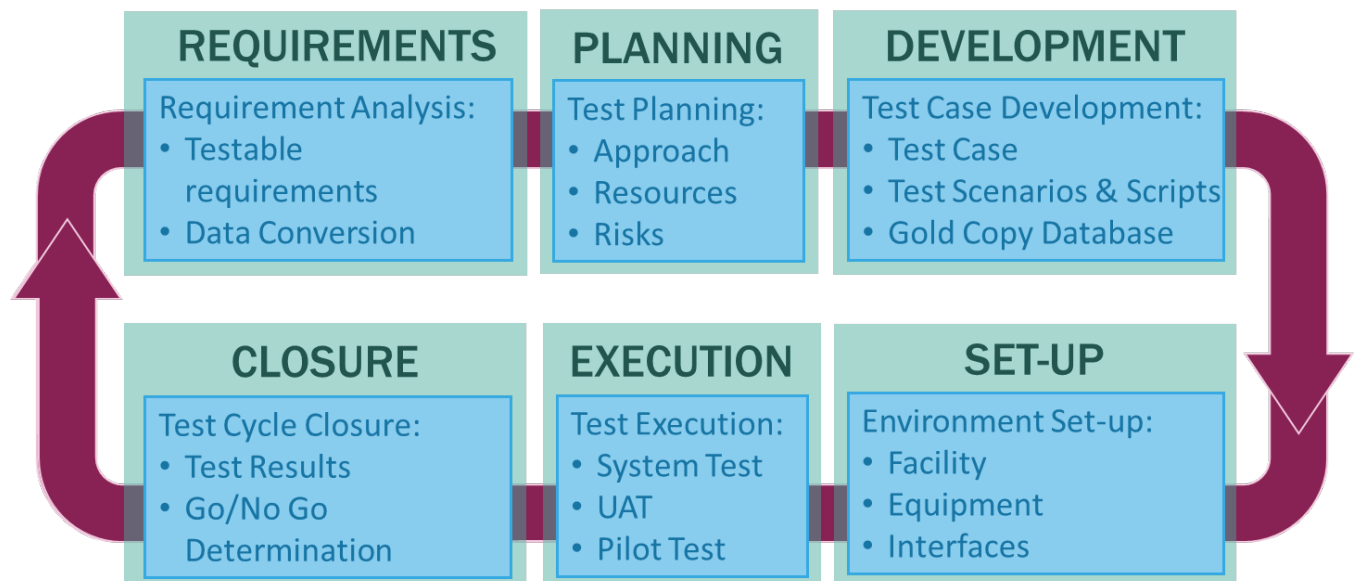


Figure 46: Typical Test Lifecycle

It is common for the test lifecycle to be repeated multiple times during the life of a project. For example, if a server fails during a test session, the Test Environment Setup process, and possibly the Test Execution process, will need repeating. That in turn may require the Test Planning phase to be updated to accommodate the changes required to restore testing capabilities. If the project is an iterative development effort (e.g., Agile), the test lifecycle itself should repeat for every planned iteration and increment.

6.3 Requirements Analysis Phase

Requirements analysis is the complete evaluation of an enterprise and its business operations in order to identify what may be required in an IT system to meet the organization’s needs. It is a task that impacts test planning activities. During **System Planning** (see chapter **5.0**), the requirements analysis phase is conducted by systems and software engineers working with program staff and users to develop specific definitions of system functions and capabilities. Requirements are often assembled into a requirements traceability matrix (RTM) to ensure

implementation and testing activities are performed systematically. The requirements analysis and definition activities should directly interface with the test planning effort to determine the testability of the requirements. Requirements analysis during test planning involves two steps: analyzing the requirements to develop tests for each one and analyzing each requirement for testability.

6.3.1 Planning Requirements Testing

The first step during test planning is to analyze requirements to establish how they will be tested. This is an initial assessment of what is necessary to test each requirement developed during system planning. It is a precursor to developing complete test cases, test scripts, and test data to support testing. Test planning encompasses more than developing tests for technical specifications found in a requirements traceability matrix. It must address building test cases, scenarios, and scripts to evaluate that the IT system fulfills the business and operational needs of the enterprise. Test planning involves collecting the appropriate requirements to consider for test under a variety of conditions (i.e., individually or collectively), from unit testing and functional testing through integration testing, end-to-end testing, Systems Testing, UAT, and Pilot testing. In some cases, individual requirements must be tested, while in other cases, groups of requirements can be tested collectively to verify and validate system capabilities and performance. This is the purpose of analyzing requirements for testing. A system specification is a good first input. However, there are other types of requirements that should be considered for analysis prior to test planning and during test case and test scenario development. Some are included in the following list:

- Customer Requirements/Needs – Statements of facts and assumptions that define expectations of the system. This is an example of where collectively testing requirements is a better means of ensuring the system performs according to the customer’s requirements and expectations. The SNAP and WIC System Integrity Review Tools are valuable resources as a starting point for identifying these requirements and needs.



FNS has developed a checklist of program functions for the SNAP and WIC programs called the System Integrity Review Tool (SIRT). FNS encourages States to use the SIRT prior to and during UAT for checking system functions and capability. FNS will use the SIRT prior to and during UAT and Pilot testing. The SIRT is divided into general program features and subdivided into specific functions/requirements.



See the [SNAP System Integrity Review Tool \(SIRT\)](#) and the [WIC System Integrity Review Tool \(SIRT\)](#) for detailed information.

- Core vs. Ancillary Functionality Requirements:
 - Core requirements are necessary for the product to be useful and support the essential business needs of the customer (e.g., business rules, calculations, data entry validation)
 - Ancillary Requirements are supportive of the core requirements, but not absolutely necessary for product functionality (e.g., look of the interface, safety, user friendliness)
- Performance Requirements – The measurable extent to which a function must be executed, usually measured in terms of meeting technical requirements, quality, coverage, timeliness, readiness, throughput, bandwidth, and connectivity
- Allocated Requirements – Determining which requirements will be fulfilled by hardware or software

6.3.2 Requirements Testability

The second part of the requirements analysis phase is determining the testability of each requirement. A requirement is testable if its function, capability, or purpose can be verified through observable indicators. The test should either pass or fail. To be testable, requirements should be clear, precise, and unambiguous. This is where requirements analysis and test planning intersect. Feedback from test planning should produce better defined requirements that are testable by identifying vague, imprecise, or ambiguous requirement definitions. Without this feedback, a requirement may be implemented, but cannot be verified because of lack of clarity and precision. It is even possible the requirement was implemented in such a way as not to produce the customer's intended function or capability. A requirement becomes untestable when the inability to verify it through observing specific criteria arises. There should be only one way to interpret the requirement.



A project risk should be documented and presented to project management for each requirement that is determined to be not testable. The risk itself is addressed by the use of a contingency plan (mitigation, acceptance, transfer, and others).



6.3.3 Use Cases

State agencies should consider the inclusion of use cases in their requirements analysis phase as a useful tool for assisting test planning for requirements. A use case is a written description of how users will perform tasks using an information system. It outlines, from a user's point of view, a system's behavior as it responds to user requests for information or inputs to the system. Use cases are built around how a system is used to perform business requirements and how the technology supports business processes. Each use case is represented as a sequence of simple steps, beginning with a user's goal and ending when that goal is fulfilled. Use cases add value because they help explain how the system should behave. The use case would contain all system activities that have significance to the users.

Use case analysis is a methodology used in system analysis to identify, clarify, and organize system requirements. When developing use cases, they also help brainstorm what could go wrong. They provide a list of goals and this list can be used to establish the functionality, capabilities, cost, and complexity of the system. A use case is a software modeling technique that defines the features to be implemented and the resolution of any errors that may be encountered.

Use cases support the practical application of the SNAP and WIC SIRTs business operations and system operators. A summary of use case methodology inputs is included in **Table 30**.

Table 300: Use Case Methodology Inputs

1	Demographic data – should have access to the data repository discussed in section 6.5.5 Test Data .
2	SNAP System Integrity Review Tool (7 CFR 272.10)
3	WIC functional requirements ⁵⁰
4	Other business rules – Federal and State
5	Regulatory requirements – Federal and State

Once complete, use cases can be employed during several stages of software development. For example, use cases greatly facilitate planning system requirements, validating design, testing software, and creating an outline for online help and user manuals. They also provide a structured method to ensure that technical requirements and business activities are included for design and test purposes. Finally, they provide an end-to-end perspective for testing activities that goes beyond testing specifications individually. They provide the framework for building test cases and test scripts that reflect how the system is used as a whole rather than collectively testing individual system requirements. Use cases do not replace collective requirements testing, but supplement and enhance those testing procedures. See sections **6.5.1** and **6.5.2** for more on the relationship between use cases and test cases.



6.3.4 Data Conversion and Migration

When implementing a new IS, data from the legacy system will need to be converted from the legacy system's data types to those of the new IS and transferred to the new IS. This process includes activities for preparing the data for conversion, converting the data, and migrating (i.e., transferring) it to the new system. Data conversion plays a major factor in a successful system implementation due to the importance of maintaining data accuracy during the migration and later when interfacing with other systems. Eligibility and Issuance determinations make it imperative that the data is both transmitted and received correctly. Testing the results of the data conversion and migration must be addressed during test planning. There are different types of data (e.g., numeric, text, date and time, etc.) and each IS and database management system technology handles data differently. Consequently, data conversion is linked to requirements analysis, which in turn is linked to the testability of requirements. The State agency should have an approach and a plan for data preparation, conversion, and migration, to include testing to ensure the process produces accurate results.

Data conversion and migration testing should describe how data migration and conversion will be tested. The data conversion and testing approach should contain:

- The basics of how data conversion, migration, and preparation will be done
- The responsible organization for completing and testing the conversion and migration
- The responsible organization for generating and verifying the database
- A data conversion and migration milestone on the project and test schedule
- A milestone for generating a test database for the System Test, the UAT, and Pilot

Once data has been converted and migrated, it should be tested for accuracy as soon as is practical. As the project approaches end-to-end, performance, and system testing, having real data for testing purposes further establishes confidence in the system's accuracy. Actual data, as opposed to test data that is designed to trigger system logic and business rules, may be used as ad hoc test data. See section 6.5.5 for additional information on test data.

6.4 Test Planning Phase

The test planning phase focuses on building overall plans for executing testing. As test planning proceeds and decisions are made, it may be necessary to repeat some earlier planning activities due to decisions made later in the process. Key test planning activities include:

- Developing an overall testing approach compatible with the development methodology (e.g., waterfall, incremental, iterative)
- Defining issue and defect tracking, prioritization, and resolution procedures



- Determining necessary resources to support testing (e.g., support software, test environment, staffing, training needs)
- Deciding on staff roles and responsibilities
- Building a schedule to include major testing milestones (e.g., data conversion, Systems Test, UAT, Pilot)
- Establishing procedures for risks to testing and developing contingency plans
- Identifying testing constraints
- Defining Go/No-Go criteria to proceed from UAT to Pilot and from Pilot to Implementation (i.e., Roll-Out)

6.4.1 Testing Approach

A test approach is the test strategy implementation of a project. The approach should include specifics for each type of testing, such as unit testing, functional testing, integration testing, and so on. It should also include which requirements will be tested individually and which ones will be tested collectively. Objectives for each test should be defined. Developing a testing approach is a blend of different techniques and strategies. No single technique or strategy will provide the necessary comprehensive testing needed to verify and validate any software or IS solution.

There are two common test approach techniques:

- **Proactive:** An approach in which the test design process is initiated as early as possible in order to find and fix the defects before the build is created
- **Reactive:** An approach in which the testing is not started until after design and coding are completed

The testing approach should consider the following factors, some more proactive and others more reactive.

- **Risks:** Risk management is very important during testing, so consider the risks and the level of risk. For a well-established application that is evolving slowly, regression is an important risk, so regression-averse strategies make sense. For a new application, a risk analysis may reveal different risks.
- **Skills:** Consider which skills testers possess and lack because strategies must not only be chosen, they must also be executed.
- **Objectives:** Testing must satisfy the needs and requirements of stakeholders to be successful. The test approach should focus on verifying and validating those objectives are met. This may involve a dynamic approach such as exploratory testing that concentrates on finding as many defects as possible during test execution and adapting to the realities of the system under test.

- **Regulations:** Satisfying regulatory requirements requires a methodical test strategy. A methodical test strategy is based on designing, implementing, and executing tests following an outline based on regulatory requirements. Methodical test strategies adhere to a pre-planned, systematic approach.
- **Product:** Contract-based software development projects tend to have well-specified requirements. This leads to synergy with a requirements-based analytical strategy where an analysis of the requirements specification forms the basis for planning, estimating, and designing tests.
- **Business:** Business considerations and business continuity are often important. A legacy system may serve as a model for a new system for developing an approach to ensure core capabilities produce the same results.

The overall testing approach should establish procedures for how testing will be executed. This includes entry/exit criteria for each type of testing, pass/fail criteria, and conditions for suspending or resuming testing.

6.4.1.1 Entry / Exit Criteria

Entry and exit criteria are part of the comprehensive test plan the State agency must develop to produce a testing approach compatible with the project's IS development methodology (e.g., waterfall, incremental, iterative). For example, in an Agile approach, there should be criteria for beginning testing of each increment (i.e., entry criteria) and criteria for ending testing of each increment (i.e., exit criteria). In Agile development, this may occur multiple times before a system is ready for UAT. In a waterfall approach, the entry and exit criteria may be applied to unit testing, integration testing, end-to-end testing, performance testing, and systems testing. These would occur before a system is ready for UAT.



Entry and exit criteria are not the same as Go/No-Go criteria. Entry and exit criteria are not the basis for getting FNS concurrence, Go/No-Go criteria are. For continued FFP, FNS concurrence is required to proceed from UAT to Pilot. FNS approval is required to proceed from Pilot to Implementation.

In spite of early approval, the project team needs to understand that entry and exit criteria may be subject to changes as the details of the project become clearer. The changes should be managed through established procedures, such as a configuration management plan, a change control board, or both.

Entry criteria are the minimum set of conditions that should be complete in order to start the testing work. Entry criteria are documented and agreed to by the State agency during the test-planning phase and are included in the relevant test plans depending on the development methodology.



Examples of some typical entry criteria include:

- An approved test plan is available
- Approved test cases, test scripts, and test data are available
- All test hardware platforms have been successfully installed, configured, and are functioning properly
- No critical or major severity issues remain from previous testing
- Training has been completed
- Site readiness is completed
- A person is designated with authority to approve the alternative plan or waive the incomplete entry item

If any of the conditions specified in the entry criteria cannot be met, an alternative should be recommended and approved prior to starting the test, or testing should be delayed.

Exit criteria are the minimum set of conditions that must be met to successfully close a particular test event. Exit criteria are documented and agreed to by the State agency during the test planning phase and are included in the relevant test plans. These criteria should be agreed upon as early as possible.

Examples of some typical exit criteria include:

- Successful execution of Test Cases and Test Scripts is complete with an acceptable pass rate
- No open issues exist unless the issue is determined to be low impact and/or low risk
- Open items must be reviewed with Project Manager, Test Manager, and Development Team for acceptable resolution
- A pre-determined acceptable level of requirements coverage has been achieved
- All high-risk areas have been fully tested, with only minor residual risks left outstanding
- Data conversion match rate(s) are within acceptable tolerances

Entry and exit criteria are used for the User Acceptance Test and the Pilot. While these are not the same as Go/No-Go criteria, they are one of the factors used to make a Go/No-Go decision. In other words, the entry and exit criteria are one set of Go/No-Go criteria among many. See section **6.4.7** for more details.

6.4.1.2 Pass / Fail Criteria

Once the testing entrance criteria are satisfied and testing commences, there must be criteria for when test cases and test scripts pass or fail. One of the main exit criteria is successful completion of testing, typically based on tests passing or failing. A test passes if the system responds in a manner as documented in a test case or script's expected results. A test fails if the system does not deliver the expected result in a test step as required by the test script. A test also fails in the event of the system freezing, crashing, or stopping execution while testing, or



refusing to accept or allow the test action. After failure of a test step within a test script, the test as a whole is deemed to have failed.

Any test repeats or restarts should be at the discretion of the Test Manager in coordination with the test committee or relevant decision making team. Any failure is registered as a defect in the defect tracking tool, sent through the error handling process, (see section **6.5.8 Error Handling**) and should be reflected in the test results report.

6.4.1.3 Test Suspension / Resumption Criteria

A test suspension is not the same as a test failure. Section **6.4.1.2 Pass / Fail Criteria** defines the failing criteria for a specific test case or test script. A test suspension defines the criteria for stopping, usually temporarily, all or portions of a test session. A criterion that allows the test session to continue is resumption criteria. The testing approach should include a list of all test suspension criteria and all resumption criteria.

Examples of Suspension Criteria:

- Unavailability of external dependent systems during testing
- When a test case or script fails that prohibits further testing

Examples of Resumption Criteria:

- Any dependent unavailable system becomes available
- The test team is notified a fix is successfully implemented and a patch is ready for installation

6.4.2 Issue and Defect Tracking

When a test case or script fails, the item being tested must be resolved. The failed item or requirement is a defect or issue that must be tracked to a resolution. A defect and an error are not the same. An error is a predicted condition based on incorrect user input, business rules, or data validation routines. A defect is not expected and often means the system has encountered a malfunction. If the resolution involves correcting software programming, the change must be handled in such a way to ensure the change does not cause other problems and that the change is traceable to a root cause. Typically, this is handled through a defect tracking system and a configuration management system that maintains integrity over the source code. Part of the issue and defect tracking involves prioritizing the defect. Prioritization should include severity levels. **Table 31** provides some example severity codes.



Table 31: Example Defect Severity Codes

Severe	Affects accurate determination of eligibility, benefit amount, or has an unacceptable impact on system performance
Priority	Impacts eligibility, benefit amount, or system performance, but a tested workaround is a viable option
Medium	Does not meet system requirements, but does not affect accuracy of eligibility and benefit amount, and the performance impact is acceptable in the short term
Minor	Does not meet system requirements, but the impact is negligible, inconvenient, or cosmetic

6.4.3 Resource Determination

During system development, resources needed for testing are different from those needed for user acceptance testing and the Pilot. All of the resources needed for different testing events must be accounted for and put into place at the right time. Determining what testing resources are needed at what time will impact the testing schedule. The availability of resources may be affected by known workload cycles, holidays, union rules, hiring freezes and other events. The testing schedule should take these constraints into account.

6.4.3.1 Support Software

Support software is needed for the testing but is not a part of the system being tested. Identifying tools should include the name of the product, the version number planned on being used, and its function.

The listing should include tools that provide:

- Systems support
- Communications
- Applications (DBMS, Office Productivity, Requirements Tracking, Server formatting, Internet browser)
- Recording and storage for data and media
- Automated Test Scripts generation
- Configuration Management Software for source code control and integrity
- Defect or Issue Tracking Software



6.4.3.2 Test Environment / Staffing / Training Needs

Test planning for the resources needed to conduct the test is vital to successful testing. If these resources cannot be provided as planned, then either an alternative solution will be required, or a risk to the project should be documented.

A testing environment is a setup of software and hardware on which the testing team will perform the testing of the new IS. This setup consists of the physical hardware setup and the logical setup that includes the server operating system, client operating system, database server, runtime environment, or any other software components required to run the software product to be tested. During any formal test, the test environment should replicate as closely as possible the production system. Any known differences in reliability and performance for items included in the test environment that will be different from the production system must be included in the planning as potential risks. As risks, there should be contingency plans for these elements.

The test plan should include the following:

- The test environment hardware (e.g., computers for testers, printers, projectors, servers, phones, telecommunications equipment, Internet connections, browser name)
- Interfaces to other test systems
- Support Software
- Office supplies (e.g., printer paper, pens, pencils, whiteboards, note pads)
- The facility
 - Space for test participants and equipment
 - Power requirements
 - Air Conditioning requirements
 - Fire and Safety needs
- Furniture (tables, desks, chairs, trashcans, etc.)

Testing requires many people over the course of the project. Planning should identify these people, their roles and responsibilities, and when during the project they will be needed for testing. An organization chart for the entire test team detailing names, organization, and test responsibilities is a very useful tool. This is also the time to identify all test staffing training needs for each test event (e.g., Systems Testing, UAT, Pilot). Participants from the developing contractor, the State agency, local agency, FNS, QA, and other support organizations should be included and details provided if they are more than an observer. For participants, define a role for his or her organization and their responsibilities during the test. Roles should include, but are not limited to, test manager, test analysts, application database administrator, QA, developer representative, application tester, test leads, and customer representative. An example would be **Table 32**.



Table 32: Example of Test Staffing and Training Table

Role	Team Member	Responsibilities	Training Needed
Test Manager	State agency Management (as appropriate)	Provide daily test status. Observe test events. Make intermediate decisions using Suspension/Resumption criteria. Determine Daily Test Schedule	Test Manager training if available. Detailed familiarity with the test environment and design of the software.
Application Test Analyst	Contractor/Developer Team	Test to validate the infrastructure / application for function testing. Perform proper defect tracking (identification, fixing, re-testing and migration of defects). Follow the testing scenarios/scripts, standards, guidelines, and testing methodology as specified in the testing approach. Document outcome of each test. Review test results to validate that they meet the entry and exit criteria.	Training in industry standard testing techniques. Detailed familiarity with the test environment and design of the software.
IT Specialist Subject Matter Expert Super User	State Agency	Test to validate the infrastructure / application for function testing. Perform proper defect tracking (identification, reporting, and re-testing). Follow the testing scenarios/scripts, standards, guidelines, and testing methodology as specified in the testing approach. Document outcome of each test. Review test results to validate that they meet the entry and exit criteria.	Training in industry standard testing techniques. Detailed knowledge of business functions system is supposed to support. Detailed familiarity with the test environment and design of the software.

Table 32: Example of Test Staffing and Training Table

Role	Team Member	Responsibilities	Training Needed
Test Leads	Contractor Team, State Agency staff	Authority and accountability for all work performed by the specific Test Teams (e.g., functional, integration, performance, UAT). Primary responsibility for the Test and Acceptance Plan, Test Cases, Test Scripts and Expected Results, Defect Tracking Report, User Acceptance Test (UAT), Stress Test, Acceptance Reports, and Pilot Acceptance Report deliverables. Serve as the primary contact with the state on testing issues.	Training in industry standard testing techniques. Project Management. Configuration Management. Quality Control. Detailed familiarity with the test environment and design of the software.
Tester	State Agency staff	Document outcome of each test. Review test results to validate that they meet the entry and exit criteria. Follow test scripts, as written, per their training, and document the results.	Training on how to perform test scripts and document outcomes. Training to recognize when a given script succeeds or fails.

6.4.4 Test Schedule Planning and Milestones

Testing involves a multitude of events that need to be scheduled. At the simplest level, the schedule begins as milestones and major testing events during the project. This initial planning is normally submitted with the IAPD. As the test approach planning matures, more details are added to the schedule. Over the course of the STLC, more and more information is assembled into a comprehensive test plan. This includes further developing the schedule. One of the major milestones on the testing schedule is the delivery of the “Complete and Final Test Plan.” When that date arrives, the State agency should have a robust test schedule accounting for all of the testing activities and events, not just the major milestones.

FNS guidance for the minimum set of milestones in the “Complete and Final Test Plan” includes:

- Pre-testing validation of all functional requirements (System Integrity Review Tool)
- System accepted for UAT (meaning that the system meets the State agency’s testing entrance criteria, including passing earlier testing phases conducted by the developer)

- Training on system and on test procedures
- User Acceptance Testing
- UAT Evaluation performed by the State agency (FNS concurrence required) (See section **6.4.7 Go/No-Go Decision Process**)
- Pilot to include data conversion/migration/preparation plan
- Pilot Evaluation performed by the State agency (FNS approval required) (See section **6.4.7 Go/No-Go Decision Process**)
- Statewide Rollout (FNS approval required)

i If an Agile development process is being used, the timeline will need to have multiple functional iterations.

Figure 47 provides an example milestone schedule for a Waterfall type project.

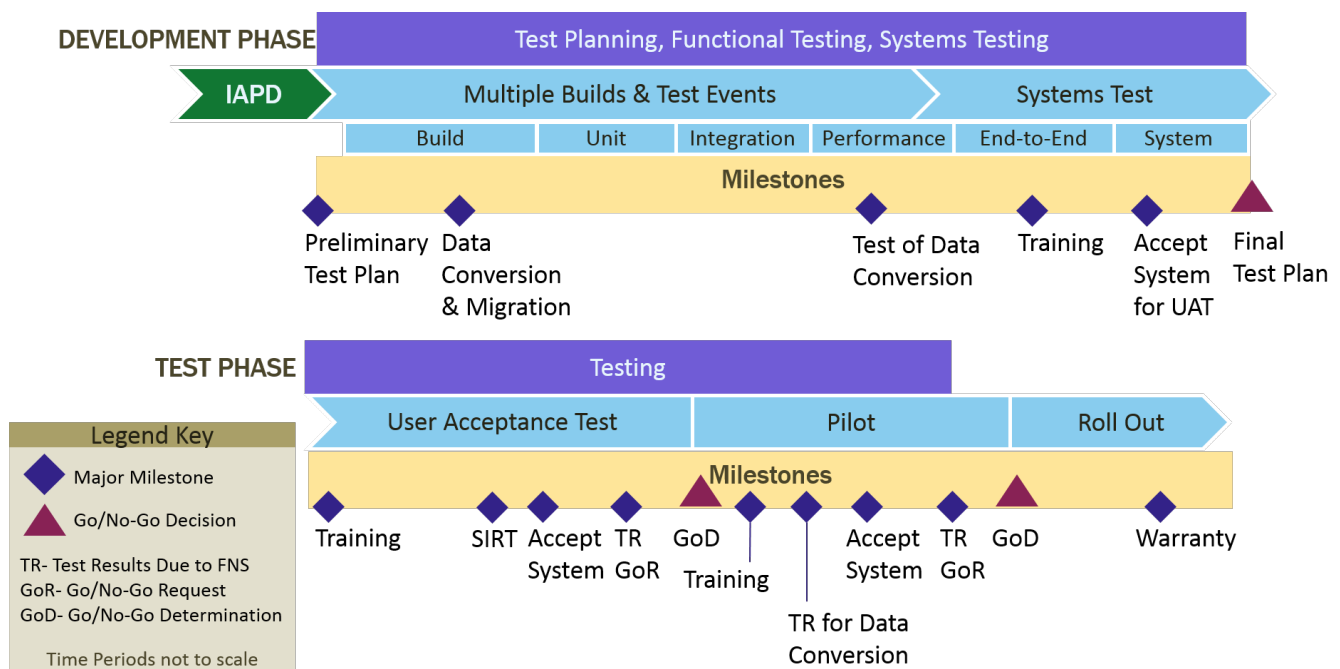


Figure 47: Testing Milestones

6.4.5 Test Risks/Issues

A risk is a possible future unfavorable outcome to a project (cost, schedule, technical). The purpose of a contingency plan (or workaround) is to deal with a risk that becomes an issue. Each risk should have a schedule and associated cost to implement the contingency plan. If the unfavorable event occurs, the risk becomes an issue, or something that is now broken and usually requires a contingency plan.

Risks are generated from many sources but some of the most common areas where test risks can be identified include:

- Requirement Analysis phase if untestable requirements are discovered
- Planning phase if resources needed are not available, not supported, or are at end of life
- Planning phase if training needed is too short, occurs too long before implementation, is not available when needed, or fails to adequately prepare system users
- Planning phase if there are known constraints to testing
- Test Execution phase if entry and exit criteria are not met
- Test Execution phase if there is conflict with available resources

One often overlooked risk is when testing demonstrates that the system is not ready for implementation. The State agency needs to plan for the possibility of an extended delay in the project in which the legacy system must continue to support the SNAP or WIC programs. Another consideration, regardless of how remote it might seem, is the possibility that the system under development is abandoned entirely. The need for the legacy system to remain in place must be planned for in this case as well. (See section **6.9.1** for additional information on the Roll Back Contingency Plan.)



FNS requires a contingency plan for extended delays in implementing a new system, or abandonment of a system under development that provides:

- A strategy to return to the legacy system during conversion or go-live
- The projected time to return to legacy
- An explanation of the impact on the stakeholders

The test plan should provide a list of known risks to the test effort and describe severity level and the management technique for dealing with the risk. If a risk becomes realized, then a contingency plan may have to be set in

motion. An example of a risk and how it would be presented in a test plan can be seen in appendix **A15 Final Test Plan Template**.

6.4.6 Test Constraints

Anything that inhibits a tester’s ability to accomplish their test responsibility, or achieve the testing objectives of test cases and scenarios, is a constraint. This activity comes near the end of developing the test approach so that the test planning team knows as much as possible about their test strategy and all of its elements to identify possible constraints. Done too early, without sufficient approach planning might result in overlooked constraints due to lack of information. In many cases, test constraints will result in risks for testing that must be addressed in the testing risk management plan, as well as the overall project risk management plan.

The most common constraints that inhibit a test effort include:

- Limited schedule and or budget
- Changes in technology
- Limited tester skills
- Limited resources available to complete all testing described in the test plan milestone schedule
- Using incomplete, improper or poorly written test cases

Insufficient testing or “hurry-up” testing (referred to as under-testing) usually occurs as a result of schedule and/or budget constraints to testing.



Lessons learned from industry show that under-testing is directly translated into system defects present in the production system. Each fix costs much more to correct than if the testing was not constrained and problems were identified sooner.

Technological constraints are external to the system being tested, but directly impact the ability to test the system. Because they are external to the system being tested, the test team has little influence over these constraints. Nonetheless, they must recognize that these constraints exist and plan accordingly for them.

Common types of technological constraints to testing include:

- **Integration** - Businesses being unable to operate without computer technology (i.e., loss of connectivity to external system or interface)

- **System Chains** - Systems are interconnected into cycles of chains such that problems in one system can cascade into and affect others
- **The Domino Effect** - A system defect can cause hundreds or even thousands of similar errors within a few minutes
- **Multiple Users** - A defect can no longer be isolated to a single user organization

Testers should be competent in all test knowledge categories to be effective. Lack of the skills needed for a specific test assignment constrains the ability of the testers to effectively complete that assignment.

Resource limitations include funding, people, facilities, equipment, and access to testing environments. Sometimes any or all of these may be due to multiple IT projects within a State competing for limited resources.

6.4.7 Go/No-Go Decision Process

Federal policy requires FNS ensure that all eligibility systems are adequately reviewed and tested. This requires accountability for ensuring test results are satisfactory prior to system implementation as a condition for continued funding. FNS has established two project milestones for a Go/No-Go determination. One milestone is after completion of UAT and the other is after completion of Pilot.



The Go/No-Go determination by the State agency is followed by a formal request to FNS for approval to continue to the next phase of the program. The request is submitted in a UAT results report or Pilot results report, sometimes called a “Go/No-Go Document.” This is required to receive continued FFP. This happens at least twice, once after UAT and once after Pilot. FNS may also request additional results reporting during an incremental implementation.

For each Go/No-Go determination scheduled, the State agency must:

- Generate a Go/No-Go decision document based on test results of
 - UAT (prior to Pilot)
 - Pilot results (prior to rollout)
- Perform a Go/No-Go decision assessment by using
 - Actual test results
 - Expected test results
 - Go/No-Go test criteria and data metrics

- Stated Exit Criteria achieved
- Make a Go/No-Go recommendation
 - Justify items that are on the checklist that did not receive an acceptable rating including recommendations for improvement
 - Send the Go/No-Go document to FNS and formally request concurrence for project continuation

At any point in the system test lifecycle, the State agency or FNS may establish Go/No-Go decision points to assess the project status and determine if continuing is in the best interest of the project. The project should not advance to the next phase requiring a Go/No-Go decision until all criteria are met.

Go/No-Go decision criteria should be specific and measurable and include specific test results that will need to be met before the State agency exits the testing phase. The State agency must identify staff responsible for verifying the criteria have been met supporting the State agency's Go/No-Go decisions.

In spite of early approval, the project team needs to understand that Go/No-Go criteria may be subject to changes as the details of the project become clearer. The changes should be managed through established procedures such as a configuration management plan, a change control board, or both. In the event of a controlled change to the Go/No-Go criteria, the State agency must notify FNS prior to making the change to ensure the impact of the change is analyzed and a decision to proceed is given.

In an effort to stay on schedule, vendors may sometimes rely on UAT to find defects that should have been identified in Systems Testing and fixed prior to UAT. Strong entrance criteria will assure that the system is actually ready for UAT. Emphasis should be placed on Entry/Exit criteria for UAT because these will comprise the basis of the Go/No-Go decision. For a more detailed discussion on the testing Entry/Exit process see section **6.4.1.1**.

FNS encourages the State agency to develop the Go/No-Go document well ahead of the decision date and continually share iterations with FNS.



See the FNS [SNAP Eligibility System Go Live Requirement](#) document and [WIC Go/No-Go Decision Checklist](#) for the Go/No-Go decision items that must be included within a decision package.



6.5 Test Case Development Phase

This phase of the STLC is the time when end user scenarios are determined and incorporated into the tests. Test cases are the top of the software test hierarchy and are usually related to use cases. Where use cases describe the business processes from a user's perspective, test cases describe testing the system's ability to fulfill the purposes of the use cases. (See section **6.3.3 Use Cases**.) The final outcome of the Test Case Development Phase activities culminates in a suite of test cases with procedures for executing them and an orderly progression through testing.

This phase of the STLC is usually worked in parallel with test planning. In fact, most of the results of this phase will be documented and incorporated into the State agency's comprehensive test plan. Test case development involves identifying how to test the requirements, capabilities, and functions to be tested, collectively referred to as "items to be tested." There are several components to a test case. These include test scenarios and conditions, test scripts, test data, test criteria, expected results, and test procedures.

6.5.1 Items to be Tested

A test case is often related to a particular system capability that is given a short title and brief description of what is being tested. Three simple examples would be:

Table 33: Example of a Test Case Table Listing

Test Case Name	Test Case Description
Client Intake	Enter client's application information into system
Client Certification	Certify client's application information
Client Eligibility	Determine client's eligibility

It is easy to recognize these test cases as business processes that might be represented in a use case. When use cases are part of system planning and requirements analysis, multiple requirements may be necessary for the use case to be implemented. (See section **6.3.3** for more information about Use Cases.) Likewise, a test case may be built to verify and validate numerous requirements at one time. If the collective case is tested and passes, it is logical to assume that all of the supporting requirements were implemented correctly and produce the desired capability. Thus, a test case identifies an "item to be tested" in lieu of individually testing the multiple requirements needed to make the capability function. However, there are some requirements that have to be tested individually. Examples would include data elements that went through data conversion and migration; performance and capacity requirements; and internal and external system interfaces. These individual requirements are also "items to be tested" but are more discrete than collective requirements.



“Items to be Tested” is a general term used to describe both collective requirement testing using test cases, and discrete testing for individual requirements.

6.5.2 Test Cases

A Test Case is a collection of test scenarios and test scripts designed to verify the system under test performs as expected. Each test case is related to an item to be tested. Test cases are comprised of test scenarios, test scripts, test data, expected results, related error handling routines, and specific test procedures for progressing through each test case. Testing any IS involves having a suite of test cases to verify and validate the system against requirements. **Figure 48: Test Cases as a Test Case Suite** illustrates the composition of test cases and how several test cases form a suite of test cases for the overall test plan.

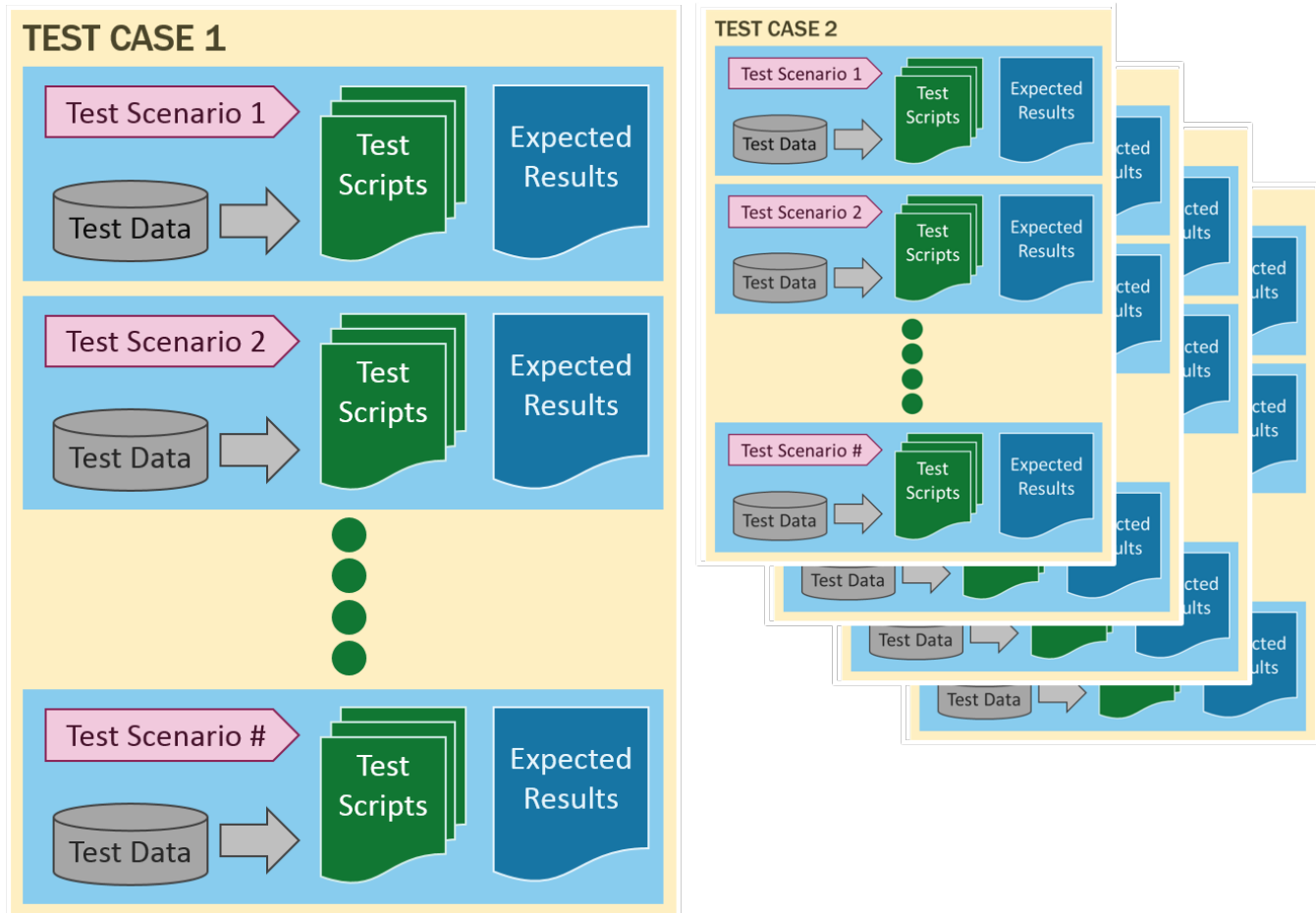


Figure 48: Test Cases as a Test Case Suite

6.5.3 Test Scenarios / Test Conditions

A test scenario is part of a test case that describes any number of possible permutations for how the capability being tested might be handled. Some test cases may have only one scenario while others may have several. The test scenario is a one-line pointer that describes “What” is going to be tested with respect to a certain feature. For example, using the “Client Certification” example from **Table 33: Example of a Test Case Table Listing**, there may be different outcomes for the certification process. Each of these outcomes is a scenario that must be tested. As a result, a single test case may have several test scenarios. A test condition on the other hand is more specific and can be defined as the aim or goal for each scenario. State agencies should consider employing use case methodologies (see sections **6.3.3 - Use Cases** and **6.5.5 - Test Data**) to develop test cases and the related expected results (see section **6.5.7**). Test conditions are different than expected results because expected results



are very detailed, usually for each step in a test script, where the test condition is a description of an overall outcome of the scenario.

Table 34 is an example list of Test Scenarios and Test Conditions based on the “Client Certification” example from **Table 33: Example of a Test Case Table Listing**.

Table 34: Example Test Scenario and Test Conditions Table

Test Scenario	Test Conditions
Client Certification Validated	Application data correctly entered into system <u>without</u> errors
Client Certification Not Validated	Application data correctly entered into system <u>with</u> errors
Client Certification Verified	Application data verified with external system <u>without</u> errors
Client Certification Not Verified	Application data verified with external system <u>with</u> errors

6.5.4 Test Scripts

A Test Script is a sequence of test steps (i.e., set of instructions) designed to verify the system under test performs as expected. Test scripts are often written to be performed manually by a person testing the system and are organized to test each test scenario. Some test cases that are built for testing individual requirements, such as system interfaces, may be automated using a scripting programming language. Test cases for capacity and performance testing may use a semi-automated test script combining manual testing to execute automated scripts following a specific set of procedures and progression. Deciding whether to use manual, semi-automated, automated scripts, or some combination should be based on the item to be tested and the applicable test scenario.

6.5.5 Test Data

Most testing begins by defining prerequisite input data needed to verify a requirement. The test plan should include sets of demographic data useable as standard test data when executing test cases, scenarios, and scripts. Client^{§§§§} cases with different sets of circumstances for receiving benefits should be capable of being saved, queried, and loaded into a test environment. *Ad hoc* data and data queried from the system at the time of testing is inconsistent and randomly selected, making it much more difficult to determine if a problem is in the data or the system programming. However, developing standard test data, which supplements client case data and *ad hoc* data queried from the system, better supports evaluation of testing results. Standard test data provides an effective and consistent way to evaluate a system’s performance. Consistent test data intentionally designed to trigger system logic provides the means to assess whether a system is properly supporting FNS policies. If data is

^{§§§§} In this context, a client is a person seeking SNAP or WIC benefits. It may encompass a household.

consistent and known when a system is not meeting policy requirements, it is easier to isolate the problem to programming logic because the data is a known quantity.



Querying data from the system implies that the data is real information about real people. The accuracy of this data as ad hoc data depends on correct data conversion and validation. Furthermore, this information is subject to the Privacy Act.

Used in conjunction with the use case methodology (see section **6.3.3 Use Cases**), each business functional requirement should be paired with specific demographic data resulting in a unique test scenario with known results. Use cases then become the basis for standard test cases with expected results based on known data designed to trigger system logic supporting the use case. A recommendation for any test effort is to develop a Gold Copy Database (GCD) to use in testing.



'Gold Copy' commonly refers to a copy of the production database that has been migrated into a development, testing, or QA environment and is used as a standard set of data to test with.

A list of common capabilities and characteristics of a GCD are included in the following tables.

Table 35: Gold Copy Database Characteristics

1	A standard set of data used to test functionality
2	Production-like data
3	All the data needed to run tests
4	Enough data to test with repeatedly
5	Up-to-date data
6	All previous data used in earlier testing (e.g., unit testing, integration testing, functional testing, etc.)
7	Links to matching data in other systems

Table 36: Gold Copy Database Capabilities

1	Be able to have automated tests run against it



Table 36: Gold Copy Database Capabilities

2	Protect sets of data so that others can't corrupt or change
3	Capture and store sets of production data that illustrate unusual combinations of information
4	Contain 'bad data' as proof points that program logic works properly
5	Be fully documented
6	Be quickly cloned
7	Contain no Personally Identifiable Information (PII)

The benefit of using a GCD during test is that:

- Standard test data, contained within a GCD as described above, to supplement case data queried from the system and ad hoc data, would support better evaluation of testing results to ensure a State agency is compliant with federal eligibility and issuance policy
- Development of standard test data designed to trigger business rules supporting eligibility and issuance policy would further provide evidence of a State agency's processing of exceptions to household and applicant cases permitted by federal policy. Likewise, "what-if" scenarios could be more readily tested with a preexisting library of test data designed for that purpose
- Business function test cases could be used as an important tool for users of the system to recommend changes to requirements or suggest business processes that need tailoring to accomplish the mission

The plan for test data should describe how data will be controlled for input, how unexpected results will be handled, and how data will be collected and controlled during output.

- **Input Test Data Control:** This should describe the sources for the data input during the test. Specify if control will permit automated data input or test operator data input. Specify if the data is prerequisite (defined prior to the test) or random (invented and input during the test). If random data is not allowed by an operator, make that part of the description. Data input during the test should be monitored by QA.
- **Output Test Data Control:** This should describe how evidence collection and control will be accomplished for the test effort being planned. Output control is usually performed in one of two ways:
 1. Manual collection and collation of system test output into test sequence order, followed by verification of the results
 2. Automatic inspection of test results obtained by data recording means using a test data reduction program followed by manual inspection of selected test results which do not lend themselves to complete test data reduction by automatic means



6.5.6 Test Criteria

Test tolerance and sample criteria are used heavily during performance testing and end-to-end testing. It is used to check system data usage, bandwidth, CPU usage, memory buffer, and system response time.

Test criteria are usually described with several terms that include:

- **Tolerance** – a range of acceptable values obtained in a test result
- **Samples**
 - The number of times a test can be rerun to determine a statistical measure of test results, or
 - The number of times a test will be rerun while changing the number of combinations or alternatives of input conditions
- **System breaks** – any part of the system unexpectedly stops functioning
- **Pass/Fail** – these criteria go hand in hand with tolerance. Any test within tolerance has succeeded in passing the test while any test out of tolerance is a failure

Acceptable test tolerance for the function, feature or item being tested is part of developing each test script. For tests that will specify test criteria, the details of acceptable tolerance ranges should be defined. For tests that will run test samples, the details of the changes in the test conditions for each sample should be described. These are typically summarized in a table or bulleted list. Considering the scope of software testing, some of these factors may not be applicable to the test being conducted (See section **6.5.1 Items to be Tested**).

6.5.7 Expected Results

A test case describes an input, action or event, and an expected result response. *Expected results are not limited to technical and functional specifications only. Expected results also demonstrate system performance according to a requirement or regulation.* State agencies should consider employing use case methodologies to develop test cases and the related expected results. The test plan should provide a description of the expected results for each Item to be tested based on test conditions, test scenarios, and system outputs for each. Expected results should be linked to the underlying specific requirements in a test case, especially when it is a collective test case for many requirements.

Using our Test Case “Client Certification” example from **Table 33: Example of a Test Case Table Listing**, and the related “Client Certification Validated” from **Table 34: Example Test Scenario and Test Conditions Table**, an example of expected results might include:

- When “Submit for Certification” button pushed, no system error messages occurred
- System provided confirmation message from external system used for validating client certification information



- When confirmation message dismissed, field “Certified –Yes/No” indicates “Yes”
- When confirmation message dismissed, field “Date Certified” indicates current calendar date

6.5.8 Error Handling

Errors are different from defects in that they are anticipated and expected system responses to incorrect data entry or events that trigger business rules for incorrect conditions. These are presented to the user as error messages that describe status or limitations on internal performance. As part of developing test cases, the system’s ability to handle errors should be tested with the same attention as testing for correct system functionality. Test cases should describe conditions when errors should occur. This includes the conditions that trigger the error message and the message the system provides to the user explaining what the error is and why it occurred. How to resolve the error should also be explained in the error message.

6.5.9 Test Procedures and Progression

Testing necessitates more than developing test cases, test scenarios, test scripts, and test data. Other types of procedures are needed during formal software testing to ensure completion of testing in an efficient and orderly manner. Procedures for executing the test cases and progress through the suite of test cases is also important. Other testing procedures should include:

- Hardware system setup
- Initialization of the system (hardware, software, tools, applications, data reduction, etc.)
- Preparation for special operations (data dumps, data recording, interim results)
- Test termination and shutdown
- Step-by-step procedures to perform the activities in the test

Most of these procedures should exist in the State agency’s comprehensive test plan and are used during test execution. They should be witnessed by both IT and QA personnel.

6.6 Environment Setup Phase

The test environment is a crucial part of the test lifecycle. (See section **6.4.3.2** for a description of what the Test Environment includes.) The test environment set-up is based on resource requirements established during the test planning phase. Due to its complexities, interfaces, and numerous hardware and tool options available, this phase is often conducted by IT specialists and systems engineers. Prior to the start of the test execution phase, it becomes imperative to ensure that several activities have been completed. The test environment phase becomes critical, as these tasks must allow for:

- Equipment definition approval and purchasing (if applicable)
- System assembly and integration
- Test Environment readiness testing
- Test Environment use procedure development (see section **6.5.9 Test Procedures**)
- User training

All of the above efforts must be completed prior to the start of the test execution phase. The testing environment should be available, configured for test, checked out, and scheduled for testing. Last, all test participants and observers should be thoroughly familiar with the operational capabilities of the test facility. This applies even when the test team members are not directly involved with the integration of the test environment. Test environment setup milestones that need to be scheduled include:

- Test environment definition (included facility, interfaces, security)
- For each type of test: development, integration, System Test, and UAT
 - Test environment procurement
 - Test environment integration
 - Test environment checkout
 - Test environment training

6.7 Test Execution Phase

All of the activities during the earlier STLC phases were related to planning and preparing to test. Over the course of the IS' development, testing will be executed for unit testing, integration testing, performance testing, end-to-end testing, and Systems Testing. These testing events should all be on the State agency's testing schedule and are required prerequisites to entering the "Testing Phase."



For purposes of [7 CFR 277.18\(g\)\(2\)\(i\)](#) and HB901, the "Testing Phase" is a general term used to describe testing that occurs during the User Acceptance Test and the Pilot. The "Complete and Final Test Plan" is specific to the "Testing Phase" events, which is the basis of the required content for the "Complete and Final Test Plan."

The test process in **Figure 49** depicts the basic test execution process. This is repeated many times during test execution as the unit testing, integration testing, functional testing, system testing, regression testing, UAT, and the Pilot activities are accomplished. Prior to the start of the "Testing Phase," this testing is typically done by the developer and implementation team. Reporting is internal to the State agency and is not a deliverable to FNS.

This does not relieve the State agency of maintaining good test records. FNS may request additional testing information from testing completed during system design, development, implementation, and operations.⁵¹

1. **Test Preparation** – Scheduling resources, training as needed, test environment set-up
4. **Test Execution** – Executing the test plan, cases, scenarios, scripts
5. **Results Analysis** – Analyze results and report defects
6. **Defect Tracking** – Analyze defects and track through resolution and re-testing
7. **Reporting** – Documenting test results to inform upcoming test cycles and regression testing
8. **Test Plan Updates** – Update the test plan, cases, scenarios, scripts to reflect changes and lessons learned.



Figure 49: Testing Process

6.7.1 The Systems Test

The Systems Test is the developer's and State agency's final preparation for the User's Acceptance Test. One major objective of the Systems Test is to ensure the best possible system is available for UAT. Since the Systems Test is preparing for UAT, the test should be conducted, as much as feasible, in a user environment where simulated or real target platforms and infrastructures are used. At a minimum, this environment should be separate from the development and production environments. It should mirror, or be as identical as possible to, the production environment.

A thorough Systems Test will include:

- Functional tests (Inputs from the unit and integration tests conducted during requirements verification including Eligibility, Issuance, and Notice verification)
- Data Conversion Testing (file formats, data formats, parity)
- End-to-End testing (system interfaces, communication and data transfer between systems,)
- Performance testing (Stress testing, load testing, bandwidth capacity)
- Regression testing (ripple effects of defect corrections and new code affecting existing code)
- Security tests (identification and authentication, sign on, passwords, personal client data)

FNS may request results from the System Integration Testing (SIT) as part of UAT as evidence of rigorous regression testing that resolved defects and errors before UAT proceeded.

6.7.2 User Acceptance Test



DO NOT begin UAT activities until a “Complete and Final Test Plan” is submitted to FNS.

This test will be a repeat of the Systems Test (see section **6.7.1 The Systems Test.**), but how it will be performed is a key difference. The contractor development and implementation team must not perform UAT testing. This provides a new set of testers who concentrate on validation rather than verification done by testers during system design, development, and implementation. Furthermore, testers for UAT should include State and local agency/clinic personnel who will be operating the system when it is rolled out. The primary purpose of UAT is to determine whether the system satisfies acceptance criteria, and to enable the users to determine whether or not to accept the system.

The testing methodology must be rigorous and results must be documented thoroughly. If defects are identified in the system’s functionality or performance, the fixes the developer makes to the system to resolve these defects should be retested with close attention paid to regression test results. Only when these conditions are met can testing be considered adequate to demonstrate that the system is ready for Pilot. Once UAT is executed, a “Go/No-Go” assessment is conducted by the State agency. The State agency analyzes UAT results and compares them against expected results, test metrics, and predetermined criteria. This is the basis for the State agency recommending a Go/No-Go decision be made to proceed to Pilot. The test assessment, test results, and recommendation become a formal Go/No-Go decision document and are sent to FNS with a formal request for concurrence to move to Pilot and for continued funding. (See section **6.4.7 Go/No-Go Decision Process** for additional information.)

UAT milestones on the test schedule include:

- Pre-testing validation of functional requirements (System Integrity Review Tool)
- Accepting system for UAT
- Training on system and on test procedures
- UAT
- UAT results evaluation (FNS concurrence required)
- Pilot
- Pilot Evaluation (FNS approval required)
- Statewide rollout



The following documents are deliverable to FNS as a result of this test.

- UAT Test Plan (If modified since last shared with FNS)
 - UAT Test Procedures
 - UAT Test Cases and Scripts (upon request)
 - UAT Report on Open Risks
- UAT Test Results and Report
 - UAT Report on failures with severity levels

6.7.3 Pilot

The Pilot is a transitional milestone in project development and occurs after a successful UAT. In a Pilot, the system goes live for a reduced population of users. These users will be operating with a fully functional system in a live environment. If a legacy system exists, the State is encouraged to continue to run client data through the legacy system in parallel with live operations in the pilot area, and then compare the results, to further validate the accuracy of the new system.

Keep in mind, a Pilot is important for more than just providing a trial run for the computer system. It is a time to test the system in an operational environment to detect problems prior to full implementation. Problems can be fixed and the system regressively tested to ensure the fixes did not cause unintended consequences. It is also an opportunity for State agencies to determine and ensure that all stakeholders (e.g., recipients and State/local staff) can successfully navigate the system, the State agency's approach to training is effective, and any program and system interfaces are effective.

Sufficient time must be built into the Pilot to thoroughly test all system functionality and to evaluate Pilot results. While State agencies will continue to have latitude in choosing the Pilot site(s), they should consider how well the Pilot's caseload represents the demands on the operational system.

The duration of the pilot must be for a sufficient period of time to thoroughly evaluate the system (usually a minimum duration of three months). The Pilot should include such factors as:

- The size of the Pilot
- The rate of phase-in of the Pilot caseload
- The track record (defects, changes, restarts) of the system being implemented

When a contractor is used for system development, the contract should specify that the State agency's approval of the Pilot results is a condition of project continuation. This provision ensures that State agencies have control of the development process. Pilot testing is performed by the State agency. The development and implementation contractor may still be supporting the Pilot by correcting defects found during the Pilot. However,



the contractor may not participate in the Pilot. To do so would be a conflict of interest. FNS may monitor the Pilot test in person to corroborate the findings of the State agency. If the State agency intends to use an independent contractor for testing, those roles and activities must be reflected in the “Complete and Final Test Plan.”

Documentation of the Pilot results and a formal Go/No-Go document must be provided to FNS for approval with the decision to proceed with implementation (i.e., rollout) (see section **6.4.7 Go/No-Go Decision Process**). It is also a condition to continue to receive federal funding.

The Pilot report list of recommended results includes:

- An itemization of the Pilot goals in progress or achieved
- The number of cases processed in the new system
- The total universe of defects going into Pilot by severity level
- The number of new defects by severity level identified during Pilot
- The number of defects by severity level resolved and successfully regression tested
- The number of defects outstanding by severity level
- The results of the conversion to Pilot and the management strategy for any post-conversion clean-up work that will be required as a result of the Pilot
- A sign off by the interface partners assuring that they are satisfied with the functionality of the interfaces
- Other pertinent readiness issues (i.e. network, facility, equipment readiness, training)
- During a phased rollout **FNS** may **elect to** evaluate performance region by region
- The State agency’s strategy to prepare a region that has particularly poor performance

6.8 Test Cycle Closure Phase

The Test Cycle Closure activity wraps up testing for the current iteration. During development and implementation, the unit, integration, end-to-end, and performance testing will eventually end. These testing activities need to be formally closed as part of the STLC. Closure of these activities is an internal State agency activity, and should be recorded appropriately. Some of this information may be provided to FNS as part of Pilot results or upon request. Test metrics will be reviewed together with the test results and selected project status indicators to form the basis of proceeding to the Systems Test and for continued system operation. (See section **6.4.7** for additional Go/No-Go information.)

In addition to the test results for UAT or Pilot, other information reviewed and considered for a Go/No-Go decision includes:

- Exit criteria completeness
- Risk data and status
- Test coverage conducted (test case completeness, test case results versus expectations)
- Cost and time to test
- Business objectives completed
- Areas for improvement, lessons learned
- Defect severity levels documented

6.9 Test Lifecycle Support

6.9.1 Roll Back Contingency Plan

A decision may have to be made to stop testing based on the number and severity of the defects or problems identified. The amount of time needed to fix the defect(s) is also a significant factor if it means tying up testing resources for an unacceptable period. A further decision will have to be made to reschedule testing or to consider options as severe as restarting or ending the project.

The Roll Back Contingency Plan should:

- Explain the strategy if it is necessary to roll back to the legacy system
- Project how long that decision to roll back can be delayed if things go badly
- Explain the impact to stakeholders of a rollback

This roll back contingency plan is included as part of the Go/No-Go decision document for UAT and Pilot.



See section **6.4.7** for more information on the Go/No-Go process, [the FNS SNAP Eligibility System Go Live Requirements](#), and [WIC Go/No-Go Decision Checklist](#) on the FNS public website.

6.9.2 Quality Assurance

Quality Assurance is a continuous management process that must take place throughout all phases of the project lifecycle, including testing. QA is the responsibility of the State agency and may be accomplished using State resources. However, many State agencies use contractor resources to perform QA activities if State resources are not available. All QA resources must be separated organizationally from the development and implementation



resources to provide objectivity. Regardless of who actually assumes QA duties, they should be objective and empowered to point out if either party, State agency or contractor, is not fulfilling its responsibilities or achieving agreed upon results.

FNS expects State agencies to establish a planning and monitoring process as a condition of project approval for the development of State automation projects. **Table 37** lists additional QA functions related to testing.

Table 37: QA Interface with the Test Lifecycle

Activity	Responsibilities
Ensure Adequate Reviews Conducted	Review all deliverables to ensure that they meet contractual requirements, as well as State expectations
	Verify and document that the system adequately meets all FNS and State requirements
	Validate review findings with users and stakeholders
	Participate in internal system tests before user acceptance testing
Continuously Monitor Actions and Timelines	Monitor milestone schedule, accomplishments, and timelines to ensure that project is on track
	Monitor and determine impact of new guidelines, requirements, and outside influences on planning and procurement processes
Ensure Open and Regular Communication	Help establish robust communication processes among key stakeholders

6.9.3 Independent Verification & Validation

Definitions of the terms verification and validation at times are hard to simplify. The Institute of Electrical and Electronics Engineers (IEEE) Computer Society uses the terminology defined by the Project Management Institute (PMI)⁵²:

- **Verification:** The evaluation of whether or not a product, service, or system, complies with regulations, requirement, specification, or imposed condition. It is often an internal process.
- **Validation:** The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers.

The key difference is that one process is an “internal evaluation” and the other process provides an “external assurance.”



IV&V is a process performed by an organization that is technically, managerially, and financially independent of the development organization. It provides management with an independent perspective on project activities and promotes early detection of project and product variances. This process should not be confused with QA although it is very similar to QA except for three main differences. The first is that QA resides within the project while IV&V does not, and secondly, QA personnel are project management oriented while IV&V staffs are systems engineering oriented.

The last difference is the amount of project coordination conducted. While not a “hard and fast rule,” in QA, there is often extensive collaboration during the course of deliverables review and testing. This QA collaboration involves not only identifying problems but also working with the project team to solve the problems. IV&V conclusions usually result in a report identifying problems and recommended ways to address the deficiencies. It is then the project team’s responsibility to resolve the deficiencies without the assistance of the IV&V team.

If a State agency contracts for an IV&V effort, there are several model entry points as seen in **Table 38**.

Table 38: IV&V Typical Task Models

Model Type	IV&V Tasks	Advantage	Disadvantage
Prior to Contract	- Independent assessment of a vendor’s proposed approach - Review of the proposed contract	- Inexpensive - Project receives help at critical start up point	No further examination during the lifecycle
Targeted	IV&V team is engaged at the beginning of the project and performs V&V efforts only at specific key point or at pre-agreed intervals (e.g., test deliveries)	Costs are incurred only at the target points	Difficult for IV&V vendor to maintain product continuity from one target point to the next
Full	IV&V team is added at the beginning of the project and performs its efforts on a day to day basis for the duration of the project	- An independent set of eyes performing standard management reviews and analysis - Error detection and prevention discovered earlier in the lifecycle	Most expensive
End of Project	IV&V effort is performed only at the end of the effort to provide final review, audit, and approval to go live	Relatively inexpensive	Any errors detected at this point are the most expensive to fix

Notwithstanding the cost of an additional set of eyes on the test process, effective IV&V does increase the odds of the following:

- Objectivity with test decisions (scalability, testability, usability, etc.)
- Earlier detection of errors reducing the cost to fix the defect
- Technical analysis for root causes of defects and eliminating errors

6.10 Beyond Rollout

Assuming a successful system rollout, and with a warranty in place, the system should be considered in an operational and maintenance (M&O) phase.



A post-implementation review (generally 6 months after rollout) conducted by the State agency and/or FNS is optional.

Software, hardware, and interfaces will continue to change and be updated throughout the life of the system. Testing does not end with system implementation. It continues throughout the system's lifecycle. Changes, upgrades, fixes to problems discovered during M&O need to be tested with the same discipline as during development. Thus, State agencies should have a test plan for the M&O phase of SDLC that makes use of testing activities similar to those used prior to and during implementation. If changes during M&O exceed certain thresholds, a new APD may be required. (See chapter **3.0 The Advance Planning Document Process** for additional guidance.) Each time a test session is scheduled with the intent of releasing an updated product, best practice concepts of test planning, executing, documenting, and reporting should continue with both State agency and FNS oversight and involvement.

6.11 Test Planning Summary

- The State agency must provide a preliminary test plan in its initial IAPD submission and a "Complete and Final Test Plan" prior to the start of the UAT
 - Preliminary plans may be based on information available at the time of the initial IAPD and completed in more detail during the appropriate phase of the project
 - FNS evaluates the information to determine if the State agency's plans, methodology, results tracking, and analysis approach are adequate and whether additional information is needed



- The State agency must provide a “Complete and Final Test Plan” to FNS prior to the start of the UAT
 - The “Complete and Final Test Plan” itself does not require approval
- The requirements analysis and definition activities should directly interface with the test planning effort to determine the testability of the requirements
 - Requirements analysis during test planning involves two steps: analyzing the requirements to develop tests for each one and analyzing each requirement for testability
 - The first step is to analyze requirements to establish how they will be tested
 - This is an initial assessment of what is necessary to test each requirement developed during system planning
 - It is a precursor to developing complete test cases, test scripts, and test data to support testing
 - The second part of the requirements analysis phase is determining the testability of each requirement
 - A requirement is testable if its function, capability, or purpose can be verified through observable indicators
 - The test should either pass or fail
 - To be testable, requirements should be clear, precise, and unambiguous
 - This is where requirements analysis and test planning intersect
- The “Complete and Final Test Plan” should contain, at a minimum, these components:
 - Timeline/Milestones
 - Testing Resources
 - Test Environment and Equipment
 - Roles and Responsibilities
 - Test Approach
 - Items to be Tested
 - Roll Back Contingency Plan
 - Risk Management
 - System Security
 - Stress/Load Testing
 - Data Conversion
- Federal policy requires FNS ensure that all eligibility systems are adequately reviewed and tested, which FNS accomplishes through the Go/No-Go Decision Process
 - FNS has established two project milestones for a Go/No-Go determination
 - The State agency must assess the results of the UAT and prepare a formal recommendation for a Go/No-Go decision to FNS



- FNS' concurrence is required after UAT for continued system development and funding for the Pilot
- A similar assessment of results and Go/No-Go recommendation must be submitted to FNS after the Pilot to secure FNS' approval to proceed to system implementation (i.e., rollout)
- FNS may require additional milestones during rollout

Endnotes

⁴⁴ "Pre-implementation", 7 CFR 277.18(g)(2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=2738636c7b014e16c731ee710dd741b7&mc=true&node=se7.4.277_118&rgn=div8

⁴⁵ "Preservation of access and payment accuracy", Food Conservation and Energy Act of 2008 Section 4121, U.S. Government, http://www.nrcs.usda.gov/Internet/FSE_DOCUMENTS/stelprdb1045987.pdf

⁴⁶ "Testing", 7 CFR 277.18(g)(2)(i), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277_118&rgn=div8

⁴⁷ "Testing", 7 CFR 277.18(g)(2)(i), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277_118&rgn=div8

⁴⁸ "Information Security Program", 7 CFR 277.18(m)(2)(ii)(B) through (D), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277_118&rgn=div8

⁴⁹ "Pilot", 7 CFR 277.18(g)(2)(ii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277_118&rgn=div8



⁵⁰ "Functional Requirements Documents (FRd) for a Model WIC System", U.S. Government, <http://www.fns.usda.gov/apd/wic-fred>

⁵¹ "Access to the system and records", 7 CFR 277.18(k), U.S. Government, [http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277 118&rgn=div8](http://www.ecfr.gov/cgi-bin/text-idx?SID=10170aa98d677fc8397ab1f6c76d9e7c&mc=true&node=se7.4.277%20118&rgn=div8)

⁵² "A Guide to the Project Management Body of Knowledge" (PMBOK- Fifth Edition), Project Management Institute, 2013, page 566.



7.0 Project Management

Key Points

The information in this section should allow you to understand the following:

- What is a project?
- Who is responsible for a project?
- What are the common components of a project?
- What is the governing documentation of a project?
- What are common tools for managing a project?
- How do you close a project?

Chapter Contents

7.1	Project Management	339
7.1.1	Managing IT Projects	339
7.1.2	Role of the Project Manager	341
7.2	Project Management Knowledge	343
7.3	Roles & Responsibilities	345
7.4	Project Management Plan	347
7.4.1	Requirements Management Plan	348
7.4.2	Communications Management Plan	349
7.4.3	Risk Management Plan	351
7.5	Monitoring and Control	355
7.5.1	State Agency Project Monitoring & Control	355
7.5.2	FNS Project Monitoring	357
7.6	Project Closure	358
7.7	Other Resources	360



7.8	Summary.....	361

Chapter Acronyms

ANSI	American National Standards Institute
CCB	Change Control Board
CIO	Chief Information Officer
FRD	Functional Requirements Document
PM	Project Manager
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMLC	Project Management Lifecycle
PMP	Project Management Professional
QA	Quality Assurance
RACI	Responsible Accountable Consult Inform
RTM	Requirements Traceability Matrix
SDLC	System Development Lifecycle
UAT	User Acceptance Testing
WBS	Work Breakdown Structure



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.

7.1 Project Management

The project management industry defines a project as a temporary group of related tasks undertaken to create a unique product, service, or similar result. For the State agency, the APD process could be considered a series of projects. Progressing through the PAPD until reaching PAPD closure could be considered one project, with a distinct team and scope during a defined period. Progressing through the IAPD until reaching IAPD closure might be another project with differing team makeup, scope, and period of performance.



“Project means a related set of information technology related tasks, undertaken by a State, to improve the efficiency, economy, and effectiveness of administration and/or operation of its human services programs. A project may also be a less comprehensive activity such as office automation, enhancements to an existing system, or an upgrade of computer hardware.” – 7 CFR 277.18(b)

The goal of project management, in its broadest sense, is the effort to control The Triple Constraint. The Triple Constraint, also known as the “Iron Triangle,” is the concept that scope, time, and cost are interrelated. One element cannot be changed without affecting at least one of the others. The correlation of these constraints dictates the quality of the project results. Professional and conscientious project management is essential to a successful project outcome. State agency staff overseeing project tasks and deliverables must ensure the project is being implemented as stated in the PAPD or IAPD. State agency staff must maintain overall project management responsibility by providing project management resources appropriate to the level of project complexity being undertaken. The purpose of this chapter is to provide project planning and management guidance for Information Technology (IT) projects.

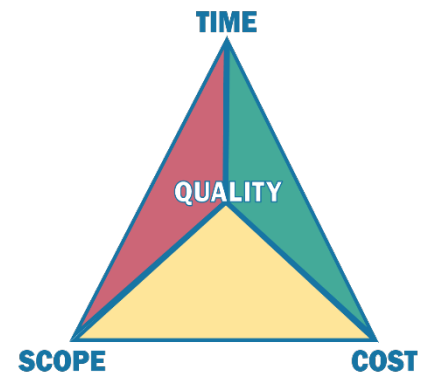


Figure 50: The Triple Constraint

7.1.1 Managing IT Projects

Managing an IT project shares the same characteristics of any well managed project. Successfully managing any project means:

- Identifying requirements



- Establishing goals
- Balancing demands of quality with time, scope, and cost
- Adapting specifications, plans, and approach to meet stakeholder needs and expectations
- Assigning a full-time, experienced, formally trained, certified professional Project Manager (PM)
- Using qualified State agency or contracted resources to hire qualified personnel
- Developing a project plan before starting the project to include:
 - High-level Work Breakdown Structure (WBS)
 - Schedule
 - Risk assessment
 - Staffing
 - Quality and communications plans
- Identifying and managing stakeholders
- Fully describing and documenting the project's business and process changes
- Setting clear performance expectations and establishing a communications protocol with all contractors involved in the project
- Making contingency plans for the unexpected, as well as anticipated, problems
- Training all workers in a timely fashion - not too early and not too late
- Providing appropriate training for the kind of work individuals will do
- Inviting feedback throughout the process
- Broadcasting achievements throughout the process
- Managing expectations

IT projects have a particular focus that means you have to concentrate on the specific IT related tasks. You should always remain aware of the APD process and FNS' objectives when conducting your project.

Successful system development and implementation requires the State agency to take the following actions:

- Ensure the system design reflects sound planning
- Build plenty of time into the project schedule for State internal and federal review and approval of all required documents
- Make extensive testing a priority (e.g., performance, usability, acceptance, and regression testing)
- Use the system pilot to discover problems that could become disastrous during rollout and beyond
- Provide documentation of the pilot evaluation to FNS
- Complete testing before starting a rollout

- Plan a reasonable rollout schedule to provide the opportunity for making course corrections and adjustments along the way
 - Use a phased approach
 - Avoid a “big bang” approach
- Turn to federal and State partners for technical assistance whenever necessary

7.1.2 Role of the Project Manager

A PM should be assigned very early and is ideally involved from the beginning of the project. A PM is not the same as a functional manager. A functional manager is the head of a group of employees with similar skill sets, such as the head of IT or accounting departments. In some cases, a functional manager is the project sponsor responsible for providing the resources for the project. A PM’s duty is not focused on particular employee skill sets, but on the project goal as a whole. A project team may consist of employees from multiple departments. As such, the PM must be empowered by the sponsor, and knowledgeable of each functional area to direct the work of team members.

An effective PM is expected be well versed in the following areas of expertise:

- Application area knowledge, standards, and regulations (e.g., functional, technical, financial, and procurement)
- Project environment (i.e., cultural, social, and political)
- General management skills and knowledge
- Communication skills
- Interpersonal skills



Further information can be obtained from [PMI’s website \(http://www.pmi.org\)](http://www.pmi.org) or its publication, “*A Guide to the Project Management Body of Knowledge.*”

While a knowledgeable PM is responsible for efficient project oversight, the PM relies on a knowledgeable State agency and federal project staff. The project staff is equally responsible for being knowledgeable of the critical activities of the project to include efficient use of funds. The project staff should clearly understand the role of the PM and how it relates to their roles.

The Project Manager:

- Does no work other than managing the project
- Does not take on assignments or participate as a member of workgroups
- Keeps the project on schedule, on budget, and within scope
- Understands the environment in which the project will operate
- Understands that each project is different depending on the technology, culture, and personalities of critical stakeholders
- Guides the project toward the most realistic definition of success
- Oversees development of the requirements in order to successfully implement the project's scope
- Identifies the most disruptive risks and develops response plans with the team that eliminate or reduce consequences
- Avoids confusion by clearly outlining the critical path when creating the project schedule
- Establishes the right relationships with team members and stakeholders along with a speedy issue-resolution process
- Works with complex scenarios and decisions involving numbers, and the politics that may accompany some project decisions
- Understands that the operations perspective is key to turnover of the system to the production world
- Is flexible, yet firm, and checks their ego at the door
- Spends 90% of their other time communicating with and facilitating the project team

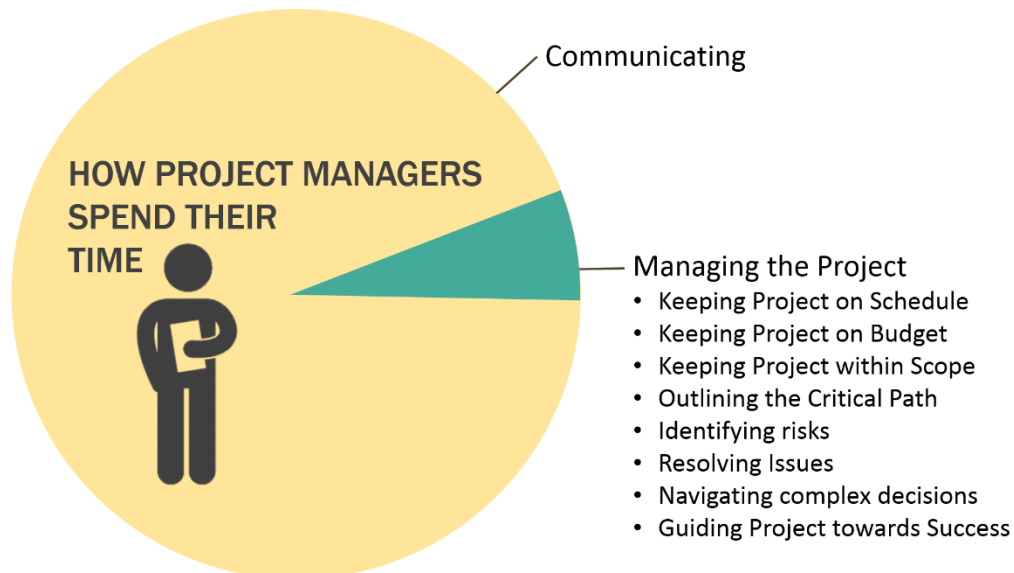


Figure 51: PM Responsibilities

7.2 Project Management Knowledge

The Project Management Institute (PMI®) is a professional organization recognized as the leader in the project management field.

PMI has organized project processes into five categories. These five categories are the basis of the Project Management Lifecycle (PMLC) discussed in chapter 2.0:

1. Initiating
2. Planning
3. Executing
4. Monitoring and Controlling
5. Closing



Figure 52: PMI Project Processes



PMI's "A Guide to the Project Management Body of Knowledge" (PMBOK®) is the only American National Standards Institute (ANSI) standard for project management.

PMI's project management knowledge topic areas include:

Project Integration Management – The processes required to ensure that the various elements of the project are properly coordinated. These include the project charter, project plan development, project plan execution, integrated change control, and project closure.

Project Scope Management – The processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. It consists of initiation, scope planning and definition, scope verification, and scope change control. Scope management also includes creating the Work Breakdown Structure (WBS).

Project Time Management – The processes required to ensure timely completion of the project. It consists of activity definition, activity sequencing, schedule development, and schedule control, as well as analyzing activity sequences, activity durations, and resource requirements to create the project schedule.



Project Cost Management – The processes required to ensure that the project is completed within the approved budget. It consists of resource planning, cost estimating, cost budgeting, and cost control.

Project Quality Management – The processes required to ensure the project will meet the requirements and needs for which it was approved. Quality Management consists of:

- Quality planning – Identifying the quality standards relevant to the project and determining how to satisfy them
- Quality assurance – Evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards
- Quality control – Monitoring specific project results to determine whether they comply with relevant quality standards and identifying ways to eliminate causes of unsatisfactory performance

Project Human Resource Management – The processes required to make the most effective use of the people involved with the project, those who organize, and those who manage the project team. Management consists of organizational planning, obtaining staff, and team development.

Project Communications Management – The processes required to ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information. It consists of communications planning, information distribution, performance reporting, and administrative closure of the project.

Project Risk Management – The systematic process of identifying, analyzing, and responding to project risk to project objectives. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events. Activities include risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring and control.

Project Procurement Management – The processes required for acquiring goods and services to attain project scope from outside the performing organization. It consists of procurement planning, solicitation planning, solicitation, source selection, contract administration, and contract closeout.

Project Procurement Management should serve the following purposes:

- Provide an open, fair, and competitive process that minimizes opportunities for corruption and ensures the impartial selection of a contractor
- Avoid potential and actual conflicts of interest or the appearance of a conflict of interest
- Establish an objective basis for contractor selection
- Obtain the best value in terms of price and quality
- Document the requirements that a contractor must meet to obtain payment
- Provide a basis for evaluating and overseeing the work of the contractor

- Allow flexible arrangements for obtaining products and services given the particular circumstances, provided such arrangements do not violate the other purposes of Project Procurement Management



For more information on **Procurement**, refer to chapter **4.0** of this handbook.

Project Stakeholder Management – The processes required to identify all people or organizations impacted by the project (i.e., the stakeholders) and analyze their expectations. Additionally, this includes evaluating their impact on the project and developing appropriate management strategies for effectively engaging stakeholders in project decisions and execution. These processes include planning stakeholder management, managing stakeholder engagement, and controlling stakeholder engagement.

To supplement this chapter, IT project managers should refer to additional resources (see Section **7.7 Other Resources**, on pg. 360), colleagues in other State agencies, and industry best practices.

7.3 Roles & Responsibilities

Project managers should have a defined formal structure for the project and for the project staff. This provides each individual with a clear understanding of their authority and responsibilities for successfully accomplishing project activities. Project team member accountability is essential for effective assignment performance and for achieving project goals and objectives. When team members participate in the planning process, they will have a sense of ownership and buy-in to the project management plan. This promotes responsibility and accountability for successfully completing the project. The roles and responsibilities of project participants will vary. Determining and defining participant requirements should be done during the project management planning process.

A good “rule of thumb” when defining participant requirements is:

- On a large project, individual role assignments may require full-time support of the function
- On smaller projects, role assignments may be performed part-time, with staff sharing in the execution of multiple functions

Tasking and individual responsibilities are covered in section **1.8 Roles and Responsibilities**, as activity assignments are defined in the planning process. Typically, these assignments are shorter term and exist only until the completion of the activity deliverable.

State agencies may choose to have FNS participate as “ex-officio” members of a project’s executive steering committee. This provides an opportunity to obtain federal reaction to plans and challenges at the earliest stages,

and to obtain federal buy-in when necessary. FNS may also participate as technical advisors on the project throughout the SDLC and PMLC, or on an as needed basis.

A Responsibility Assignment Matrix is a common tool used in project management. It is also referred to as a Responsibility, Accountability, Consult, Inform (RACI) Chart (See **Figure 53**). The RACI Chart defines each stakeholder's role by task or activity. A stakeholder should only fill one role per activity.

There are four possible roles that a stakeholder may be assigned:

1. **Responsible** – the stakeholder must perform that activity
2. **Accountable** – the stakeholder must make decisions regarding the activity, and be responsible for any consequences resulting from those decisions
3. **Consult** – the stakeholder only provides input
4. **Inform** – the stakeholder is only kept abreast of the activity's progress

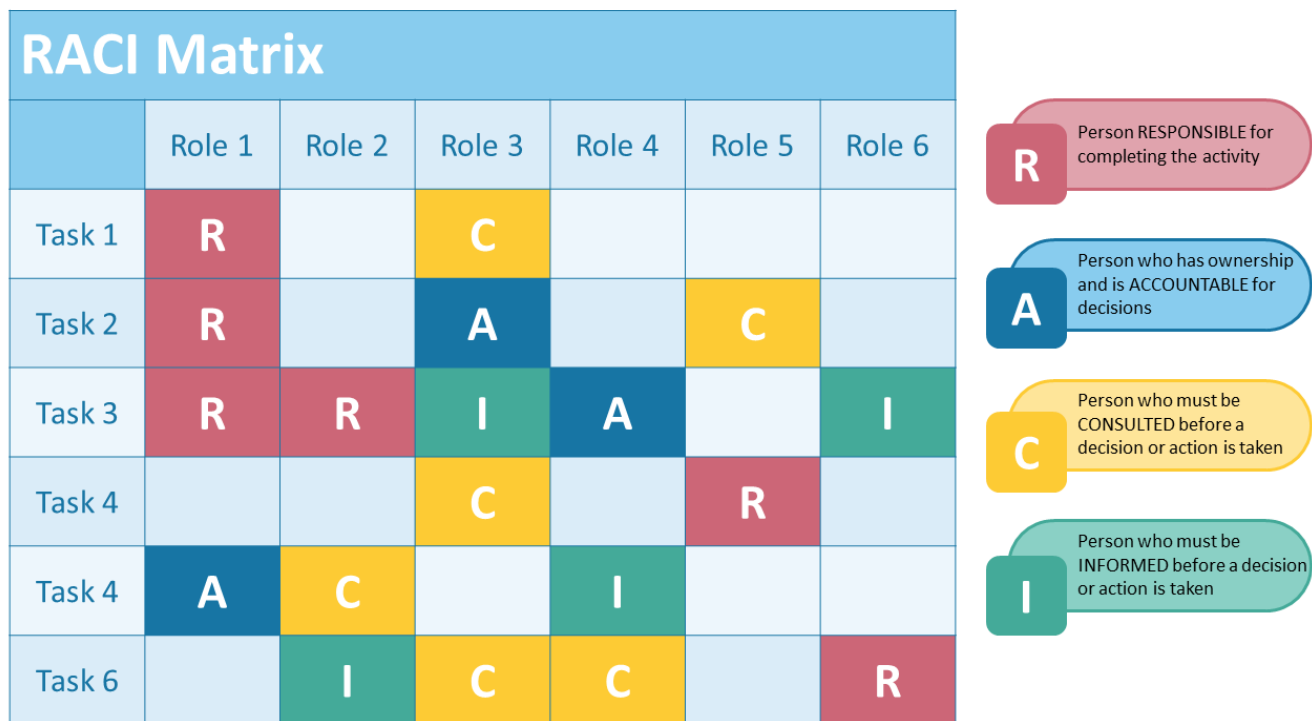


Figure 53: Example of a RACI Matrix



7.4 Project Management Plan

A Project Management Plan is a formally approved document defining how a project is managed, executed, and controlled. It documents the established “ground rules” such as procedures, priorities, and responsibility for handling various situations. It establishes the baselines from which performance metrics are measured. The Project Management Plan is generated during the initiation phase of a project. Specific details may be missing at that time or circumstances may change. Because of this, the information within a Project Management Plan is “progressively elaborated” as the project progresses. Any changes to the Project Management Plan must be approved by the Change Control Board (CCB) in accordance with the Change Management Plan section of the Project Management Plan. The CCB is a formally chartered group responsible for reviewing, evaluating, approving, delaying, or rejecting changes to the project. The RACI Matrix and the Communications Management Plan section of the Project Management Plan explain how changes are communicated.

A Project Management Plan is made up of the following components:

- **Change Management Plan** – Documents how change will be monitored and controlled to include managing the change control process involving the CCB
- **Configuration Management Plan** – Documents the functional and physical characteristics, how to control any changes to such characteristics, record and report the implementation status of the changes, and support auditing to verify conformance to requirements
- **Requirements Management Plan** – Describes how requirements will be analyzed, documented and managed
- **Scope Management Plan** – Describes how the scope will be defined, developed, monitored, controlled, and verified
- **Scope Baseline** – The approved version of the scope statement with a Work Breakdown Structure (WBS) that is used as the basis for comparison and can only be updated through the formal change control process
- **Schedule Management Plan** – Establishes the criteria and activities for developing, monitoring, and controlling the schedule
- **Schedule Baseline** – The approved version of the schedule that is used as the basis for comparison and can only be updated through the formal change control process
- **Cost Management Plan** – Describes how costs will be planned, structured, and controlled
- **Cost Baseline** – The approved version of the budget that is used as the basis for comparison and can only be updated through the formal change control process
- **Quality Management Plan** – Describes how an organization’s quality policies will be implemented
- **Process Improvement Plan** – Describes how activities will be reviewed and analyzed so that efficiency improves as the project progresses



- **Human Resource Management Plan** – Describes how the roles and responsibilities, reporting relationships, and staff management will be addressed and structured
- **Communications Management Plan** – Describes how, when, and by whom information about the project will be administered and disseminated
- **Risk Management Plan** – Describes how risk management activities will be structured and performed
- **Procurement Management Plan** – Describes how a project team will acquire goods and services from outside the performing organization
- **Stakeholder Management Plan** – Defines the processes, procedures, tools, and techniques to effectively engage the stakeholders in project decisions and execution based on the analysis of their needs, interests, and potential impact as well as defining who the stakeholders are

These components may contain additional sub-components that further support the plan depending on the complexity of the project and the PM's chosen methodologies. The following subsections discuss some of the higher priority Project Management Plan components in more detail. However, this information is not exhaustive, and additional resources are outlined in section 7.7.

7.4.1 Requirements Management Plan

A Requirements Management Plan defines the methodology a PM intends to use to compile and evaluate requirements, maintain requirement documentation and tracking, and manage related activities. This plan directly impacts the team's generation of a Functional Requirements Documentation (FRD). A Requirements Traceability Matrix (RTM) is a common component of the Requirements Management Plan. An RTM tracks requirements from origination to implementation in the final result. It supports testing activities by linking requirements to specific tests for requirements. An RTM is also a useful tool in managing the scope of a project. The RTM is useful not only throughout the life of the project, but after project completion it provides a history of the system from inception to decommissioning. This may prove helpful in the M&O phase to perform maintenance, define the scope and effect of enhancements, and serve as a functionality baseline when system replacement is considered.



Requirements Traceability Matrix								
Project Name:								
Cost Center:								
Project Description:								
ID	Associate ID	Requirement Description	Business Needs, Opportunities, Goals, Objectives	Project Objectives	WBS Deliverables	Product Design	Product Development	Test Cases
001	1.0							
	1.1							
	1.2							
	1.2.1							
002	2.0							
	2.1							
	2.1.1							
003	3.0							
	3.1							
	3.2							
004	4.0							
005	5.0							

Figure 54: Example of a Requirements Traceability Matrix

7.4.2 Communications Management Plan

Communication is widely considered the most important PM skill. Any factors or activities that may impact the quality and progress of work being performed must be communicated to the appropriate stakeholders. A PM must be proactive and thorough in distributing accurate information in a timely manner to the right audience. The Communications Management Plan describes the communications process the PM will use for this purpose.

To ensure effective communications, a PM must develop a Communications Management Plan that establishes “ground rules” known and adhered to by all stakeholders. A Communications Management Plan contains information regarding:

- Who sends and receives communication
- What communication is sent
- How communication is sent (e.g., by telephone, in a meeting, by e-mail, etc.)

- How often communication is updated
- What terms to include in a glossary

Who sends and receives communication is key to understanding and managing all the channels of communication. The potential number of communication channels can be calculated by $n(n-1)/2$, where n is the number of stakeholders. Using this formula, a project with 10 stakeholders has 45 channels of communication.

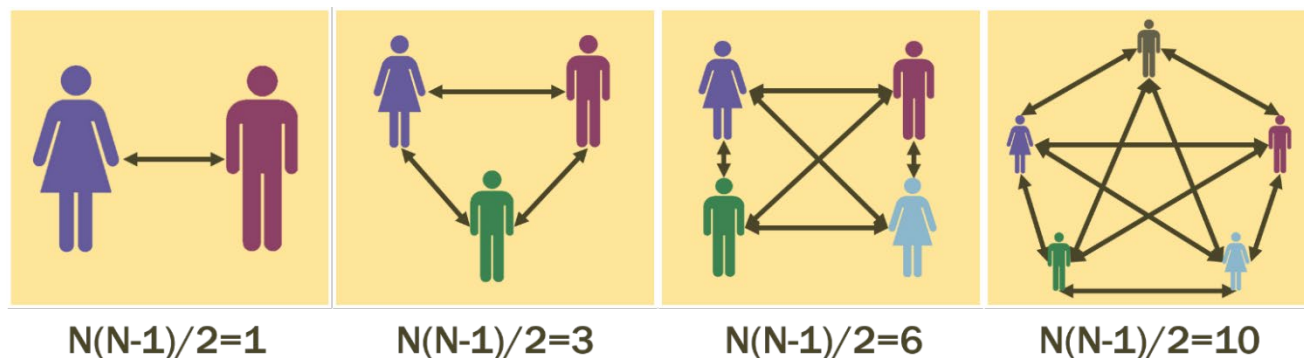


Figure 55: Lines of Communication

This is not the same as the number of messages to be communicated or how often communications occur. Not defining who can communicate to whom could result in inadvertently leaving key personal out of conversations and/or distorting messages. The RACI Chart (see **Figure 53, page 346**) is a valuable tool to use in developing the Communications Management Plan.

What is communicated is key to ensuring that relevant information is being shared with the stakeholders who need it. Inundating communication channels with information that stakeholders find irrelevant will upset stakeholders and potentially cause them to ignore communications. As an example accountants do not need, nor want, to be informed of the results of an engineer's testing.

The medium used to send communication can determine the effectiveness of the information. This may include e-mail, phone calls, websites, in person, etc. Each medium has pros and cons which make them situationally appropriate, or more effective. Stakeholder preferences, location, and the importance of the message are key determining factors in selecting a communication medium.

Managing the frequency of communications should be based on how often messages need be updated. Communicating too much may generate a false sense of urgency or create a sense of minutiae. In either case, too many communications may result in stakeholders devaluing communications. Not communicating enough is a far more common occurrence, and starves stakeholders of vital information.

Communications require a glossary of terms to ensure everyone receives and understands the same message. Misinterpretations because of differing terminology is common, especially in organizations where acronyms and jargon are prevalent. While it may seem tedious, defining common and not-so-common terms is the best way to mitigate communication issues.

7.4.3 Risk Management Plan

The risk management plan is where the PM defines the methodology used to identify risks and the methodology used to generate appropriate responses. The risk management plan may also contain sub-components such as a risk register (or log) and response plans. These sub-components individually identify risks, their impacts, and possible responses. Building a risk management plan requires doing risk analysis. When risks are identified, they need to be analyzed for the probability of occurring, the consequences if they occur, and reasons they might occur. The risk's impact to scope, schedule and cost must be determined, rated for severity and prioritized for action.

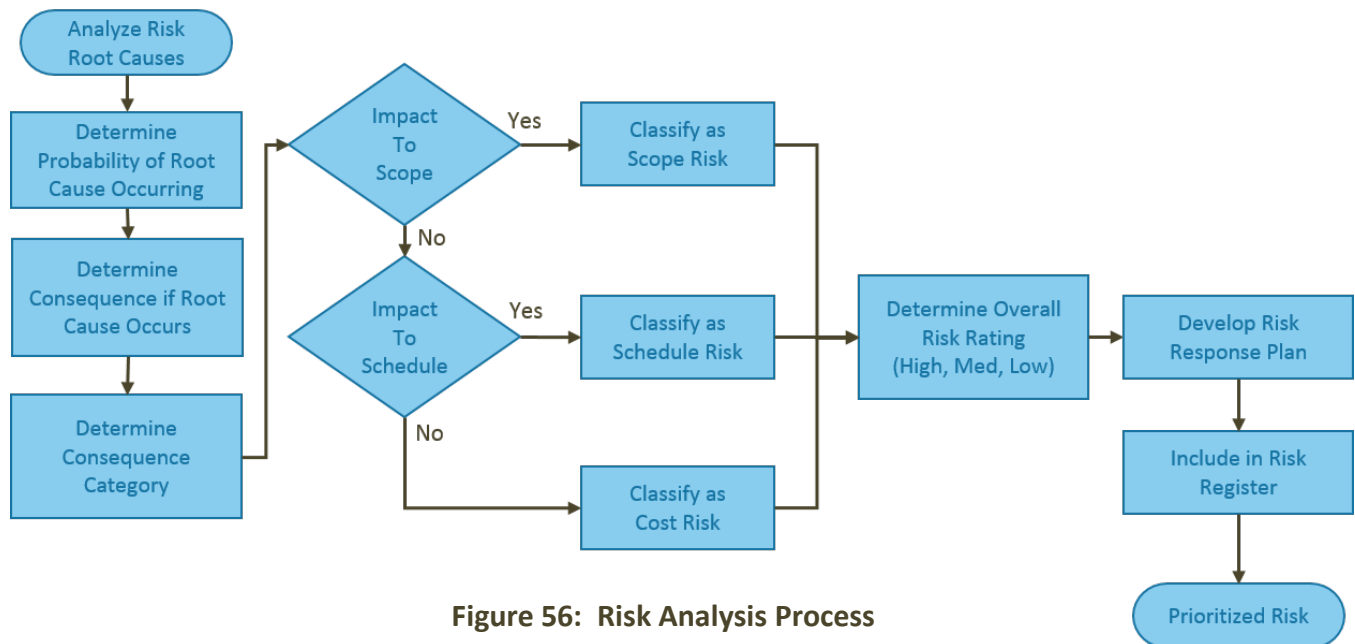


Figure 56: Risk Analysis Process

Risks must have an appropriate response when they are identified and ranked. They may be mitigated, accepted, transferred, or avoided. The PM must continually look for new risks, reassess old ones, and re-evaluate risk response plans. The PM has to make sure the right people are still assigned to response actions and that the actions still make sense in the context of the latest project developments. Risk management should be reported as part of project status reports.



See appendix **A13 Sample Status Report** for a sample Risk Register in section **A13.12** and for a sample Risk Response Document in section **A13.13**.

Project integrity is achieved by adopting and practicing continuous project risk management. Disciplined risk management provides repeatable processes for delivering the quality required for business success. Past projects and lessons learned from other similar projects are good ways State agencies can identify risks.

7.4.3.1 General APD Project Risks

FNS SSO has observed the following risks as common to APD projects:

- Poorly defined requirements
- Scope creep
- Lack of stakeholder management
- Political pressure
- Subcontractor management
- Inadequate planning
- Miscommunication
- Lack of focus
- Procurement process delays
- Failure to secure prior federal approval and funding
- Incremental or limited funding
- Inadequate State agency oversight and project management
- Turnover of key staff

7.4.3.2 Recurring APD Process Risks

FNS has identified several recurring issues specifically associated with the APD process that are risks State agencies should consider in their risk analysis and risk management planning. These issues may delay the APD process and cause risks for cost and schedule. These risks arise from the State agencies' unfamiliarity with the APD process, or failure to recognize these issues' relevancy to a current effort until they are in the middle of a project.

Examples of recurring issues that add risk to a project include:

- A lack of understanding that a partnership exists between the State agency and the federal government, which relies on good communication and collaboration



- Lack of familiarity with the dollar thresholds for APDs, RFPs, and contracts requiring FNS approval
- Lack of current technical knowledge and expertise within the State agency to write or review critical APD documents, to include:
 - Requests For Proposals (RFP) and contracts
 - system design and functional requirements
- Over reliance on the contractor to prepare required APD documentation, which can render a State vulnerable to the contractors' idea of what would be best, leading to costly consequences
- Mistaken perception that FNS can always absorb or compensate for cost overruns
- Incomplete cost allocation methodology that excludes State-only cases or doesn't include all participating federal programs
- Exclusion of State staff costs as part of the project's budget
- Insufficient understanding of the impact and resources involved for data conversion strategy and schedule
- Inadequate descriptions for system maintenance and operations methodology, costs, and assignment of responsibilities
- Inadequate time in the project schedule to assess the full impact on business processes, change business rules where necessary, and prepare staff for the transition
- Underestimation of the strain of new IS development on the entire organization
- Insufficient funding for user training and user support functions
- Not involving State IT and procurement staff throughout the project
- State program staff may be unaware of State standards, current procurements and contracts, and even conflicts with existing development efforts
- Not performing adequate testing (including the pilot) before and after implementation of a new system or major enhancement(s)

Project planning is the best time for recognizing these common issues among all State agencies. Preparing risk mitigation plans for a project will significantly reduce the risk of running out of time, or federal funds, prior to a project's completion.

7.4.3.3 Common IS Project Risks

Some risks are common to all IS projects, regardless of the technologies or methodologies being utilized. Common difficulties related to project management are:

- Giving the contractor too much control, responsibility, or authority, or both on behalf of the State agency (i.e., abdicating strategic decision making and fiscal responsibilities)



- Not managing changes to the project scope, also known as “scope creep” (adding functions to a task after development is underway)
- Placing a large focus on front-end/user interface modules while neglecting other critical elements of the system such as security, system capacity, notices, and reporting
- Delaying or neglecting management reporting
- Staying abreast of all aspects of the project budget, not just the implementation contractor costs
- Not obtaining prior approval from all applicable federal agencies before the project starts
- Not obtaining prior approval of changes and updates that occur while the project progresses
- Not realizing that changes in cost, scope, and schedule, or procurement changes, must be submitted as an APD Update (APDU) and approved by FNS before new significant costs may be incurred (i.e., erroneously thinking retroactive approval can be sought)

7.4.3.4 Risk Management and the SDLC

Risk management is implemented to minimize negative impacts on an organization and provide a basis for sound decision making. Effective risk management must be totally integrated into the SDLC and the PMLC. While each phase of the SDLC and PMLC have different risks, the basics of risk management methodology are the same regardless of the phase. Risk management is a repetitive process that needs to be performed during each major phase of the SDLC and the PMLC. The risk management plan needs to be constantly re-evaluated. As each SDLC and PMLC phase proceeds, new circumstances will arise that may not have been foreseen during initial risk analysis. Furthermore, problems solved during the course of the project may introduce risks directly related to the solution. This will prompt the risk analysis re-assessment process. **Table 39** describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

Table 39: Risk Management in Support of SDLC Phases

SDLC Phase	Phase Characteristics	Support from Risk Management Activities
Initiation	The need for an IT system is determined and the purpose and scope of the IT system is documented.	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy). Data conversion is another high risk area for consideration at this stage.
Development	The IT system is designed, purchased, programmed, developed, or otherwise constructed. The system is tested and User Acceptance Testing is completed.	The risks identified during this phase can be used to support the security analyses of the IT system, which may lead to architecture and design tradeoffs during system development.

Table 39: Risk Management in Support of SDLC Phases

SDLC Phase	Phase Characteristics	Support from Risk Management Activities
Implementation	The system is piloted and rolled-out to the user community. The system security features should be configured, enabled, tested, and verified.	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding any risks identified must be made prior to system operation, including data conversion.
Maintenance & Operation	The system performs its functions. Typically, the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures.	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whatever major changes are made to the IT system in its operational, production environment (e.g. new system interfaces).
Disposal	This phase may involve the disposition of data, hardware, and software. Activities may include moving, archiving, discarding, or destroying data and sanitizing the hardware and software.	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.



Refer to chapter **6.0** Test Planning for additional information on testing risks.
Refer to chapter **9.0 Systems Security** for security related risk management.

7.5 Monitoring and Control

7.5.1 State Agency Project Monitoring & Control

Monitoring and control of a project is the process of tracking, reviewing, and reporting project progress against performance objectives which were defined in the Project Management Plan. The State agency is primarily responsible for these activities, but FNS is involved to some extent as well. FNS expects State agencies to establish a plan for monitoring the development of State automation projects as a condition of project approval. Overall project monitoring includes specifically monitoring project procurements and formal acceptance of contracted

services. The results of State agency monitoring are reported either in the APDU, or at critical junctures in project execution. FNS may require specific State monitoring activities to ensure appropriate project oversight. Likewise, FNS may participate in State agency monitoring activities or conduct additional review activities at its discretion.



Reviews should be conducted periodically throughout the PMLC to gauge project progress and status.

Quality Assurance (QA) is a key activity of monitoring and control. It may be performed by a QA contractor or by qualified State agency staff. The QA contractor must not be the same as the project management contractor. Likewise, the State QA staff should be independent from the project management or development staff. Implementation QA includes independent monitoring of project status indicators such as schedules, accomplishments, deliverables, and costs. Implementation QA also incorporates formal reviews of development and implementation activities. These reviews are critical to the oversight of IS development projects.

State agencies should have detailed project schedules. They should establish and maintain frequent status reports to oversee their staff and contractors on the project level. They should submit status reports to FNS to ensure overall program administration. FNS may require the State agency to provide contractor and project status reports for informational purposes throughout the project. These may be outlined as conditions for funding approval.

The results of State agency monitoring may be reported in routine status reports in addition to APDUs. For management to make informed and timely decisions regarding work efforts, status reports should reasonably reflect current project performance.



See the ***Sample Status Report*** in appendix **A13**.

Contractors are often required to provide monthly reports to the State agency (in accordance with the contract). These reports are a significant source of much of the information needed to keep FNS informed of the project status. In some cases, contractor reports can be forwarded directly to FNS with no additional work. If contractor reports are incomplete, the State agency must supplement contractor information in the status report. It is essential for FNS to have a clear understanding of the project's status. Status reports need not be lengthy to be informative and meet FNS expectations. Thorough status reports make annual APDUs easier to compile. Project



changes that exceed program thresholds must be approved in advance by FNS through the submission of an APDU As-Needed.

When submitting status reports to FNS, State agencies should include the following information:

- The time period covered by the report
- Narrative description of current project status
- Description of activities that took place in the reporting period
 - Explain if activities were added or omitted from those in the approved APD
 - Areas where activities did not correspond to the project work plan
- Significant accomplishments
- Major deliverables received/approved
- Areas where the project is behind, why, and what steps are being taken to make up time or adjust the remaining schedule
- Status of previously identified problems or concerns
- Newly identified problems or concerns
 - A contractor and the State may have a different idea of what constitutes a concern
 - In addition to the reports, consult FNS for guidance in resolving problems
- Status of any items in the State's risk assessment that apply to this project phase
- Project staffing changes
- Budget that shows any known or expected variations from the approved APD budget in a way that FNS can see what has changed
 - Previous quarters should show actual costs
 - Future quarters should show budgeted costs
- A thorough narrative of all "significant changes"
- For future quarters, review all estimated costs to the budget
 - Show changes for all line items you anticipate will change and explain why
 - The most common reason would be for delays, when a cost is moved to a future quarter
- Contractor bills and payments made

7.5.2 FNS Project Monitoring

FNS will perform its own monitoring in addition to the activities performed by the State agency. FNS will monitor State agency projects using a variety of methods such as reviewing documents and reports, and participating in conference calls and virtual demonstrations. FNS reserves the right to conduct on-site monitoring through project status visits; local or state agency reviews, or both; participating in user training; and participating in User Acceptance Testing (UAT).

FNS may elect to conduct a System Functional Requirements Review after the system has passed UAT, before the pilot, or before the deployment of software. FNS may decide to do all of these. Please note that this does not have to be an on-site review. The review may be conducted by reviewing UAT or Pilot Evaluation documentation, or both, provided by the State agency.

Reasons for doing this include:

- Evaluating system performance and accuracy
- Looking for indicators of successful development
- Verifying that functional requirements were met
- Ensuring that all policy to be administered through the system is accurate
- Analyzing the integrity of data capture, edits, and calculations
- Verifying that UAT was thorough and successfully completed
- Ensuring the system interfaces successfully with other program IS and external entities, including EBT
- Reviewing the project FRD to ensure it meets all State and federal requirements



Please see chapter **6.0 Test Planning** for more information about testing requirements.

7.6 Project Closure

The purpose of project closeout is primarily to bring closure to all of the project's administrative activities. This means providing feedback on project team member's performance, updating the skills inventory, capturing key project metrics, and filing all pertinent project materials into the project repository. This includes documenting final actual project expenditures, closing open contracts, and finalizing project records. All finalized project documents should be archived for future reference for other projects.

At this point the project is within the closing phase of the PMLC and the responsibilities of the project manager are to:

- Assess how closely the project met customer needs
- Highlight what worked well
- Learn from mistakes made during the project
- Identify patterns and trends
- Derive ways to improve on processes executed throughout the project
- Communicate results to all stakeholders



There are many activities executed throughout the life of a project that require documentation during closeout. These activities may include:

- Managing project scope
- Managing the project's schedule will result in the final project schedule
- Managing the budget will result in a final budget in the form of an actual expenditures report
- Monitoring and controlling risks that have been recorded in an updated risk management worksheet
- Managing change control and deliverable acceptance
- Documenting organizational changes in final approval forms
- Issuing logs and status reports

Project closure may include a post-implementation review, preferably six months after implementation and roll-out are completed. The purpose of conducting a post-implementation review is to gather the information required to meet IAPD process responsibilities. The review may be conducted by the State agency as a deliverable, by FNS, or a combination. This review is a time to assess the project and derive any lessons learned and best practices to be applied to future projects. The post-implementation report may be used for an internal State agency review of the project's closure or in response to an additional requirement imposed by FNS prior to the closure of the project's APD. The information is sent to FNS in a post-implementation report. Many State agencies may have a formal post-implementation review process in place. Others may use a less formal method that achieves the same results.

The review has three main tasks:

- Solicit feedback
- Conduct project assessment
- Prepare post-implementation report

The review may start with a survey designed to solicit feedback from the project team, end users, and other stakeholders. The PM should gather feedback using a survey appropriate to the project. Depending on the size and type of the project, and the structure of the responsible State agency, different surveys may be required for different stakeholder groups. At a minimum, feedback should be solicited from the project sponsor (this may be the director or CIO), project team members, and end users. Once feedback has been collected and evaluated, an assessment meeting may be conducted to derive best practices and formulate lessons learned to inform future efforts. The PM should gain consensus on what was successful and what was not and derive best practices and lessons learned. These should be documented both for the individual State agency, as well as for the benefit of other State agencies. Ideally, the best practices and lessons learned should be stored in a centralized organizational repository, facilitating access and retrieval by managers of future projects. The PM may conduct the project assessment by meeting with select members of the project team and stakeholders to present the

summarized results. Other topics of discussion should include results of the feedback surveys and other aspects of the completed project.

After the project assessment, the PM prepares a post-implementation report, which is a distillation of the information gleaned from the assessment that is organized, according to feedback categories, and has added information on key project metrics. Topics to include in the report are an assessment on the effectiveness of project management, risk management, communications, change management, issues management, implementation and transition, and performance of the project team. The PM must present or distribute the post-implementation report to members of the responsible organization and should share it with FNS.



A critical reason for the post-implementation review is to ensure that the system is reviewed and evaluated before the warranty period expires. States often tend to relax after implementation and forget that they have a limited time to identify any problems or shortcomings with the system and get them fixed during the warranty period. See chapter **3.0 The Advance Planning Document Process** for more details.

7.7 Other Resources

For additional information on project management, consult any of the resources listed in **Table 40 and Table 41**.

Table 40: Internet Project Management Resources

FNS	http://www.fns.usda.gov/
Project Management Institute (PMI®)	http://www.pmi.org
New York State Project Management Guidebook Release 2	https://its.ny.gov/nys-project-management-guidebook-release-2
North Dakota Information Technology Department, Project Management	http://www.nd.gov/itd
North Dakota Project Management Guidebooks and Templates	https://www.nd.gov/itd/services/project-management/customized-project-management-tools-and-templates
NIST Information Systems Guide Conducting Risk Assessments	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf



Table 41: Literary Project Management Resources

A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Project Management Institute
Lientz, Bennet P. and Kathryn P. Rea, <i>Project Management for the 21st Century</i> , (Academic Press, 2002).
Kerzner, Harold, <i>Project Management: A Systems Approach to Planning, Scheduling, and Controlling</i> , (Wiley, 2006).

7.8 Project Management Summary

For purposes of the APD process, a “Project” is a set of information technology related tasks, undertaken by a State agency to improve the efficiency, economy, and effectiveness of administration and/or operation of its human services programs.

- Project managers should have a defined formal structure for the project and project staff
 - Project team members should have a clear understanding of their authority and responsibilities for successfully accomplishing project activities
 - See **1.8 Roles and Responsibilities**
- A Project Management Plan defines how a project is managed, executed, and controlled. It contains these core components:
 - Change Management Plan
 - Scope Baseline and Management Plan
 - Schedule Baseline and Management Plan
 - Cost Baseline and Management Plan
 - Quality Management Plan
 - Communications Management Plan
 - Risk Management Plan
 - Procurement Management Plan
 - Stakeholder Management Plan
- Governance of the project is based largely on Project Management Plan components and those directly responsible for them
- Managing the project is part of the Monitoring and Control functions of the project Management Lifecycle
 - Common tools used for managing the project include the Scope, Cost, and Schedule Baselines, Quality Assurance (QA), and the annual APD Updates (APDU)



- Project closeout brings closure to all of the project's administrative activities
 - Documents final, actual project expenditures; closes completed contracts; and finalizes project materiel
 - May include a post-implementation review, preferably six months after implementation and roll-out are completed



8.0 Financial Management

Key Points

The information in this section should allow you to understand the following:

- What federal Regulations and guidelines govern the financial management of IS projects?
- How are allowable costs determined and allocated in a budget?
- What financial information must be submitted with the APD to obtain FFP approval?
- What are the guidelines for Cost Allocation when planning, implementing and maintaining an IS?
- What reporting guidelines and forms are mandatory for the State agencies to use when reporting costs?

Chapter Contents

8.1	APD Financial Preparations	366
8.1.1	General APD Funding Requests	366
8.1.2	Regulatory Guidance	367
8.1.3	Administrative Requirements	369
8.2	Allocable Costs	369
8.2.1	Necessary and Reasonable Costs	369
8.2.2	Direct and Indirect Costs	370
8.2.3	Allowable Costs	370
8.2.4	Unallowable Costs	371
8.2.5	Processing Cost Disallowances	372
8.2.6	Developmental Versus Operational Costs	374
8.3	Common Cost Items for IT Systems Projects	374
8.3.1	Compensation for Personnel Services (Staff Costs)	374
8.3.2	Outside Contractor Professional Services	375
8.3.3	Internal/State IT Professional Services	375



8.3.4	Documentation/Materials	376
8.3.5	Telecommunications	376
8.3.6	Equipment and Other Capital Expenditures	376
8.4	Waivers of Depreciation	377
8.4.1	Software Costs	378
8.4.2	Hardware Costs	378
8.4.3	Site Preparation Costs	378
8.4.4	Interest	378
8.5	Cost Allocation	379
8.5.1	Division of Cost Allocation Services (CAS)	380
8.5.2	Cost Allocation Stakeholders	381
8.5.3	Cost Allocation Plan	382
8.5.4	Cost Allocation Methodologies	382
8.5.5	Indirect Cost Proposals	384
8.6	Cost Reviews and Audits	385
8.6.1	Office of Management and Budget (OMB) Responsibilities	385
8.6.2	Food and Nutrition Service (FNS) Review	386
8.6.3	General Budget Estimates	387
8.6.4	Operational Budget Estimating	389
8.6.5	Completing the Planning Advanced Planning Document Budget	389
8.6.6	Completing the Implementation Advance Planning Document Budget	390
8.6.7	Completing an APDU Budget	391
8.7	Expenditure Reporting	391
8.7.1	Revised Project Cost Estimate	391
8.7.2	Actual Costs to Date	392
8.7.3	Program and Budget Summary for SNAP APDs	392



8.7.4	WIC Developmental Costs	393
8.7.5	WIC- State Agency Management Information System Annual Cost Survey.....	393
8.7.6	Annual APDU Expenditure Reporting	393
8.7.7	Regional Office Expenditure Review.....	394
8.8	Other Resources	394
8.9	Summary.....	395

Chapter Acronyms

ADP	Automated Data Processing
CAP	Cost Allocation Plan
CFR	Code of Federal Regulations
EAR	Emergency Acquisition Request
EBT	Electronic Benefit Transfer
FFP	Federal financial participation
FFR	Federal Financial Report (Form FS-425)
IS	Information System or Systems
M&O	Maintenance and Operations
MIS	Management Information Systems
NSA	Nutrition Services & Administration
OMB	Office of Management and Budget
RO	Regional Office
SAE	State Administrative Expense
SAM	State Agency Model
SDLC	System Development Lifecycle
SSO	State Systems Office



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.

8.1 APD Financial Preparations

One of the major purposes for submitting an Advance Planning Document (APD) is to secure federal funding for systems planning and/or development of eligibility and issuance systems. Sound financial planning and cost determination activities are essential for preparing the APD. Costs must be determined, allocated, and identified to support the APD submission. They are also integral for establishing APD activities based on expected funding thresholds. (See section **1.5.1 Thresholds** for applicable APD funding thresholds.)



Most costs associated with new or upgraded IS are not considered administrative and must be approved beforehand through the use of an Advance Planning Document. Without prior approval, State agencies are at risk for not being reimbursed. Therefore, State agencies must follow the APD process to obtain FNS approval before they initiate activities. See chapter 3.0 The APD Process for a detailed look at the APD process.

8.1.1 General APD Funding Requests

Guidance for acquiring information systems through the APD process can be found in [7 CFR 277.18](#).⁵³ This regulatory section establishes conditions for requesting Federal financial participation (FFP) funds and the related documentation for IS Purchases.

State agencies must follow the APD process to obtain FNS approval before they initiate activities to:

- Plan for procuring the IS
- Procure the IS
- Implement the IS
- Perform Maintenance and Operations (M&O) on the IS



Preparing and reviewing APDs encompasses not only programmatic and technical considerations, but also a host of financial management concerns. These include:

- Assigning costs to the correct costing categories
- Determining costs allowable under federal regulations
- Assessing equipment and handling depreciation
- Allocating those costs to the correct program
- Preparing IS project budgets
- Reporting, reviewing, and reimbursing subsequent costs

Funding acquired through the APD process is available for activities such as procuring contractors for planning, development, and M&O. M&O procurement activities include installation or upgrade to a State agency's eligibility/issuance information system. Financial resources are available for these activities if the IS project meets FNS program objectives and requirements for eligibility and issuance system funding. For example, the APD process is not used for telephony systems or payroll systems that aren't used directly as part of the development of an eligibility/issuance system. The approval of funding not directly related to an eligibility/issuance system's development is accomplished as part of the State agency's annual request for administrative funding.

This chapter covers topics related to the financial management of IS projects supporting SNAP and WIC. Because many practices are governed by program-specific regulations, there is a close relationship between financial management requirements and the entire APD process. Therefore, a State agency must be familiar with the program-specific IS requirements as a basis for understanding and using the financial management information presented in this chapter. It is important to understand the prior-approval thresholds, funding sources, and reimbursement rates for each program when applying the financial management guidance in this chapter.



For more information on the relationship between the APD process and Financial Management, see chapters **1.0** and **2.0**.

8.1.2 Regulatory Guidance

The Code of Federal Regulations concerning Grants and Agreements should be used as a base reference during the APD process, especially in regard to the Department of Agriculture.⁵⁴ The information in [2 CFR Subtitle A -- OMB Guidance for Grants and Agreements and Subtitle B – FAR for Grants and Agreements](#)⁵⁵ applies to organizations that receive federal funds. This may be either directly from the federal government or passed through to an entity such as a local government, nonprofit organization, or educational institution. State agencies also need to follow the financial management requirements for SNAP (7 CFR 277.1 through 285.5)⁵⁶ and WIC (7 CFR 246.1 through 246.28).⁵⁷



The factors affecting the allowability of State agency IS project costs under federal Awards are included in sections [2 CFR 200.403 \(a\) through \(g\)](#).⁵⁸ This regulatory section covers the allowable cost determination, but does not identify specific circumstances or dictate the extent of federal or government unit financial participation of a particular program or project.



Costs must meet general criteria in order to be allowable under materiel awards.
- 2 CFR 200.403

Table 42 lists Regulations and Policies to assist State Agencies with preparing an APD and assigning correct funding and cost areas.

Table 42: Regulations and Policy Governing Financial Management

Authority	Topic - Purpose
2 CFR 200.0 to 200.521 ⁵⁹	Title 2 – Subtitle A – Chapter II – Office of Management and Budget Guidance Part 200 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards
2 CFR 200.400 ⁶⁰	Title 2 – Subtitle A – Chapter II—Office of Management and Budget Guidance – Subpart E – Policy Guide
7 CFR 277.1 to 277.18 ⁶¹	Title 7 – Subtitle B – Chapter II – Subchapter C – Part 277 – Payments of Certain Administrative Costs of State Agencies
7 CFR 277 Appendix A ⁶²	Title 7 – Subtitle B – Chapter II – Subchapter C – Part 277 – Appendix A – Principles for Determining Costs Applicable to Administration of the Food Stamp Program by State Agencies
7 CFR 246.1 to 246.28 ⁶³	Title 7 – Subtitle B – Chapter II – Subchapter A – Part 246 – Special Supplemental Nutrition Program For Women, Infants And Children
7 CFR 271.1 to 285.5 ⁶⁴	Title 7 – Subtitle B – Chapter II – Subchapter C – Part 271-285 – Food Stamp and Food Distribution Program



8.1.3 Administrative Requirements

The federal awarding agency must manage and administer the federal award so that funding is expended and associated programs are implemented in full accordance with U.S. statutory and public policy requirements as stated in [2 CFR 200.300\(a\)](#). State agencies are responsible for complying with all requirements of the federal award to include provisions and requirements referenced in 2 CFR 200.300 to 2 CFR 200.345.

8.2 Allocable Costs

A cost is allocable to a particular cost objective if the goods or services involved can be charged or assigned to that cost objective according to the relative benefits received. All activities that benefit from the State agency's indirect costs, including unallowable activities and services donated to the State by third parties, will receive an appropriate allocation of indirect costs.

Any cost allocable to a particular federal award or cost objective may not be charged to other federal awards to overcome fund deficiencies, to avoid restrictions imposed by law, to change terms of the federal awards, or for other reasons. Such a practice constitutes unallowable cost shifting. However, this prohibition does not preclude State agencies from charging costs that are allowable and allocable under two or more awards, pursuant to existing program agreements. Such charges are viewed as funding allocations rather than as cost allocations.

Cost principles as described in 7 CFR 200.400 through 200.475 must be used in determining the allowable costs and cost allocation of work performed by non-federal entities under federal awards. These principles must also be used by non-federal entities as a guide for contract and subcontract pricing.



For cases in which an accumulation of indirect costs will ultimately result in charges to a Federal award, a cost allocation plan or indirect cost rate agreement will be required.
- 2 CFR 200.416

8.2.1 Necessary and Reasonable Costs

A cost is considered necessary if it is crucial for proper and efficient performance and administration of a federal award. A cost is reasonable if in its nature and amount it does not exceed that which would be incurred by a prudent person under the circumstances prevailing at the time the decision was made to incur the cost.



In determining reasonableness of a given cost, consideration should be given to the following questions:

- Is it a type of cost that is generally recognized as ordinary and necessary for the operation of the State agency or the performance of the federal award?
- Do the costs fall within the restraints or requirements imposed by such factors as sound business practices, arms-length bargaining, applicable regulations, or federal award terms and conditions?
- Are the costs normal market prices for comparable goods or services?
- Do individuals involved in the project act with prudence in the circumstances, considering their responsibilities to the State agency, its employees, the public at large, and the federal government?
- Are there significant deviations from the established practices of the State agency that have unjustifiably caused increases in the federal award's cost?

When reviewing the total proposed project, FNS will closely examine the reasonableness of specific components of the project. One example might be the State's choice of hardware equipment and related costs. On the basis of judgments about the necessity and reasonableness of the technical approach and its costs, specific costs may be disapproved. If disapproved, FNS must clearly document the reasons and provide justification to the State agency.

8.2.2 Direct and Indirect Costs

To be reimbursed for both direct and indirect IS acquisition costs, State agencies must apply federal cost principles when preparing APDs. Specifically, the State agency must demonstrate that their projected direct and indirect costs are allowable, reasonable, and allocable. To do this properly, State agencies must follow guidance published in [2 CFR 200.412](#) and [200.415](#).⁶⁵

Direct costs can be specifically identified as benefiting a program with a particular cost objective, such as a grant, contract, project, function, or activity. Indirect costs are not readily identifiable with a benefitting program. Indirect costs are necessary to the general operation of the grantee and the activities it performs (i.e., costs incurred in operating and maintaining buildings and equipment, administrative salaries, and so on).

8.2.3 Allowable Costs

FNS uses the projected costs and any associated procurement documents to assess whether the costs associated with the project are allowable. If the submission of an APD is not required on the basis of the program's thresholds and conditions, the State agency must demonstrate to FNS the approval of State plans and associated budgets, specific grant agreements, or both. State agencies frequently encounter problems because they neglect to separate IS-related costs from other program costs, including M&O.



Thresholds and conditions for SNAP and WIC APDs are discussed in chapter **1.0 *Getting Started with the Advance Planning Document (APD) Process***.

Subject to program, grant, and prior approval requirements and conditions, costs are allowable and FFP can be used if the costs are:

- Necessary, reasonable, and allocable to the program
- Compliant with any limitations or conditions of program regulations or FFP conditions
- Allocated to the FFP on a basis consistent with policies applicable to all activities of the awardee
- Accounted for consistently and in accordance with generally accepted accounting principles
- Not allocated to or included in the cost in any other federally-funded program

Aside from initial APD requests for funding, and related base contracts, there are related funding thresholds related to procurements



For more information on the acquisition thresholds, see chapter **4.0 *Procurement***.

FNS will not disallow costs that were not subject to approval.⁶⁶ See section **4.2.4.3** for additional information about contract amendments.

8.2.4 Unallowable Costs

FNS will disallow costs when a program claims more funds against FFP than were entitled or claimed funds for unallowable or inappropriate items. Inappropriate charges may result from exceeding approved budget levels, including charges for unallowable or unapproved costs, or for unapproved procurements. Specific cost items or categories normally are not approved separately by FNS. While individual cost categories within a budget are typically allowed, specific items of costs may be disapproved at the point of submission or disallowed after they were incurred. Retroactive costs are disapproved or disallowed in most cases.

Cost disallowances may occur as a result of one or more of the following reasons:

- Charging unallowable costs to the FFP
- Charging costs to the FFP without prior FNS approval or inconsistent with the FFP award such as time period and purpose
- Charging costs to the FFP in excess of acceptable documentation of costs incurred
- Exceeding approved funding levels or the rates of the State agency's approved cost allocation plan

- Charging costs in violation of grant conditions or other restrictions placed on the reimbursement of charges by FNS

Examples of costs that cannot be charged to FFP include the following:

- Bad debts
- Contingencies representing contributions to a reserve fund
- Contributions and donations made by the organization
- Entertainment expenses
- Alcoholic beverages
- Fines and penalties
- Fund-raising
- General government expenses, such as governor's office expenditures
- Investment management
- Legal expenses for prosecution of claims against the federal government
- Lobbying
- Under-recovery of costs under federal agreements
- Indemnification costs to indemnify the State agency against liabilities to third parties and other losses not compensated by insurance
- Costs for proprietary software applications developed specifically for SNAP and WIC
- Value of contributions or services donated by nonpublic entities



See [2 CFR 200.402](#) "Composition of Costs" and [2 CFR 200.403](#) – "Factors Affecting Allowability of Costs" for guidance concerning unallowable costs.

When costs are disallowed, this represents a debt due to the federal Government. FNS will record the value of cost disallowances as accounts receivable and pursue recovery of disallowed funds consistent with the procedures in [2 CFR 200.403 \(a\) through \(g\)](#)⁶⁷ or other appropriate policy.

8.2.5 Processing Cost Disallowances

FNS will notify the State agency of the amount and reasons for the cost disallowance. According to SNAP and WIC regulations, FNS decisions can be appealed. **Table 43** describes FNS and State agency actions and deadlines for appeals for SNAP and WIC as described in [7 CFR 246.22](#)⁶⁸ and [7 CFR 276.7](#)⁶⁹. If an appeal is not granted, FNS will pursue recovery of the disallowed funds consistent with the appropriate policy.

**Table 43: SNAP and WIC Timeline for Appeals**

Action	SNAP	WIC
FNS Sanction in writing to State agency	Evidence of delivery	Certified Mail-Return Receipt Requested
Appeal in writing via Certified Mail-Return Receipt Requested	Within 10 days receipt	Within 30 days receipt
FNS acknowledges receipt of appeal	Upon Receipt	15 days
State agency submits information listed in related Federal Regulation	Within 30 days 7 CFR 276.7 (g)(1)(i-vii)	Within 30 days 7 CFR 246.22 (b)(2)(i-vii)
FNS Hearing	Schedule hearing within 60 days / 10 days advance notice of location	Schedule hearing within 60 days / 10 days advance notice of location
Additional factual information – post hearing submission	Before 10 days after hearing close	No provision
FNS Final Determination	Within 30 days	Within 30 days
FNS Final Determination in Effect	At 30 days after delivery of FNS Decision	Receipt of Final Decision



“State agency costs means the State agency outlays from its funds available for program administration. Unless authorized by Federal legislation, costs charged to other Federal grants or to other Federal contracts may not be considered as State agency costs reimbursable under this authority.” - 7 CFR 277.2

FNS will provide notice of disallowance to the Regional Office (RO) of the federal programs involved and to the appropriate office of the Department of Health and Human Services (DHHS) Division of Cost Allocation Services (CAS). FNS also will notify the appropriate office of the DHHS CAS if it determines that the State failed to comply with an approved cost allocation plan. In such cases, FNS will coordinate with the appropriate CAS office before proceeding with a cost disallowance.⁷⁰



8.2.6 Developmental Versus Operational Costs

There comes a point in all successful projects when the development phase ends and the M&O phase begins. The change in System Development Lifecycle (SDLC) phases is particularly important in the APD process. The costs for the development phase are budgeted and reported differently than those for the M&O phase. Consequently, each requires different cost allocation plans.

In addition, funding may come from different sources. The change from development to M&O occurs on the first day of the federal fiscal quarter after development has been completed, accepted, and implemented by the State agency. This may occur all at once or in a phased rollout of the system until it is implemented statewide.

8.3 Common Cost Items for IT Systems Projects

8.3.1 Compensation for Personnel Services (Staff Costs)

It is important to consider staff time as a project cost. State agencies must be able to determine the amount of staff salaries and benefits needed to support the development and implementation of the new system. State staff members may serve as part of an advisory committee, be involved in development sessions, or be asked to serve on review panels, design modules, testing scenarios, and so forth. Staff costs should be captured by determining salary and benefit costs by fiscal quarter for each position. States should remember to anticipate the time and commitment placed on existing staff resources for supporting development and implementation of the new system. Estimates should include level of effort (i.e., staff hours) and travel costs for State and local staff to attend meetings and training. Precisely assessing the factors contributing to personnel costs is not always feasible. Relying on estimates with a degree of tolerance for time and effort reporting is appropriate.

For staff not spending 100% of their time on the project, the State will need to determine the percentage of time each staff will spend on the project. This participation in the system's development and implementation is the basis for calculating costs. Determining the participation time can be done by using random moment time studies or time sheets for staff who may work across different programs. However, staff spending less than 10% of their time in a given fiscal quarter need not be included. Depending upon the development stage of the system, the percentage of time will likely change from quarter to quarter. State agencies must budget personnel services. However, reported actual costs must be based upon time distribution records or the Random Moment Sampling study. See **2 CFR 200.412- 415** for more details.⁷¹



For SNAP, full-time staff salaries and benefits directly related to the program must be identified in the budget submission, as well as part-time staff hours directly devoted to the project.

[-2 CFR 200.413\(b\)](#)



For WIC, Staff salaries and benefits must be identified in the budget submission to reflect an accurate projection of the total cost of the project, regardless of the funding source. For WIC, the funding source (e.g., NSA) should be identified if different from that of the project itself.

[-2 CFR 246.13](#)

8.3.2 Outside Contractor Professional Services

If a State agency intends to enter into one or more contracts for professional services, it must include all the costs for the services to be performed, to include the following costs and services:

- Planning, system design, development, testing, pilot, data conversion, deployment or rollout Statewide
- Staff training
- EBT processor services
- Quality Assurance (QA) services
- Project Management (PM) services
- Independent Validation and Verification (IV&V)
- Travel costs for the contractor

Some contractor costs may be limited by contract or not permitted. Unauthorized contractor costs are discussed in more detail under the related cost identifiers found in [2 CFR 200.459](#).⁷²

8.3.3 Internal/State IT Professional Services

If a State agency intends to have services provided by one or more departmental or other State agency IT group(s), it must include the costs for the services to be performed. These include system planning, design, development, testing, pilot, data conversion, staff training, deployment or Statewide rollout, QA services, PM services, and IV&V.

Travel expenses incurred specifically to carry out the award for departmental or State agency IT personnel are also included. Program staff activities should not be included here.

8.3.4 Documentation/Materials

A well-planned IS project requires considerable documentation. Often this material is prepared by contractors who are developing and implementing the system. However, this documentation may also be prepared in-house by IT staff or occasionally by program staff.



The cost of developing this documentation and material should be captured. If the cost is already reflected in another category (i.e., State staff time or contractor services) do not include it again.

Include the cost for training manuals, other written training materials, audio/visual or online training materials, user manuals, help desk manuals, data dictionary, annotated code, other system documents, hardware inventory, software inventory, and contingency plans. Each of these costs should be separately identified.

8.3.5 Telecommunications

Telecommunication costs are the costs to transmit data between sites. These costs would be charged by local or long distance telephone providers, Internet service providers, or other telecommunications providers. Quarterly costs should be recorded.

8.3.6 Equipment and Other Capital Expenditures

Cost of capital expenditures, including equipment, site preparation, and other capital improvements must be recovered by the State agency through depreciation or use allowances. Guidance on equipment expenditure is found in [2 CFR 200.439](#).⁷³ Guidance on allowable depreciation is found in [2 CFR 200.436](#).⁷⁴ When converting from use allowance to depreciation, the balance to be depreciated will be computed using a *pro forma* depreciation schedule starting with the date of acquisition.



For WIC, costs of any amount for IS equipment will be charged to FNS programs through interest or a depreciation schedule.

The costs of IS equipment having unit or total aggregate acquisition costs in excess of \$25,000 will be charged to FNS programs through interest or a depreciation schedule. Interest is allowable for costs that are charged through a depreciation schedule [7 CFR 277.18 \(j\)\(3\)](#).⁷⁵ Capital expenditures may only be allowed as a direct cost with prior approval. Therefore, the total cost, including the acquisition cost and interest, must be charged through a depreciation schedule unless a waiver of depreciation is granted by the funding agencies. Depreciation schedules must be reviewed and approved. Normally, Internal Revenue Service (IRS) standards⁷⁶ are used for determining a depreciation schedule. However, State agencies may propose alternatives based on useful life. After equipment is fully depreciated, no further charges may be made to FNS.

8.4 Waivers of Depreciation

A waiver of depreciation is a written request to change the method of accounting and claiming for the cost of equipment. The written request asks for agency permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly known as “expensing”). Unless agency permission is received, the equipment cost must be based on depreciation over the life of the equipment.

A typical waiver of depreciation requests to depreciate the cost of equipment over the expected life of the equipment for the purposes of APD budgeting. When it is more beneficial to expense or pay upfront the full price of the equipment, FNS may allow expensing of capital expenditures and grant a waiver of depreciation. Waivers of depreciation are normally granted only when it is cost-beneficial to FNS.

In evaluating a request for a waiver of depreciation, FNS will examine the following criteria:

- Documentation from the State agency justifies that expensing costs in the period acquired would be more cost beneficial to the federal government than depreciating the costs
- Sufficient funds exist within the current-year federal appropriation to allow expensing of costs within the period of acquisition



If sufficient criteria are met, and if the equipment acquisition is part of an APD, any request for a waiver of depreciation or interest as cost-charging methods should be submitted as part of the Implementation APD (IAPD). For projects in which an APD is not required, the State must submit those waiver requests to FNS with sufficient explanation for the criteria listed above.

8.4.1 Software Costs

Most new computer systems and transfers involve some custom code. Other costs in this category may include license fees for items such as server licenses, commercial off-the-shelf (COTS) software, security and network software, and operating system (OS) software.

8.4.2 Hardware Costs

Include all the hardware for this effort, including laptops, desktops, modems, printers for offices as well as food instruments, servers, monitors, uninterrupted power supplies, network equipment (hubs, routers, etc.), and the location where the hardware will be used, price per unit, and number of units to be procured.

8.4.3 Site Preparation Costs

New computer systems often require considerable changes to program operations. Sites often require wiring for electricity, telecommunications, and computer cabling for local area networks. Another common cost is improved site security. Include any other costs incurred in the preparation of the site for the new system.

8.4.4 Interest

Allowable interest is subject to the following conditions:

- Pending payment of the acquisition costs, interest earned on borrowed funds is used to offset the current period's cost or the capitalized interest, as appropriate. Earnings subject to reporting to the Federal IRS under arbitrage requirements may be excluded.
- State agencies will negotiate the amount of allowable interest whenever payments (e.g., interest, depreciation, use allowances, and contributions) exceed State agency's cash payments and other contributions attributable to that portion of real property used for federal awards.

Retroactive claims for interest paid in prior periods are unallowable. For facilities, [7 CFR 246.15](#)⁷⁷ also requires earnings on construction borrowings be offset against income expense. For cases in which depreciation and interest expense exceed principal and interest payments (positive cash flow), the State agency is required to



negotiate the amount of allowable interest with the Cognizant Federal agency (e.g., CAS). See section **8.5.1-Division of Cost Allocation Services (CAS)** for more information related to the Cognizant Federal agency.

8.5 Cost Allocation

Federal agencies use the APD process to receive and approve State agency requests for FFP for systems with anticipated total project costs (both Federal and State funds) based on the thresholds described in chapter **1.0 Getting Started with the Advance Planning Document (APD) Process**. As part of the APD process, State agencies are required to submit cost allocation information beginning with State agency system planning and continuing through system development and operations. Allocation means the process of assigning a cost or a group of costs to one or more cost objectives in reasonable proportion to the benefit provided or other equitable relationship. The process may entail assigning cost directly to a final cost objective or through one or more intermediate cost objectives as described in [2 CFR 200.4](#).⁷⁸ Increasingly, as new technologies and design approaches have become available, State agencies are integrating their systems to administer several Federal and State programs simultaneously. Equitable cost sharing is very important because system integration and modernization costs are substantial.

State agencies almost universally use IS to administer multiple Federal and State public assistance programs where multiple federal agencies provide FFP. Federal and State public assistance programs may include these programs:

- SNAP
- WIC
- Farmers Market Nutrition Program (FMNP)
- Medicaid
- Temporary Assistance for Needy Families (TANF)
- Child care
- Child support enforcement
- Child welfare programs
- Refugee assistance programs

Cost allocation requires the identification of two types of costs: direct costs (i.e., costs for system functions or activities benefiting only one State or Federal program) and shared costs (i.e., costs for system functions or activities that benefit two or more State or Federal programs).



Software development is usually the single largest cost item at more than 50% of total system costs.

Costs of integrated IS will be shared equitably by all users of IS systems, [2 CFR 200.416\(a\)](#).⁷⁹ Costs incurred in the development of systems are shared differently from those incurred in operations. Therefore, benefiting agencies retain the authority to approve cost allocation methods for development. Operational cost allocation plans for state agencies are reviewed and approved by the Cognizant Federal agency, DHHS' Division of Cost Allocation Services (CAS). CAS reviews only operational cost allocation plans.



"Cognizant Federal agency means the Federal agency that, on behalf of all Federal agencies, is responsible for establishing final indirect cost rates and forward pricing rates, if applicable, and administering cost accounting standards for all contracts in a business unit."

- [48 CFR 2.101](#)

8.5.1 Division of Cost Allocation Services (CAS)

Allocation of system development costs was assigned to the funding agencies in 1986. All participating federal agencies must approve cost allocation plans for development costs. Indirect cost rates and cost allocation plans are used by grantee institutions to charge federal programs for administrative and facility costs associated with conducting federal programs. The Office of Management and Budget (OMB) has designated DHHS' Division of Cost Allocation Services as the "Cognizant Federal agency" for approval of operational cost allocation plans only. As the Cognizant Federal agency, DHHS' Division of Cost Allocation Services is responsible for reviewing and negotiating facility and administrative (indirect) cost rates, fringe benefit rates, and special rates as determined to be appropriate. This includes costs related to researching patient care rates and statewide cost allocation plans and public assistance cost allocation plans for operational costs.

The CAS provides technical assistance and guidance to both federal departments and agencies and the grantee community. The CAS resolves audits involving indirect costs, cost allocation issues, and cost allocation methodologies. The CAS provides indirect cost rate and cost allocation plan negotiation services to federal departments and agencies for which DHHS is designated by OMB as the Cognizant Federal agency. The CAS

represents the federal government during negotiations and has a fiduciary responsibility to protect the public funds and to communicate and negotiate with the grantee community.

The Bureau of Indian Affairs is the “Cognizant Federal agency” for indirect costs and cost allocation plans for the Indian Tribal Organizations.

8.5.2 Cost Allocation Stakeholders

Because of the special nature of the cost allocation plans for IS, various agencies must agree on cost allocation for the system being developed. Operational cost allocation plans are reviewed and approved, in consultation with the participating agencies, by DHHS’ CAS.



The Central Service Cost Allocation Plan (CSCAP) documents the process used to align the statewide costs and their allocation for review and approval by the DHHS’ CAS. CSCAPs must include all central service costs that will be claimed under Federal awards, whether as a billed or an allocated cost. Costs of central services omitted from the plan will not be reimbursed.

For an effective and accurate cost allocation plan, State agencies need to build a team early in the system planning process for systems that support more than one federal program. This team should be cross-functional and include representatives from program, technical, and financial management staff as described in [2 CFR 200.416](#).⁸⁰

Depending on the business environment, contractor staff may also need to be included. Benefiting Federal and State program staff that need to be included in the cost allocation process include the following personnel:

- FNS program and financial management staff, typically located in a RO or FNS headquarters
- State program staff
- System (IT) staff
- State Program staff (SNAP, WIC, TANF, Medicaid, etc., as well as State public assistance programs using the system)
- State financial management and accounting staff
- Contractors (if applicable)

At the outset, the State agency cost allocation team should establish communication with federal benefiting program representatives. The State team can describe the cost allocation methodology it is considering and get helpful feedback from its federal benefiting program representatives. The earlier in the cost allocation process



the State and Federal representatives begin working together, the more likely there will be no surprises when the cost allocation plan is submitted for approval.

8.5.3 Cost Allocation Plan

A cost allocation plan is the document that State agencies submit to federal benefiting programs for approval during the APD process to obtain federal funding for a portion of State system costs. The cost allocation plan documents the State agency's methodology for cost allocation and shows the proposed benefiting programs' share of cost by percentage and dollar share amount. Each federal benefiting program must approve the State agency's cost allocation plan.

Most State agencies provide certain services on a centralized basis. Such services may include motor pools, computer centers, purchasing, and accounting to operating agencies. Because federally-supported awards are performed in the individual operating agencies, there must be a process to reasonably and consistently identify and align costs to the appropriate activities.

Plans must include a projection of the coming year's allocated central services cost. Projected costs should be based on either actual cost for the most recently completed year or on the budget projection for the coming year. Plans must also include a reconciliation of the actual costs.

8.5.4 Cost Allocation Methodologies

The methodology for allocating costs for the planning phase of a project is not as complex as during the development phase. Common methodologies include simply splitting the costs equally among all benefiting programs or according to each program's share of the total caseload or the duplicated recipient counts. Other methodologies that a State agency may propose will also be considered. Allocating costs during the development phase are more complex and must be in line with the methodology used in the Cost Allocation Methodologies (CAM) Toolkit.⁸¹ The CAM Toolkit (see **Figure 57**) models a simple, consistent, and objective cost allocation methodology for assisting States in determining equitable distributions of software development costs. This helps expedite the federal approval process, offers a training tool for staff, and provides a valuable resource during the planning phase of the system's lifecycle. It is available to Federal, State, and local agencies through collaboration among the DHHS Administration for Children and Families (ACF) and Office of Child Support Enforcement (OCSE), FNS, and representatives from the States of Kansas and Texas. This toolkit is designed for use by staff typically responsible for cost allocation planning and implementation for State IS supporting Federal and State public assistance programs.

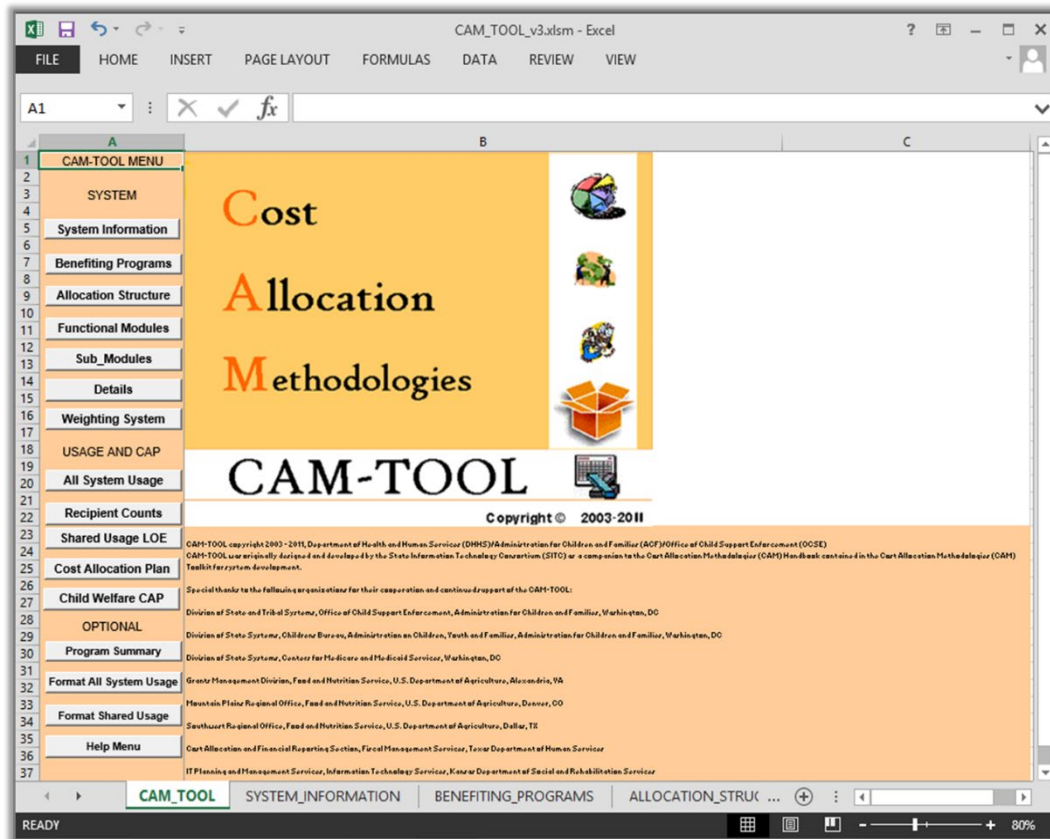


Figure 57: The CAM-TOOL for Cost Allocation Methodologies

Because policies, laws, and regulations change often, State agencies should refer to the FNS Web site CAM Toolkit. Regular communication, benchmarking other State agency information and processes, and diligent research will combine to make cost allocation and the APD process in general go smoother.



For proper results, the CAM Tool should be downloaded to the user's PC and macros must be enabled in MS-Excel. The current CAM Tool version is written in MS-Excel 2010 and can be downloaded at: <https://www.fns.usda.gov/sso/cam-toolkit>.



The Toolkit includes:

- **CAM Handbook (MS Word)** - The CAM Handbook presents a comprehensive introduction to cost allocation. It contains practical guidance on preparing cost allocation plans throughout the system lifecycle in conjunction with the federal APD process.
- **CAM-Tool (MS Excel)** - This MS Excel tool provides a consistent, objective cost allocation process for identifying all Federal and State benefiting programs. It calculates an equitable distribution of software development costs among those benefiting programs. A series of worksheets walks the user through the cost allocation process. The CAM-Tool is designed for intermediate MS Excel users.
- **CAM-Tool User Guide (MS Word)** - This user guide supplements the on-screen help available in the CAM-Tool itself. It contains step-by-step procedures and screen displays to illustrate how to capture and analyze the data needed to produce equitable distributions of software development costs to Federal and State benefiting programs. The toolkit provides a standard process for State agencies to document system and allocation information, identify all benefiting programs, identify direct and shared costs by program, and prepare the cost allocation plan for submission and approval.

8.5.5 Indirect Cost Proposals

Indirect costs include costs originating in the department or agency carrying out the federal awards and costs of governmental central services distributed through the Central Service Cost Allocation Plan (CSCAP) that are not otherwise treated as direct costs. The State agency must prepare an indirect cost rate proposal providing necessary documentation to substantiate its request for an indirect cost rate used to charge against a federal award.

The basic steps for a simplified indirect cost rate plan are to adjust the total costs by eliminating any unallowable costs or capital expenditures. The cost rate plan will classify the remaining costs as direct or indirect and compute the rate by dividing the total indirect cost by the direct base. The direct base selected for distribution of the indirect costs may be the total grants or revenues received by the grantee or some other measure (e.g., salaries or full-time labor equivalents).

The Cognizant Federal agency will:

- Review the proposal for completeness, reliability, and accuracy
- Review prior negotiation and audit experience
- Assess the State agency's financial condition
- Determine the extent to which coordination with other awarding agencies is necessary
- Determine if it includes all activities and costs of the State agency
- Determine if allocation methods and billing mechanisms are appropriate and properly designed



- Assess the appropriate rate base for direct costs for the resulting indirect cost rate and the extent to which any rate established should be subsequently adjusted

When an Indirect Cost Proposal is approved, it results in an Indirect Cost Rate Agreement (ICRA). FNS Regional Financial Management staff verify that these agreements exist when they perform Financial Management reviews of State agencies.

8.6 Cost Reviews and Audits

Audit of federal awards aids in determining if financial information is accurate and if an award recipient has complied with terms and conditions that could have an effect on claims for costs incurred under the award. Under the ***Inspector General Act of 1978*** as amended,⁸² the Inspector General of a federal agency may audit or investigate any program, function, or activity administered by that agency. This potential for review extends to organizations (including State, local, and Indian tribal governments) that are performing under awards made by the federal agency.

As a way to ensure the best use of audit resources, the Act requires the Inspectors General to determine the extent to which they can rely on audit work performed by non-federal auditors. This policy means that these non-federal examinations are the principal means of determining a State agency's compliance with federal regulations. Likewise, the ***Single Audit Act of 1984*** as amended⁸³ requires recipients to arrange to have independent audits performed on federal financial assistance awards received.

8.6.1 Office of Management and Budget (OMB) Responsibilities

OMB is responsible for issuing and implementing policies, procedures, and guidelines under the Single Audit Act of 1984. Several of these requirements relate to policies contained in [2 CFR 200.107](#).⁸⁴

Included within the general requirements are:

- Allowable costs and cost principles
- Federal financial reports
- Administrative requirements

Applicable OMB guidance for auditors performing audits under the Single Audit Act of 1984 identifies general and specific requirements against which the auditor is expected to test a State agency's compliance.



8.6.2 Food and Nutrition Service (FNS) Review

FNS may conduct cost reviews for IS development and operations, as may other federal or contracted personnel. State agencies need to provide access to all cost records relating to system development and operations as defined in [7 CFR 277.18\(i\)\(2\)](#).⁸⁵ FNS may use data mining software during these reviews. This will require the State agency to provide FNS staff with project expenditures in an electronic format. Failure to cooperate with federal requests for information in support of a review or audit may result in suspension or termination of FNS funding for the system and its operations.

FNS reserves the right to review specific cost items during the life of the information system. Selection of these items will be based on problems disclosed through audits, document reviews, or initial project review. All costs may be reviewed, whether charged by the primary State agency or by other agencies in the State or local government.

The following items may be assessed during the cost review process:

- Organizational charts covering both State agency and contracted staff that show all personnel and include functional descriptions.
- ADP cost allocation and direct charging plans. (Special development plans and existing operational plans. Ensure that they are current and approved by relevant federal agencies.)
- Hardware and software inventories by location and user, with the appropriate depreciation, lease, and rental schedules, to ensure correct inventorying, prior approval, and expensing and acquisition methods.
- Current configuration charts for computer systems and communication networks to ascertain that they match the approved APD Listings of current equipment and service agreements and contracts. (Service agreements must be reviewed to ensure that they are up to date and include the signatures of the appropriate officials. Rates for all users must be the same, and any refunds and discounts must be equally shared.)
- Year-to-date expense reports by cost center and expense reports for the most current federal fiscal year to ascertain that the reports match the information provided to FNS.
- Cost recovery and billing system algorithms, justifications, and operating documentation relating to the method of recovering operational costs by the State agency or the central data services center. (Review must ensure that the billing method is not being used to fund equipment and site replacement.)
- PCs, laptops, and similar equipment issuance for full-time equivalent staff and ratios of printers to staff, excluding training and intake.
- Cost charges for equipment and use of State contracts to determine if equipment acquisition is being conducted in the most cost-effective manner.

- Contracted staff's hourly and annual wages compared with the ones listed in industry publications.

If operating balances are being used for equipment replacement, the billing rate must be revised and overcharges must be accounted for either through an offset to future claims or direct payment to FNS.

In certain situations, such as when system development has been suspended or discontinued, total program costs incurred to date may require review. After a system is operational, specific charges to an FNS grant may be reviewed and validated periodically.

8.6.3 General Budget Estimates

Valid budget estimates are required because of their importance in evaluating and funding IS projects. The budget is the source of the financial information needed to make valid decisions concerning cost-benefit analyses and overall cost controls. A budget estimate must reflect the total anticipated project cost, including Federal and State shares. Accurate reporting of IS expenditures is also required to perform reconciliations against budgeted and approved funding levels. All APD-related budgets should be broken down by federal fiscal year and quarter.



The budget estimate for WIC supports the ability to determine funding availability.

The State agency must break out the costs by contributing agency (i.e., by approved cost allocation) and the percentage calculated as the agency's fair share.



An approved cost allocation plan helps Federal or State benefiting programs to determine their share of system development project costs included in the project's budget estimate.

Underestimating the budget has been a frequent problem for States for a variety of reasons, including one or more of the following:

- Inaccurate contractor estimates
- Incorrect estimate of what is involved in the system upgrade, installation, and functionality
- Incorrect estimate of timelines that result in cost overruns

Some of these problems are unforeseeable, such as software license agreements suddenly being revised. However, State agencies need to conduct thorough research to get the most accurate cost estimates.

Additional problem areas that often occur with APD budgets include the following:

- Indirect costs not shown
- Staff costs not shown
- Multiple funding sources for the same staff costs
- Multiyear budget not broken out by quarters
- Budgets include primary contractor costs but failed to include the cost for other contracted services such as project management or Quality Assurance
- State agencies' use of master service agreement contractors (contractors already vetted through the State procurement process to provide services as needed) to supplement State staff with the inclusion of these costs in the budget

If a State agency does not comply with FNS required cost principals for allowable costs, there are several remedies that FNS can impose by regulation. For example, future awards can be withheld, the current award can be suspended, or other actions can be taken that are legally available and supported through [7 CFR 277.16](#).⁸⁶



FNS review of budgets is critical. Overall approval of the entire APD depends on this information.

The first step before submission of the APD should always be an analysis and validation of the financial data being submitted for approval. Following that step, the cost allocation methodology used should be reviewed.

This review should address questions common in the APD process such as these:

- Has the State complied with the agreed-upon methodology?
- Are any unallowable costs shown?
- Has any cost of normal interest paid been included?
- Are any lease charges for land and buildings shown?

In the event that a project originally estimated to cost below the thresholds, as explained in chapter **3.0 The Advance Planning Document Process**, *is determined will exceed the thresholds*, the State agency must submit an APD to FNS for approval of the entire project, not just that portion outside of the thresholds. In such a circumstance, the State agency should work with FNS to ensure that all information requirements of the APD are



met prior to submitting the APD for approval. This will assist FNS in reviewing and approval which should shorten the approval process.

8.6.4 Operational Budget Estimating

Operational costs differ from development costs. Operational costs are ongoing costs incurred to support the system. Some of these costs are:

- Staff
- Software
- Maintenance
- License fees
- Hardware costs

The budget for operational costs would not normally be included in the project budget in the IAPD. However, if the original contract with the developer also includes a period of operations and maintenance, after the completion of the project, the operational costs should be included in the IAPD for informational purposes.

The State agency must ensure that anticipated operational costs are provided to FNS in the normal State Administrative Expense or Nutrition Services & Administration budget process. FNS may verify the appropriateness of these types of expenditures during periodic management evaluations apart from project oversight.

8.6.5 Completing the Planning Advanced Planning Document Budget

The Planning APD (PAPD) budget is designed to capture quarterly costs for the entire planning phase of the project, including all anticipated expenditures. Budgets are required to be amended as more current information becomes available. Costs may not be claimed at any time if they have not been approved by FNS. A contingent or proposed cost allocation may be used for planning purposes on the basis of the current cost allocation in use by the State agency.

A new cost allocation plan may also be proposed. The allocation for planning costs will normally not be readjusted on the basis of the final approved cost allocation methodology unless a serious flaw is found in the planning allocation methodology. In the initial submission with the original PAPD, all data, including the totals line, should reflect projected costs.

Additional cost centers can be inserted into the budget, or categories can be clarified, as appropriate to the project. PAPD updates should reflect actual costs to date. The spreadsheet and the totals line will reflect these



actual costs, while the original approved total will continue to be shown on the appropriate line for comparison purposes. A final PAPD spreadsheet should be submitted after the project planning phase is completed. It should reflect actual costs incurred. When final costs are known, State agencies will submit a final budget broken down by federal fiscal year and quarter.

Significant hardware or software development costs will not be eligible for funding under project planning. However, some hardware and software that support the planning process may be approved.

During the initial process of determining a need to upgrade or replace a State agency IS, budget items should be identified, estimated, and vetted for allowability and accuracy. The State agency needs to project costs beyond actual purchase of equipment and peripherals and plan on staff expenses to include travel and training.



See appendix **A8 Sample Budgets** for an example of a PAPD Budget.

8.6.6 Completing the Implementation Advance Planning Document Budget

The IAPD budget is designed to capture quarterly costs for the life of the project through full implementation. The life of the project is considered over when the State agency has finished rolling out the system to its last local agency.

The following costs for the IAPD should be included in the budget:

- Activities, goods, and services provided by a contractor
- Activities and services provided by a State's IT Office (not program staff)
- New or additional activities and services performed by the State or local agency staff if they are anticipated to contribute for more than 10% of their time in a quarter to the project

FNS designed the budget to capture categories of costs. While the budget itself rolls up the costs for each category, the categories should reflect all the costs of the category. The budget should capture all anticipated expenditures for the project. Additional cost centers can be inserted into the budget or categories can be clarified to be more specific, as appropriate.

Some categories to consider include these costs:

- Contractor Services
- State Staffing

- Travel
- Software
- Hardware
- Infrastructure
- Site Preparation
- Other costs not previously addressed



See appendix **A8 Sample Budgets** for an example of an IAPD Budget.

8.6.7 Completing an APDU Budget

Annual APD Updates (APDUs) for all active PAPDs and IAPDs are required for any project in which total FFP costs exceed specified thresholds and when the criteria for specific triggers are met as stated in chapter **3.0 The Advance Planning Document Process**. The APDU budget format is designed to capture actual costs quarterly throughout the life of the project and to compare them with original cost estimates. This allows both the State agency and FNS to see easily and clearly where costs are changing from the approved estimates. It enables determining where new approvals are needed, and making adjustments, as appropriate, in preparing for remaining project phases. All cost categories should be the same as in the original approved IAPD budget unless they have been clarified to be more specific.

8.7 Expenditure Reporting

Program grantees should report IS related expenditures consistent with program requirements and as approved in the APD using FNS Form 778, which is included as an addendum to the **Form SF-425, Federal Financial Report**⁸⁷. Grantees are not required to report on the status of funds by object class category of expenditure (e.g., personnel, travel, and equipment).⁸⁸

8.7.1 Revised Project Cost Estimate

A revised project cost estimate should be made up of actual costs to date at the time of the report plus the estimates for remaining quarters. If the estimates for the remaining future of the project need to change to reflect new expected realities in upcoming quarters, those changes should be reflected. They must be accompanied by narrative notes explaining the nature and extent of changes to future estimates.

As the project progresses, the State agency is likely to determine that some original cost estimates were inaccurate and should seek approval for new estimates before the expenditures are made. Estimated costs to date should reflect the estimates that were most recently approved. These costs should also include estimates (by cost center) for which approval is being sought in the narrative. This is different from actual costs to date in that changes in estimates to date were projected into the future. Actual Costs to Date reflect the past costs.

8.7.2 Actual Costs to Date

Actual costs to date should reflect current actual costs for each cost category listed. Un-liquidated obligations should be included in actual costs. Significant differences between estimated and actual costs should be explained in narrative. Actual costs to date will be compared with the most recently approved estimates, not with the originally approved estimates. Although FNS does want to keep original cost estimates in mind, changes throughout the project are expected. If new cost centers need to be added that were not in the originally approved IAPD estimates, they should be explained in the narrative.

8.7.3 Program and Budget Summary for SNAP APDs



When developing an APD for SNAP, State agencies must include the budget projection for ADP development and operational costs on Form FNS-366A. Form FNS-366A is to be submitted annually to the FNS RO by August 15 for the upcoming federal fiscal year and is to be revised as needed. On an attachment to Form FNS-366A, provide for each project the project name, project ceiling, and amount budgeted. All costs must be shown for all services, including those provided by other agencies of the State that provide IT services to the grantee. Only costs that have received the necessary approvals through the budget process may be claimed for federal reimbursement on the **Form SF-425**.⁸⁹



For SNAP, the [Form SF-425](#) is submitted quarterly for the fiscal year to include the FNS addendum: FNS 778. FNS 778 should list, by open APD project, the actual total expenditures in the appropriate columns: "ADP DEV. and ADP OPER."

8.7.4 WIC Developmental Costs



WIC developmental costs must be reported in the APDU. Separate FPRS reports by grant or for NSA include both developmental and operational costs.

Developmental Costs should be listed by:

- Open APD project
- Actual total expenditures compared with the approved budget
- Actual federal share of expenditures compared with the approved federal share of the budget

In addition, State agencies should submit an attachment to the Form FNS-798. [The Form FNS-798](#) report provides all WIC administrative costs but combines the developmental and operational costs into one figure. APD costs are reported as NSA costs on the [Form FNS-798/798A](#) (regular NSA and/or operational adjustment (OA) funds) and on the Form SF-425 (Technology or Infrastructure).

8.7.5 WIC- State Agency Management Information System Annual Cost Survey



The cost survey is broken down into new Management Information System (MIS) acquisition costs, ongoing M&O costs, and major commercial hardware and software upgrade costs. It provides the total amount of funds spent on MIS during a fiscal year and a breakdown of those expenses by line item. Survey data should be provided to FNS ROs and headquarters each fiscal year to enable FNS compliance with Office of Inspector General audit requirements.

Because only preliminary expenditures are available at that time, a revised cost survey is needed at closeout to reflect final fiscal year MIS expenses incurred by the WIC Program. The preliminary report should reflect both estimated expenditures, as well as actual expenditures, where actual expenditure data is available. The final report shall be provided to FNS RO and headquarters by March 1 and March 15, respectively, for the prior fiscal year. All MIS costs incurred and paid by WIC should be reported in the annual fiscal year cost survey regardless of funding source.⁹⁰

8.7.6 Annual APDU Expenditure Reporting

The annual APDU will include a detailed accounting of all actual project development expenditures through the last full federal fiscal quarter and projected costs for the remainder of the project. All expenditures should be reported by federal fiscal quarter and cost category as follows:

- Total expenditures



- Costs allocated to each Federal and State program
- Costs claimed from each federal program
- All costs claimed by federal fiscal quarter subsequent to the last quarter
- Source of funds that reconciles with expenditures

The quarterly expenditure data reported on the annual APDU will be consistent with the data reported to FNS on Form SF-425 and any other expenditure reports used for FNS programs.

8.7.7 Regional Office Expenditure Review

FNS ROs will compare quarterly expenditures reported in the annual APD with reported expenditures for IS development from the FNS Form 778, which is an attachment to Form SF-425, or other expenditure reports. Any differences will be examined and will need to be reconciled. The expenditures reported on the FNS Form 778 should not exceed those approved on the annual APDU for that year. Reconciled expenditures should be compared with the approved APD budget to determine if budget revisions are required. In addition, the RO should examine reported expenditures against approved APD budgets to ensure that the State is complying with the requirement to submit an APDU As Needed with revised budget projections. The addendum to the 425 (i.e., the FNS 778) contains a column for reporting total ADP operations costs and another for total ADP development costs. There is no place to report for separate projects or for a comparison to budgeted amounts. The State agency will need to use its own documentation to complete this comparison. The FNS RO should notify the designated State Systems Office representative of any inconsistencies or inaccuracies in project budgets that cannot be reconciled.

8.8 Other Resources

All staff responsible for administering and overseeing FNS programs (State and Federal staff) should be aware of the program-specific IS requirements because they relate to prior-approval thresholds, funding sources, and reimbursement rates. **Table 44** lists resource Websites that can assist with the preparation of the APD. For additional information on financial management issues related to the APD process, consult FNS.

Table 44: Additional APD Resources

Resource	URL
APD Supporting Documents and Policies	http://www.fns.usda.gov/apd/apd-supporting-documents-and-policies
CAM Toolkit	https://www.fns.usda.gov/sso/cam-toolkit
FNS Handbook 901 Training and Presentations	http://www.fns.usda.gov/apd/fns-handbook-901-training-and-presentations



Table 44: Additional APD Resources

Resource	URL
Food and Nutrition Service Documents Library	http://www.fns.usda.gov/apd/document-library
DHHS Office of Grants and Acquisition Management	http://www.hhs.gov/grants/index.html
DHHS Financial Management Cost Allocation Services	https://rates.psc.gov/

8.9 Financial Management Summary

- Federal funding for systems planning and development is obtained through the APD processes. The federal awarding agency must manage and administer the federal award so that funding is expended and associated programs are implemented in full accordance with U.S. statutory and public policy requirements.
 - Guidance for acquiring information systems through the APD process is in [7 CFR 277.18](#), including conditions for requesting FFP and the related documentation
 - State agencies also need to follow the financial management requirements for SNAP (7 CFR 277.1 through 285.5) and WIC (7 CFR 246.1 through 246.28)
 - The information in “2 CFR Subtitle A -- OMB Guidance for Grants” and “Agreements and Subtitle B – FAR for Grants and Agreements” applies to organizations that receive federal funds
 - State agencies are responsible for complying with all requirements of the federal award to include provisions and requirements referenced in 2 CFR 200.300 to 2 CFR 200.345
- APD preparation encompasses not only programmatic and technical considerations, but also financial management concerns, such as:
 - Determining costs allowable under federal regulations
 - Allocating those costs to the correct program
 - Preparing IS project budgets
- As part of the APD process, State agencies are required to submit cost allocation information beginning with State agency system planning and continuing through system development and operations
 - Cost allocation requires the identification of two types of costs:
 - Direct costs (i.e., costs for system functions or activities benefiting only one State or Federal program)
 - Shared costs (i.e., costs for system functions or activities that benefit two or more State or Federal programs)



- A cost allocation plan is the document that State agencies submit to federal benefiting programs for approval during the APD process to obtain federal funding for a portion of State system costs
- The cost allocation plan documents the State agency's methodology for cost allocation and shows the proposed benefiting programs' share of cost by percentage and dollar share amount
- Each federal benefiting program must approve the State agency's cost allocation plan
- The CAM Toolkit models a simple, consistent, and objective cost allocation methodology and helps expedite the federal approval process
- Program grantees should report IS related expenditures consistent with program requirements and as approved in the APD using FNS Form 778, which is included as an addendum to the Form SF-425, Federal Financial Report
 - Actual Costs to Date should reflect current actual costs for each cost category listed
 - A Revised Project Cost Estimate should be made up of actual costs to date at the time of the report plus the estimates for remaining quarters
- Audit of federal awards aids in determining if financial information is accurate and if an award recipient has complied with terms and conditions that could have an effect on claims for costs incurred under the award
 - State agencies need to provide access to all cost records relating to system development and operations as defined in [7 CFR 277.18\(j\)\(2\)](#)



Endnotes

- ⁵³ “State System Advance Planning Document (APD) Process”, 7 CFR 277.18, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=d832d408500ee17c4fdc9746e9728d4f&mc=true&node=pt7.4.277&rgn=div5%20-%20se7.4.277_118#se7.4.277_118
- ⁵⁴ “Grants and Agreements Subtitle B—Federal Agency Regulations for Grants and Agreements Chapter IV—Department of Agriculture” 2 CFR 400.1 through 422.14, U.S. Government, <http://www.ecfr.gov/cgi-bin/text-idx?SID=f2a69707ba248f42fead79c52183da2a&mc=true&tpl=/ecfrbrowse/Title02/2chapterIV.tpl>
- ⁵⁵ “Subtitle A- Office of Management and Budget Guidance for Grants and Agreements”, 2 CFR Parts 1 through 299 and “Subtitle B- Federal Agency Regulations for Grants and Agreements”, 2 CFR Parts 400 through 422.14 - Department of Agriculture, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=7dc7f7beaf89a7c228ab50ac46c2eef7&mc=true&tpl=/ecfrbrowse/Title02/2tab_02.tpl
- ⁵⁶ “Food Stamp and Food Distribution Program”, 7 CFR 271.1 through 285.5, U.S. Government, <http://www.ecfr.gov/cgi-bin/text-idx?SID=01a1b2ed778f35f2bafb40d5e621f163&mc=true&tpl=/ecfrbrowse/Title07/7CIIsubchapC.tpl>
- ⁵⁷ “Special Supplemental Nutrition Program for Women, Infants and Children”, 7 CFR 246.1 through 246.28, U.S. Government, <http://www.ecfr.gov/cgi-bin/text-idx?SID=01a1b2ed778f35f2bafb40d5e621f163&mc=true&node=pt7.4.246&rgn=div5>
- ⁵⁸ “Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards - Factors Affecting Allowability of Costs”, 2 CFR 200.403(a) through (g), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6be2b0655b5369194c9d1f70bd206f4f&mc=true&node=pt2.1.200&rgn=div5%23se2.1.200_1401#se2.1.200_1403
- ⁵⁹ “Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards”, 2 CFR 200.0 through 200.521, U.S. Government: <http://www.ecfr.gov/cgi-bin/text-idx?gp=&SID=3fe1bf171970aff8d57510c4039c4bf9&mc=true&tpl=/ecfrbrowse/Title02/2chapterII.tpl>
- ⁶⁰ “Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards Subpart E-Cost Principles Policy Guide”, 2 CFR 200.400, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=3fe1bf171970aff8d57510c4039c4bf9&mc=true&node=se2.1.200_1400&rgn=div8
- ⁶¹ “Payments of Certain Administrative Costs of State Agencies”, 7 CFR 277.1 through 277.18, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=96a7ed1a647b2e2c34f13c46e9f5acef&mc=true&tpl=/ecfrbrowse/Title07/7cfr277_main_02.tpl
- ⁶² “Principles for Determining Costs Applicable to Administration of the Food Stamp Program by State Agencies”, 7 CFR 277 Appendix A, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=5e371cb6e99bcc7ed9f6e728003131f5&mc=true&node=pt7.4.277&rgn=div5#ap7.4.277_118.a
- ⁶³ “Special Supplemental Nutrition Program for Women, Infants and Children”, 2 CFR 246.1 through 246.28, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=96a7ed1a647b2e2c34f13c46e9f5acef&mc=true&tpl=/ecfrbrowse/Title07/7cfr246_main_02.tpl (Accessed May 27, 2016).



-
- ⁶⁴ “Food Stamp and Food Distribution Program”, 7 CFR 271.1 through 285.5, U.S. Government, <http://www.ecfr.gov/cgi-bin/text-idx?SID=96a7ed1a647b2e2c34f13c46e9f5acef&mc=true&tpl=/ecfrbrowse/Title07/7CIIsubchapC.tpl>
- ⁶⁵ “Direct and Indirect (F&A) Costs”, 2 CFR 200.412 through 200.415, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=cb63696fc9bf3fe2f3648ac8b90148fa&mc=true&node=sg2.1.200_1411.sg13&rgn=div7
- ⁶⁶ “Disallowance of Federal financial participation”, 7 CFR 277.18 (h), U.S. Government, [https://www.ecfr.gov/current/title-7/subtitle-B/chapter-II/subchapter-C/part-277/section-277.18#p-277.18\(h\)](https://www.ecfr.gov/current/title-7/subtitle-B/chapter-II/subchapter-C/part-277/section-277.18#p-277.18(h))
- ⁶⁷ “Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards - Factors Affecting Allowability of Costs”, 2 CFR 200.403(a) through (g), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6be2b0655b5369194c9d1f70bd206f4f&mc=true&node=pt2.1.200&rgn=div5%23se2.1.200_1401#se2.1.200_1403
- ⁶⁸ “Administrative appeal of FNS decisions”, 2 CFR 246.22, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=21ba1242bf0fd10ca8052a7f8206514f&mc=true&node=se7.4.246_122&rgn=div8
- ⁶⁹ “Administrative Review Process”, 2 CFR 276.7 (a) through (k), U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=25564e3ea18f96488c38c1e7685124f3&mc=true&n=pt7.4.276&r=PART&ty=HTML%23se7.4.276_17#se7.4.276_17
- ⁷⁰ “Collection of Unallowable Costs”, 2 CFR 200.410, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=cccf55739dcf177d610dde0e1e45614b&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML%23se2.1.200_1410#se2.1.200_1410
- ⁷¹ “Direct and Indirect (F&A) Costs”, 2 CFR 200.412 through 415, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=a9a49be5ee675ebcdabed11014e680d6&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML%20-%20sg2.1.200_1411.sg13%20-%20sg2.1.200_1411.sg13#sg2.1.200_1411.sg13
- ⁷² “Professional Service Costs”, 2 CFR 200.459, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=acb59287f5aa553ae8a0f42253dbb47a&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML%23se2.1.200_1459#se2.1.200_1459
- ⁷³ “Equipment and Other Capital Expenditures”, 2 CFR 200.439, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=bbd1e1cfad6ba7a80192fc53afbeb8eb&mc=true&node=se2.1.200_1439&rgn=div8
- ⁷⁴ “Depreciation”, 2 CFR 200.436, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=a230b43ed478d7b382c1641a81451a45&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML%23se2.1.200_1436#se2.1.200_1436
- ⁷⁵ “State Systems Advance Planning Document (APD) Process”, 7 CFR 277.18 (j)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=4f12a54d9e3bf46f12fabd60a2de1eaa&mc=true&node=pt7.4.277&rgn=div5#se7.4.277_118
- ⁷⁶ “How to Depreciate Property”, Internal Revenue Service Publication 946, U.S. Government, <https://www.irs.gov/publications/p946/index.html>



-
- ⁷⁷ “Program Income Other Than Grants”, 2 CFR 246.15, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=06a03bb310045467eb112f846d75ac14&mc=true&n=pt7.4.246&r=PART&ty=HTML%23se7.4.246_115#se7.4.246_115
- ⁷⁸ “Allocation”, 2 CFR 200.4, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=ccc55739dcf177d610dde0e1e45614b&mc=true&n=pt2.1.200&r=PART&ty=HTML#se2.1.200_14
- ⁷⁹ “Cost Allocation Plans and Indirect Cost Proposals”, 2 CFR 200.416 (a), U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b733153a9545dd786dd79c48590e9b36&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML%23se2.1.200_1416%20-%20se2.1.200_1416#se2.1.200_1416
- ⁸⁰ “Cost Allocation Plans and Indirect Cost Proposals”, 2 CFR 200.416, U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=ccc55739dcf177d610dde0e1e45614b&mc=true&n=sp2.1.200.e&r=SUBPART&ty=HTML#se2.1.200_1416
- ⁸¹ “CAM Toolkit”, USDA Food and Nutrition Service, <http://www.fns.usda.gov/apd/cam-toolkit>
- ⁸² “Inspector General Act of 1978”, Office of the Law Revision Counsel, U.S. Government, <http://uscode.house.gov/view.xhtml?path=/prelim@title5/title5a/node20&edition=prelim>
- ⁸³ “Single Audit Act of 1984”, Public Law 98-502, U.S. Government, <https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg2327.pdf>
- ⁸⁴ “OMB Responsibilities”, 2 CFR 200.107, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6be2b0655b5369194%20c9d1f70bd206f4f&mc=true&node=pt2.1.200&rgn=div5#se2.1.200_1107
- ⁸⁵ “State Systems Advance Planning Document (APD) Process”, 7 CFR 277.18 (j)(2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=27adf3944445fa7fdaa84de8b2958109&mc=true&node=se7.4.277_118&rgn=div8
- ⁸⁶ “Suspension, disallowance and program closeout”, 7 CFR 277.16, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=c752ace66a9ba7c68759af627989c017&mc=true&node=pt7.4.277&rgn=div5%20#se7.4.277_116
- ⁸⁷ “Federal Financial Report”, OMB Form SF-425, U.S. Government, <https://www.grants.gov/forms/post-award-reporting-forms.html>
- ⁸⁸ “Federal Financial Report”, OMB Form SF-425, U.S. Government, <https://www.grants.gov/forms/post-award-reporting-forms.html>
- ⁸⁹ “Federal Financial Report”, OMB Form SF-425, U.S. Government, <https://www.grants.gov/forms/post-award-reporting-forms.html>
- ⁹⁰ “Distribution of Funds”, 7 CFR 246.16 (6)(b)(3)(ii), U.S. Government, http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=d68397301a625eafc941ff63087f61bb&h=L&mc=true&n=sp7.4.246.e&r=SUBPART&ty=HTML#se7.4.246_116



9.0 Systems Security

Key Points

The information in this section should allow you to understand the following:

- What are FNS requirements for security for SNAP, WIC, and EBT systems?
- What security controls apply to developing and maintaining a secure computing environment?
- What are the security controls that can be put in place to protect SNAP, WIC, and EBT systems?
- What are the key considerations for information system security?
- How do contingency plans protect SNAP, WIC, and EBT systems?

Chapter Contents

9.1	Introduction.....	403
9.1.1	Security Guidance.....	404
9.1.2	Systems Security Controls	406
9.1.3	IT Security Controls.....	407
9.2	Management Controls	408
9.2.1	IS Security Policy.....	409
9.2.2	Risk Management.....	410
9.3	Operational Controls.....	412
9.3.1	Media Protection.....	412
9.3.2	Personnel Security	413
9.3.3	Physical Security	417
9.3.4	Contingency Plans	418
9.3.5	Configuration Management	424
9.4	Technical Controls.....	424
9.4.1	Identification and Authentication.....	424



9.4.2	Logical Access Control	425
9.4.3	Network Security	427
9.4.4	Firewalls	427
9.4.5	Routers and Switches	428
9.4.6	Virus Protection Controls	429
9.4.7	Penetration Testing	429
9.4.8	Audit	430
9.4.9	Internet and Web Security	430
9.5	Privacy Controls	437
9.5.1	Authority and Purpose.....	437
9.5.2	Accountability, Audit, and Risk Management.....	438
9.5.3	Data Minimization and Retention.....	438
9.5.4	Individual Participation and Redress	439
9.5.5	Transparency	440
9.5.6	Use Limitation	440
9.6	EBT - Specific Controls	441
9.6.1	EBT Cards.....	441
9.6.2	Encryption	441
9.6.3	POS Terminal and ATM Security	442
9.6.4	EBT Security Standards	442
9.7	Security Reviews and Reporting.....	443
9.7.1	Security Plans	443
9.7.2	FNS Security Plan Reviews	445
9.8	Summary.....	446



Chapter Acronyms

AV	Anti-Virus
ADP	Automated Data Processing
CM	Configuration Management
CMOS/PROM	Complementary Metal Oxide Semiconductor / Program Read-Only-Memory
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
FISMA	Federal Information Security Modernization Act of 2014
ISO	International Organization for Standardization
ISSO	Information Systems Security Office
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
POS	Point of Sale (Terminal)
PKI	Public Key Infrastructure
STIGS	Security Technical Implementation Guides
WAN	Wide Area Network



For definitions of terms used in this handbook, please see appendix **A1 Acronyms and Glossary of Terms**.



9.1 Introduction

Information technology systems used to support SNAP and WIC deliver billions of dollars in benefits and entitlements. These systems are agency-wide enterprises encompassing hardware, software, information, data, applications, communications, and personnel. State agencies are required to secure information and EBT systems involved in the administration of FNS programs.⁹¹ By securing information systems (IS), State agencies seek to mitigate risks and threats to systems and information. Contingency planning seeks to reduce the magnitude of harm resulting from the loss or misuse of data and unauthorized access or modification of these systems. State agencies are responsible for implementing and maintaining a program to ensure adequate security is provided for personnel, information collected, processed, transmitted, stored, or disseminated into general support systems and major applications.⁹² This includes the security of all projects being developed, implemented, and tested, as well as operational systems.⁹³ When security programs are part of an IS implementation, Federal financial participation (FFP) may be used to implement security for the information systems.

It is the State's responsibility to develop an Information System (IS) security plan that meets the following goals:

- Determine appropriate IS security requirements using either recognized industry standards or compliant with federal standards governing security of federal IS and information processing⁹⁴
- Comply with applicable State and Federal regulations for IS security
- Achieve data integrity, confidentiality and availability levels consistent with the sensitivity of the information processed
- Achieve system-reliability levels consistent with the sensitivity of the information processed
- Implement and maintain continuity of operations plans consistent with the criticality of user information processing requirements
- Implement and follow procedures to report and act on IS security incidents
- Implement and follow procedures to monitor the effectiveness of the State agencies' Information Systems Security Program

This chapter provides guidance for a State agency's IS security plan and addresses best practices for security controls. State agencies and FNS should work together to ensure safeguarding customer information and protecting SNAP, WIC and EBT systems.



“Information Security” is protecting information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. – FISMA 2014

9.1.1 Security Guidance

Because of the sensitive nature of the information, such as participant data, held in eligibility, case management and benefit delivery systems by State agencies, it is critical that the information within those systems is secure. Within the federal government, a number of laws and regulations mandate that agencies protect their computers, the information they process, and related technology resources (e.g., telecommunications). The most important are the [Federal Information Security Modernization Act of 2014 \(FISMA\)](#)⁹⁵ and [OMB Circular A-130 – Managing Federal Information as a Strategic Resource](#)⁹⁶. In addition to these, other important guidelines are contained in various [National Institute of Standards and Technology \(NIST\) publications](#)⁹⁷ and the [NIST Cybersecurity Framework](#).⁹⁸

Table 45: Security Related Policies and Guidance

Guide for Developing Security Plans for Federal Information Systems (NIST Special Publication 800-18) ⁹⁹
Guide for Conducting Risk Assessments: Information Security (NIST Special Publication 800-30) ¹⁰⁰
Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34) ¹⁰¹
Guide to Information Technology Security Services (NIST Special Publication 800-35) ¹⁰²
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (NIST Special Publication 800-53rev5) ¹⁰³
Computer Incident Handling Guide (NIST Special Publication 800-61) ¹⁰⁴
Systems Security Engineering, Volume 1 (NIST Special Publication 800-160) ¹⁰⁵
National Checklist Program for IT Products – Guidelines for Checklist Users and Developers”, NIST Special Publication 800-70 (Revision 4) (NIST Special Publication 800-70) ¹⁰⁶

**Table 45: Security Related Policies and Guidance**

Guidelines for Media Sanitization (NIST Special Publication 800-88) ¹⁰⁷
Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115) ¹⁰⁸
Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST Special Publication 800-124) ¹⁰⁹
Improving Critical Infrastructure Cybersecurity: Executive Order 13636 of February 12, 2013 ¹¹⁰
Security Technical Implementation Guides (STIGS) ¹¹¹
SNAP Provisions of the Agricultural Act of 2014 (Improving Exchange of Information for Sake of Security) ¹¹²

FISMA is recommended as a best practice for State agencies using FFP to administer federal programs. The FISMA Act is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002 and has been updated twice since then. **** The FISMA requires federal agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner. NIST provides guidance for compliance with FISMA. See NIST's publication, [Assessing Security and Privacy Controls in Federal Information Systems and Organizations](#).¹¹³

OMB Circular A-130 requires that federal agencies establish security programs containing specified elements. State agencies are responsible for either developing their own program-specific security plan or ensuring that program-specific security details are included in larger agency-wide or department-wide security plans. These plans should provide for on-going security of the system, staff, and data and for disaster recovery and program business continuity. For instance, a State agency disaster recovery plan should identify when SNAP and WIC systems will become operational after a major disaster disables or adversely affects them and what interim operating procedures will be enacted.

NIST is a federal agency in the U.S. Commerce Department's Technology Administration. Their mission is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that improve information protection. NIST's Computer Security Division develops security

**** FISMA 2002 was updated in 2012 and in 2014 (including a title change), but still retains the year 2002 in its official title.

standards and guidelines for federal information technology systems and works to help improve the security of commercial projects. NIST's IT security guidance focuses their activities on security of emerging technologies, security management, security testing, and improving security standards. NIST and the federal government highly recommend these standards for all non-federal government organizations and private sector companies involved in the federal information services infrastructure.

State agencies should develop IS security programs based on federal standards outlined in FISMA, OMB Circular 130, and NIST Guidelines. Compliance with USDA policy involves a biennial State agency evaluation to determine the effectiveness of their IS Security Program.¹¹⁴



State agencies must review the security of IS on a biennial basis. This includes physical and data security, operating procedures, and personnel practices. – 7 CFR 277.18(m)(3)

9.1.2 Systems Security Controls

Information systems security is a high priority at all levels of government. Information systems are vulnerable to many threats that can inflict various types of damage, resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire systems centers. Losses can stem from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry.

State agencies should develop an Information Systems Security Program to implement and maintain the most cost-effective safeguards to protect against deliberate or inadvertent acts, including:

- Unauthorized disclosure of sensitive information or manipulation of data
- Denial of service or decrease in reliability of critical information system (IS) assets
- Unauthorized use of systems resources
- Theft or destruction of systems assets
- Fraud, embezzlement, or misuse of resources and assets

State agencies must ensure that all security procedures within their area of responsibility are documented and carried out correctly.¹¹⁵



See appendix **A14** for a **Security Plan Checklist** that assesses State and Local IS security programs.



9.1.3 IT Security Controls

In general, there are three general information technology security control groupings.¹¹⁶

- **Management controls** are used to address those controls that are strategic in nature.
- **Operational controls** address security controls implemented and directly supporting the technical controls and processing environment.
- **Technical controls** are security controls implemented on systems that transmit, process, and store information.

There are two specific additional IT security controls.

- **Privacy Controls** are the administrative, technical and physical controls safeguarding the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information.¹¹⁷
- **EBT-specific controls** are security controls that are unique to an EBT system.

Each of these control topics, along with their associated subtopics, is described in detail in the following sections. The descriptions are intended to provide State agencies with a basic understanding of security controls guidance on developing and maintaining a secure computing environment. They are not intended to be an all-encompassing strategy for State agency security needs. **Table 46** provides an outline of the security control and associated subtopics discussed in the following sections.

Table 46: IT Security Controls by Category

Control Category	Control Topic
Management Controls	IT Security Program and System-Specific Policy
	Risk Management
Operational Controls	Media Protection
	Personnel Security
	Physical Security
	Contingency Plan
	Business Continuity
	Disaster Recovery Plans
	Occupant Emergency Plan
	Security Incident Response
	Recovery Teams
	Configuration Management



Table 46: IT Security Controls by Category

Control Category	Control Topic
	Security Awareness, Training, and Education
Technical Controls	Identification and Authentication
	Logical Access Control
	Audit
	Internet/Web Security
	Network Security
	Firewalls
	Routers and Switches
	Virus Protection Controls
	Penetration Testing
Privacy Controls	Authority and Purpose
	Accountability, Audit, and Risk Management
	Data Minimization and Retention
	Individual Participation and Redress
	Transparency
	Use Limitation
EBT-Specific Controls	EBT Access Cards
	Encryption
	POS Terminal and ATM Security
	EBT Security Standards

9.2 Management Controls

Management controls are a systematic process by which management compares performance to predetermined objectives in order to take corrective action when deviations are identified. The objective of management controls is to verify that personnel and other corporate resources are being used in the most cost effective way to achieve management objectives for IS security. Depending on a State's IS security program, management controls provide oversight for developing, strengthening, updating, or modifying anything necessary for a State's IS security program. Moreover, management controls are a means to evaluate where a State stands with security self-



assessment. By implementing a procedure for personnel to follow, management provides a working plan for a State to conform to federal regulations.

9.2.1 IS Security Policy

An IS security policy documents the rules for protecting organizational information assets. State agency policy formation is necessary for the standardization of a State IS security program. State agencies are responsible for creating an up-to-date IS security plan, establishing its objectives, and assigning responsibilities. Specifically, the State is responsible for providing resources to be used, assigning roles to key personnel, laying out its own strategic directions, and addressing federal compliance issues. State policy is divided into three levels, which address different issues outlined in **Table 47**.

Table 47: Policy Levels and Descriptions

Policy Level	Description
Program-Level	Program-level policy establishes the security program, assigns program management responsibilities and drafts the IS security goals and objectives. Program-level policy includes all of the organization's IT resources, including facilities, hardware, software, information, and personnel. In some instances, the relationships among various individuals and groups may also need to be defined in the program-level policy. It might be important to clarify, for example, who is responsible for approving the security measures used for new systems, or who is responsible for installing specific components.
System-Specific	System-specific security policies are extremely detailed. These policies are developed to ensure IS security at the system level. A State's system-specific policy differs from system to system. Each system needs defined security objectives based on specific operational requirements. In addition, system-specific policies focus on decisions. For example, in order to protect the security of a particular system, management may decide to inform employees that a particular kind of software is not safe.
Issue-Specific Policy	Issue-Specific Policy addresses topics of current relevance. Program-level policy is usually broad enough that it does not require much modification over time. However, issue-specific policies are likely to require more frequent revisions. As changes in technology and related factors take place, more frequent modification is required. Management may find it necessary, for instance, to issue an issue-specific policy to define what a recently-released piece of equipment is used for, such as policies on agency-issued mobile devices, or how social media may be used on agency-owned equipment.

9.2.2 Risk Management

In general, risk management is the process of identifying and assessing risks and taking steps to subsequently reduce the negative impacts to an acceptable level. The goal of security risk management is to protect State assets against service disruption and cyber threats. Risk management for an IS security program is a continuous process of identifying vulnerabilities, determining risks associated with the threat, determining security controls to mitigate the security risk, and selecting the most cost-effective controls. Risk management is based on four phases.



The four phases of Risk Management are:

- (1) Risk Assessment - Identify threats and vulnerabilities.
- (2) Risk Analysis - Determine the severity of the risks.
- (3) Risk Mitigation - Identify security controls that can lower risks. Assumption, avoidance, limitation, planning or transference; implement cost appropriate control.
- (4) Risk Monitoring – Determine effectiveness of applied mitigation and manage accordingly.

9.2.2.1 Risk Assessment

Risk assessment identifies threats, vulnerabilities, and likelihood of loss or impact to the system. These are often categorized by natural, human (intentional and unintentional) and technical (power failure, hardware failure, etc).

Threats may include, but are not limited to the following:

- System intruders (hackers)
- Malicious code (e.g., viruses, spyware, malware) and denial of service attacks
- Criminals
- Terrorists
- Espionage
- Insiders, which could be malicious intrusion or intrusion as a result of poor training
- Natural disasters
- Hardware failure



- Public utility failure

The IS security program risk assessment is used to determine if the current security controls are adequate to reduce the probability of loss from a vulnerability or potential threat. Key risk analysis activities are conducted when a system is first implemented and whenever significant modifications are made to the system. However, because threats are always evolving and never abate, risk assessment must be a continuous process.

9.2.2.2 Risk Analysis

Once the security risks have been identified during risk assessment, risk analysis is performed. Risk Analysis determines the severity of the risks and the potential threat they pose. The security levels of risks are usually measured in degrees of high, medium, or low.

HIGH – Major loss of assets and resources that have severe or catastrophic adverse impact to the organization’s mission.

MODERATE – Loss of assets and resources that have serious adverse impact to the organization’s mission.

LOW – Loss of assets and resources that have limited adverse impact to the organization’s mission.

Figure 58: Security Level Definitions

9.2.2.3 Risk Mitigation

Developing risk mitigation solutions involves evaluating security threats identified during risk analysis to determine the most appropriate security controls to counter the identified threats and vulnerabilities. **Table 48** provides options in risk mitigation.

Table 48: Risk Mitigation Options

Risk Assumption	Accept the potential risk and continue operating the IT system.
Risk Avoidance	Avoid the risk by eliminating the cause and/or consequence.
Risk Limitation	Limit the risk by implementing controls that minimize the adverse impact of a threat.



Table 48: Risk Mitigation Options

Risk Planning	Manage the risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
Risk Transference	Transfer the risk by using options to compensate loss, such as purchasing insurance.

9.2.2.4 Cost Considerations

Implementing selected security controls identified during the risk mitigation process needs to consider cost. The cost of the security controls needs to be balanced against the cost of protecting and recovering the information resource. The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. For example, the value of the data and the costs incurred in recovering from a data breach needs to be considered. If privacy data for customer account information is involved, there are costs to notify the customer. A non-monetary example may include the loss of public confidence. Security should be appropriate and proportionate to the value and degree of reliance on the IS and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IS. A cost-benefit analysis is completed to justify the cost for implementing the control versus the cost of the information or resource requiring protection.

9.3 Operational Controls

Operational controls relate to manual processes and tasks performed by users of IS. Many important issues in IS security involve the users themselves – the personnel who use a computer or other IT devices to complete their work. As opposed to management controls, operational controls and procedures oversee day-to-day operations of a State agency’s IS security program. This part of a State agency’s IS security plan is implemented and executed by State employees. Also, operational controls encompass separation of duties among staff and appropriate training related to staff duties. The relationship of management controls to operational controls is that management controls provide State policy that employees must follow during daily operations. Operational controls directly support technical controls and the technical processing environment.

9.3.1 Media Protection

Today’s data storage environment is rapidly evolving. Consequently, more personnel than ever are responsible for effectively protecting media containing sensitive information. This responsibility is not limited to those organizations that are the originators or final resting places of specific media or data. It also includes users who have privileged access to this information along the way. Protecting information stored on various forms of media is the responsibility of all who handle it. Media flows in and out of organizational control in both electronic and



printed forms. Equipment sent for repair to outside vendors is a vulnerability. E-mail and data on smartphones, tablets, laptops, thumb drives, and other portable devices issued by the organization to its employees is vulnerable. Physical media including printed documents and DVDs introduce vulnerabilities. These potential vulnerabilities can be mitigated through proper understanding of where information is located, what that information is, and how to protect it.

Two kinds of media control exist:

Computer output controls apply to all printout copies of sensitive information and require all printout copies of sensitive information be clearly marked. These outputs produce physical materials (i.e., paper documents) that must be protected with the same diligence as electronic media. Disposal in trash and recycling receptacles is one of the greatest threats posed by physical materials.

Electronic media controls encompass the same controls as printed materials, but adapted for electronic formats. Electronic media often has both physical and electronic characteristics that must be addressed. Procedures must be established to ensure that data from electronic media that contain sensitive information cannot be accessed without authorization and authentication. Disposal of electronic media must include thoroughly deleting and wiping information to prevent recovery of sensitive information from the physical device (e.g., thumb drives, computer hard drives, CDs, DVDs, magnetic tape).

9.3.2 Personnel Security

Management must approve all personnel with responsibilities for the management, maintenance, operations, or use of system resources and access to sensitive information. State IS security plans include distinguishing roles and responsibilities between physical security personnel, users who operate the system, and privileged users. All IT staff members are trained in offensive and defensive methods to protect the agency's information assets. Adequate staffing and key position backup are essential to running and maintaining a secure environment.

The following personnel security controls should be enforced on all systems:

- Documented procedures for approving and terminating personnel access
 - May include background checks
 - Collection of any mobile devices and controlled entry badges issued to personnel
- Technical support personnel from outside the agency should be escorted at all times
 - This includes maintenance personnel for areas other than IT such as electricians, plumbers, or telecommunication technicians
 - Access and activity on systems by support personnel should be monitored and logged by Government staff



- Other non-technical support staff such as housekeeping, vending machine suppliers, or office supply vendors must be escorted at all times
- Employee's Active Directory must be deactivated in the system on or before their employment termination date
- Upon termination, an employee's system access should be revoked

Personnel security also includes establishing and maintaining procedures for enforcing personnel controls, including the following:

- **Issuing and/or revoking** user identifications (IDs) and passwords
- Conducting **security training** and providing awareness tools for all staff
- Determining appropriate access levels – **physically and logically**
- **Disposing of media appropriately** (see Guidelines for Media Sanitization (NIST SP 800-88))¹¹⁸

9.3.2.1 Separation of Duties

Separation of duties means assigning different roles and responsibilities to different people. This is an example of Risk Avoidance, referenced in section **9.2.2.3 Risk Mitigation**. For instance, an employee who makes payments to a contractor is not the same person who audits those payments to that contractor. A situation where errors may go undetected is, therefore, eliminated. The separation of duties assures that mistakes, intentional or unintentional, cannot be made without being discovered by another person. See section **9.4.2 Logical Access Control**.

Logical and physical controls are established to prevent the occasion to commit fraud, knowingly or unknowingly, by State agency staff.¹¹⁹ Examples include:

- Separating system operation duties (i.e., separation of duties) manages the amount of power held by any one individual
- Fraud occurs if there is collusion when duties are not properly separated
- Development staff does not have access to production data, unless specifically authorized by the functional data owner to repair a limited number of records
- Development staff does not have access physical system level technology or database management system servers
- End users do not have access to production data except through the features and functions of the administrative applications
- End users do not have the ability to bypass or circumvent the application's validation and audit procedures
- Functional users do not access or modify application code

- Accounts are approved by a designated data steward and subsequently created by a separate, independent system security administrator
- Access to system logs and system audits are limited to the system security analysts, and all such access is reviewed by IS management
- Access to firewalls and other network security systems is limited to network security analysts, and all such access is reviewed by IS management
- System and/or procedures prevent workers from fraudulent use such as determining eligibility for or issuing benefits to oneself or friends and relatives
- Continued training maintains heightened awareness of security controls
- Monitoring and logging for incident threat protection auditing

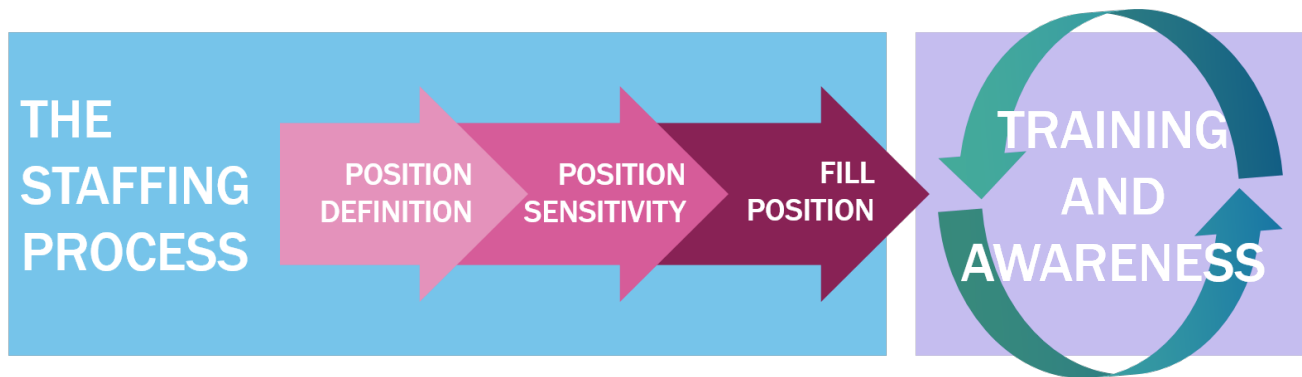


Figure 59: Staffing and Logical Controls

Table 49: Separation of Duties

Key Concept	Best Practice
Agency differences	Separation of duties may vary depending on each agency's size and structure. Duties are separated by department and by individuals within a department. The level of risk associated with a transaction comes into play when evaluating the best method for separating duties.
Demonstration	The separation of duties is able to be demonstrated to, or validated by, an outside party. Documentation of processes and authorization is helpful in demonstrating a system of control that includes separation of duties.
Document the responsibilities	Separation of duties is clearly defined, assigned, and documented. Document and clearly communicate who will initiate, submit, process, authorize, review and/or reconcile each activity within the agency.



Table 49: Separation of Duties

Key Concept	Best Practice
Review and Oversight	Management increases review and oversight when it is difficult to sufficiently separate tasks. Assess the potential for mistakes or fraudulent transactions. If the separation of duties is not sufficient to eliminate or adequately reduce the risk of discovering errors, the level of management review increases over the particular activity.

9.3.2.2 Security Awareness, Training, and Education

Personnel who manage, operate, program, maintain, or use a system must be aware of their security responsibilities. The primary purpose of security training is to ensure users understand their responsibilities and security procedures for protecting any sensitive information they manage. Security training also helps system users become familiar with using the system’s security features. Security training includes the importance of protecting client privacy and data confidentiality. Security awareness training is provided in addition to functional training, before system users are allowed access to the system. This training should be conducted periodically, at least on an annual basis.

Security awareness training should be mandatory and completed prior to granting access to the system. Periodic refresher security training (e.g., annually) is required for continued access. Therefore, each user, including contractors, must be versed in acceptable rules of behavior before being allowed access to the system. The training program also informs the user on how to identify a security incident and what actions to take in response.

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program encompasses the following seven steps:

1. Identify Program Scope, Goals, and Objectives

The scope of the program should provide training to all types of people who interact with IT systems. Since users need training which relates directly to their use of particular systems, a large organization-wide program needs to be supplemented by more system-specific programs.

2. Identify Training Staff

It is important that trainers have sufficient knowledge of computer security issues, principles, and techniques. It is also vital that they know how to communicate information and ideas effectively.

3. Identify Target Audiences



Not everyone needs the same degree or type of computer security information to do their jobs. A computer security awareness and training program should distinguish between groups of people based on roles and responsibilities. Training then presents only the information needed by the particular audience and omits irrelevant information. This approach will have the best results.

4. Motivate Management and Employees

To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consider using motivational techniques to show personnel how participation in a computer security and awareness program will benefit the organization.

5. Administer the Program

Several important considerations for administering the program include visibility, selection of appropriate training methods, topics, materials, and presentation techniques.

6. Maintain the Program

Training staff need to keep abreast of changes in computer technology and security requirements. A training program that meets an organization's needs today may be ineffective tomorrow. In order for training staff to keep current on IT security they may require consultation with IT security professionals, attending IT security seminars, and annual training.

7. Evaluate the Program

A training evaluation attempts to ascertain how much information is retained, to what extent computer security procedures are being followed, and general attitudes toward computer security.

9.3.3 Physical Security

Physical security is concerned with preventing unauthorized physical access to equipment, facilities, material, information, and documents. It includes the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

State agencies should identify critical areas and provide adequate physical protection and access control. Critical areas may include rooms containing system hardware and software such as local area network rooms or telephone closets. Other areas to safeguard include protecting check and voucher stock and EBT card stock.



Facility security measures should be developed and implemented on the basis of the level of risk to the computer and information resources, as identified during the risk assessment. Critical areas should be secured to ensure that they are accessible to authorized personnel only:

- Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server
- Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation
- Physical access controls should be reviewed for effectiveness in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied
- Electronic physical access controls should not be connected to local area network without meaningful segmentation

9.3.4 Contingency Plans

Contingency plans establish recovery procedures that address specific threats. There are several types of contingency plans. These plans help prevent minor incidents from escalating into disasters or disrupting services. Plans and strategies for mitigating risk to continuity of operations are one component in developing contingency plans. For example, a contingency plan might provide a set of procedures that defines a response required to return a computing capability to normal operation. Contingency planning directly supports an organization's goal of service continuity. Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use.

Continuity planning normally applies to the business itself; it concerns the ability to continue critical functions and processes during and after an emergency event.

Contingency planning normally applies to information systems and provides the steps needed to recover the operation of all or part of designated IS at an existing or new location in an emergency. It often involves disaster recovery and occupant emergency planning activities.

Cyber Incident Response Planning is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event.

A contingency plan provides the State agency a documented process to mitigate risks of business interruption and minimize any disruption of service, both large and small. It contains instructions for achieving a full or minimally acceptable set of business operational objectives. The plan involves preparations to respond to external circumstances that may disrupt business operations. These circumstances are determined by a risk assessment

for continuing to provide an acceptable level of service continuity. Procedures and guidelines are defined, implemented, tested, and maintained to ensure functionality of program services in the event of a disruption. Each contingency plan is uniquely tailored to program requirements. In the event of emergency, key personnel may not be available; the plan should minimize dependency on individuals for interpretation and implementation. Most important, the plan should always be maintained and updated.



See [NIST Special Publication 800-34](#) – “Contingency Planning Guide for Federal Information Systems” for guidance on contingency planning.

Contingency plans include the following:

- Communication plans are critical; they describe who is in charge of what and how they are reached, and how stakeholders are kept informed
- Backup operations plans, procedures, and responsibilities to ensure that essential and mission-critical operations will continue if normal activities are interrupted or stopped for a period of time.
- Response procedures for emergencies, including civil disorder, fire, flood, natural disaster, bomb threat, or other incidents or activities that threaten or seriously impact lives, property or the capability to perform essential functions.
- The lowest acceptable level of essential system or functional operations, so that plan priorities may be made. This must include provisions for storage, maintenance, and retrieval of essential backup and operational support data.
- Post-incident recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at a primary site or, if necessary at an alternate facility, following destruction, major damage, or other significant interruptions of the primary site.

The following five steps describe the basic functions an organization should employ when developing contingency plans:

1. Business Impact Plan

An organization identifies mission- or business-critical functions, documents these in a business impact plan and prioritizes them. In the event of a disruption event, certain business functions may not be performed. If appropriate priorities have been set and approved by senior management, then it could mean the difference in the organization’s ability to survive and recover from a disaster.

A continuity of operations plan (COOP) is another component of business impact planning. The COOP focuses on restoring an organization's mission essential functions at an alternate site and performing those functions for a limited time period (e.g., 30) days before returning to normal operations.

2. Identify Resources

Contingency planning addresses all the resources needed to perform a function. The analysis of needed resources is conducted by those who understand how the function is performed and the interdependencies among various resources. This allows an organization to assign priorities to resources since not all elements are crucial to the critical functions. The identification of resources crosses managers' areas of responsibility.

Common resources often used include:

- People Processing Capability (e.g., mainframes, personal computers, laptop computers, smartphones, mobile devices)
- Computer-Based Services (e.g., telecommunications, world wide web, Internet, wide area networks, local area networks)
- Data and Applications
- Physical Infrastructure
- Documents and Papers (e.g., documentation, blank forms, legal documents)

In addition, an organization outlines the time frames in which each resource is used:

- Is the resource needed constantly or only at the end of the month?
- What is the effect on the mission or business of the continued unavailability of the resource?

3. Develop Scenarios

An organization anticipates potential contingencies or disasters through the development of scenarios in a plan to address the wide range of things that can go wrong. Although it is impossible to think of all the things that can go wrong, an organization can identify a likely range of problems. Scenarios include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, point to other possible, but less obvious, contingencies. The contingency scenarios address each of the resources listed above.



The longer it takes to resume normal operations, the longer the agency will have to operate in recovery mode.



4. Develop Strategies

The selection of a contingency planning strategy is based on practical considerations, including feasibility and cost. Risk assessment can be used to help the feasibility of options to decide on an optimal strategy. Cost benefit analysis supplements the feasibility of the risk assessments to estimate costs for selected contingency strategies. For example, is it more expensive to purchase and maintain a generator or to move operations to an alternate site, considering the likelihood of losing electrical power for various lengths of time?

Whether the strategy is on-site or off-site, a contingency planning strategy consists of four parts:

- Emergency Response - Document the initial actions taken to protect lives and limit damage
- Recovery - Plan the steps that are taken to continue support for critical functions
- Resumption - Determine what is required in order to return to normal operations
 - The relationship between recovery and resumption is important
- Implementation - Implement the contingency plan

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the procedures, and train employees. These tasks are ongoing.

5. Test and Revise Plan

A contingency plan should be tested periodically because there may be flaws or deficiencies contained within it and its intended implementation. Responsibility for keeping the contingency plan current is assigned to specific personnel. Update the plan as time passes and as the resources used to support critical functions change. The extent and frequency of testing will vary between organizations and among systems.

9.3.4.1 Business Continuity Plan

IT facilities and systems are vulnerable to a variety of disruptions, some of which are short-term and others that last for a day or longer. The purpose of business continuity planning, a type of contingency plan, is to encourage alertness and readiness to sustain an organization's processes during and following a significant disruption in services caused by disasters and/or security failures. Business continuity begins by a risk assessment that identifies events which cause interruptions to business processes (e.g., equipment failure, flood or fire). This is followed by a business impact analysis to assess the effect of those interruptions. This assessment considers all business processes. Business continuity management includes controls to identify and reduce risks, limits the consequences of damaging incidents, and ensures that operations resume. The activation of a Business Continuity Plan may also trigger the activation of other types of contingency plans, such as Disaster Recovery Plans.

9.3.4.2 Disaster Recovery Plan



A disaster recovery plan is intended to maintain critical business processes such as Local area and Wide area networks (LANS and WANS), desktop and personal computers, websites, and distributed and mainframe systems in the event of the loss of any of the following areas for an extended period of time by physically relocating the services. Disaster Recovery Plans should contain procedures for activating Occupant Emergency Plans, extended backup operations, and recovery if a computer installation experiences a partial or total loss of computing resources. This applies to physical facilities and access to such facilities. The primary objective of this plan, used in conjunction with other types of contingency plans, is to assure that a computing installation can recover from disasters. A key part of disaster recovery planning may be to use an alternative physical location for operational use during the time that the original facility is unavailable. This includes maintaining cold, warm, and hot sites at separate locations and the appropriate failover capabilities to activate them in a reasonable amount of time to reduce service outages. A Disaster Recovery Plan may be activated on its own, or in response to the activation of another type of contingency plan such as the Business Continuity Plan. Likewise, the activation of a Disaster Recovery Plan may also trigger the activation of other contingency plans such as Occupant Emergency Plans.

9.3.4.3 Occupant Emergency Plan

An Occupant Emergency Plan outlines a specific procedure for handling physical risks to people and facilities. It may include such as items as shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake. Sensitive information and IS must be protected from access during the evacuation and absence of people in the facilities. For example, system users should log-off the system and documents with sensitive information locked in appropriate containers. If facilities cannot be occupied for extended periods of time due to damage from the emergency, a plan must exist for protecting information and IS during the vacancy. These plans are developed at the facility level and are specific to location and building design. They focus on protecting personnel and property, not maintaining business processes or information system services. They may be activated immediately as a first response or as part of a Disaster Recovery Plan.

9.3.4.4 Security Incident Response Plan

A security incident is any event or condition that has the potential to affect the security of an IS sensitive information. These incidents may result from intentional or unintentional actions and may include:

- Loss or theft of computer media
- Introduction of malicious code
- Unauthorized attempts to gain access to information
- Failure of the system security function to perform as expected
- Malicious intent by employees or other people who have authorized access

State agencies must establish and maintain incident management responsibilities and procedures to ensure a quick, effective, and orderly response to security incidents. This plan should address mitigation and isolation of compromised systems, as well as procedures for cleanup and minimization of information loss.

Procedures should cover all potential types of security incidents, including the following:

- Discovered viral infection
- Discovered malicious code (e.g., viruses, trap doors, logic bombs, worms, Trojan horses, etc.)
- Uncovered hacker activity
- Discovered system vulnerabilities
- Unauthorized attempt, successful or not, to access IS, sensitive information, or both
- Deviation from security policy
- Other unusual activities

In addition to normal contingency plans that are designed to recover systems or services as quickly as possible, the incident response procedures must also cover other specific areas:

- Analysis and identification of the cause of the incident
- Planning and implementation of remedies to prevent recurrence, if necessary
- Collection of audit trails and similar evidence
- Communication with those affected by or involved with recovery from the incident
- Report of the action to the security administration function at the agency
- Contacts for Federal, State and local authorities, as appropriate

Security Incident Response Plans are generally activated independently. However, depending on the extent of the incident, it may trigger the activation of other contingency plans such as Disaster Recovery Plans.



See [NIST Special Publication 800-61](#) – “Computer Incident Handling Guide” for details on handling security incidents.

9.3.4.5 Recovery Teams

Recovery Teams are formed to address each of the areas indicated in the contingency plans above. Teams consist of knowledgeable management and designated key personnel required for that particular area. Recovery team members need to clearly understand the team’s recovery effort goal, individual procedures the team will execute,



and how interdependencies between recovery teams may affect overall strategies. Teams should be sufficient in size to remain viable if some members are unavailable to respond or alternate team members may be designated. Similarly, team members should be familiar with the goals and procedures of other teams to facilitate cross-team coordination. All contact information should be available for IT management, team members, essential IT personnel, and designated business unit management. Upon receiving the information of a serious incident, any member of management can invoke contingency plans. Depending on the nature of the incident, a command center might be established and appropriate teams are mobilized.

9.3.5 Configuration Management

Configuration management normally addresses hardware, software, networking, and other changes. The security goal of configuration management is to know that a change occurred and what was changed. Changes should trigger a risk assessment to identify whether the change creates a weakness that can be exploited or introduces threat vulnerability. It ensures that the change does not intentionally or unintentionally diminish security. A secondary aspect of configuration management for security is to make sure the system, as changed, is updated in other system documentation such as a contingency plan. If the change is major, it may be necessary to reanalyze some of the security aspects of the system.

9.4 Technical Controls

Technical controls are security controls that the computer system executes. These controls depend on the proper configuration and functionality of the system. The implementation of technical controls requires significant operational considerations. In other words, technical controls are aligned with management's security objectives.

9.4.1 Identification and Authentication

Identification & Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Limiting system access to authorized users is an important part of security practices. This is accomplished in several ways. First, access is controlled through the use of a user identification (ID) and password combination. If a user does not have a valid user ID and password, the user is denied access to the system. For instance, if the objective is an IS security system that functions to Identify and Authenticate a specific user, the software will be configured so that the system executes the Identification and Authentication routines for that purpose every time a user attempts to gain access to the system. Second, permissions or privileges are limited to only those people necessary to perform specific job functions within systems. Supervisors and managers continuously assess the privileges granted to employees and contractors.



Based on these assessments, they submit the necessary requests to change or remove access to those system and network resources that are no longer required. Third, access to systems is controlled through the use of access control devices designed to restrict connections to the network and its resources. Access control devices such as firewalls and routers are deployed within the network infrastructure to restrict traffic into and out of the network.

9.4.1.1 Identification

User identification is used to identify people authorized to access an IS, and once the ID has been authenticated, grant them access to the system. This is the method for ensuring that the person logging on to the desktop, network or application has access permission. For this reason, all user IDs must be unique throughout the system. A password is something that only the user knows. The user ID and password combination are known as a single factor Identification and Authorization. Systems may require the use of a biometric/smartcard, digital certificates, a public key infrastructure (PKI), or a token for user ID and password authentication. Single Sign-On mechanisms provide additional security during log-in. When a user attempts to log-in, they submit their identification credentials (i.e., user ID and password) to the system for authentication.

9.4.1.2 Authentication

Authentication serves to validate the password and that it belongs to the user ID submitted with the log-in attempt. Authentication involves determining whether a user is, in fact, who he or she claims to be. User authentication is critical to ensure proper authorization and access to systems and services. Strong authentication mechanisms may be able to detect identity theft. Although authentication may not completely stop information and identity theft, it supports protecting resources by using several authentication methods. The ability to authenticate a distinct user is critical to State IS security systems.

9.4.2 Logical Access Control

Logical access control requires that the IS security system has the ability to identify and differentiate among users. NIST security guidance promotes access control based on “least privilege.” This refers to granting users only those access permissions required to perform their duties. User accountability requires linking of activities on a computer system to specific individuals, and therefore, requires the system to identify users.

An organization should consider both internal and external access control mechanisms:

- **Internal access controls** are a logical means of separating what defined users (or user groups) can or cannot do with system resources. This includes access to specific information contained in databases.
- **External access controls** are a means of controlling interactions between the system and outside people, systems, and services. “Least Privilege” is closely linked to separation of duties described in

detail in section **9.3.2.1**. In other words, users should be granted the least number of privileges necessary to perform their duties; nothing more and nothing less.



“Physical and logical access to any system should be granted based on a notion termed ‘least privilege.’ When establishing accounts, standard security principles of least privilege to perform a function should be used, where possible. Access privileges should be limited to those that the user has a genuine need for to complete job responsibilities and functions. For example, a root or administrative privileged account must not be used when a non-privileged account will do. Privileges must never be granted ‘in case’ a user might need them.” - George Mason University IT Department

9.4.2.1 Logical Access Control Software

Logical access control software provides the ability to control access to the system by establishing that only registered users with an authorized log-on ID and password can gain access to the computer system. The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. After access to the system has been granted, the next step is to control access to the data and programs residing in the system. The data or program owner can establish rules that designate those who are authorized to use the data or program.

9.4.2.2 Operating System Security

Since the application software runs on top of the operating system (OS), it is imperative that it be secured. If the OS is compromised as a result of weak security, then the applications that run on the system will also be breached. The OS is responsible for controlling the computer’s resources, and access to those resources is usually secured through the OS. The software or applications that the OS controls also need to be secure. If there is vulnerability in an application that has been granted high enough access rights (administrator or root), that application can easily be exploited to gain full control over the OS. Once the OS has been compromised, all the software it controls has also been compromised. The default installation of an OS will leave the system in an unsecured state. It is recommended that State agencies follow [Information Technology Network standards](#)¹²⁰, State standards and the contractor’s recommendation for securing their particular OS. In order to reduce these risks, it is necessary to secure the OS through a process known as “hardening.”



The following procedures are used in the hardening process:

- Eliminate unnecessary programs and services
- Close all unused ports on the system
- Change default file permission to be more restrictive
- Enable verbose logging on the system (auditing)
- Require a complementary metal oxide semiconductor/programmable read-only memory (CMOS/PROM) password
- Disable file-sharing features
- Adhere to password and user account policies and guidelines
- Apply the most current system patches for the OS

9.4.3 Network Security

Network security is an over-arching term describing policies and procedures to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. Requirements include protecting critical network services and resources from unauthorized use and security-relevant denial of service conditions. The first layer of network security is enforced through a username/password identification and authentication mechanisms. See sections **9.4.1 - Identification and Authentication** and **9.4.2 - Logical Access Control** for more detailed information. When a user is authenticated and granted specific system access, the configured firewall enforces network policies.

9.4.4 Firewalls

Firewalls block unauthorized access to or from networks. They are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall is implemented using hardware, software, or a combination of both. Firewall software is the most common way used to maintain the security of IT networks. However, a firewall can be a router, a personal computer, or a host appliance that provides additional access control to the site. These systems can be configured to control access to or from the protected networks and are most often used to shield access from the Internet. Firewalls provide greater security by enforcing access control rules before connections are made.



The following firewall requirements should be implemented:

- Firewalls that are accessible from the Internet are configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs
- Firewalls are configured to maintain audit records of all security-relevant events
 - The audit logs are archived and maintained in accordance with applicable records retention requirements and security directives
- Firewall software is kept current with the installation of all security-related updates, fixes, or modifications as soon as they are tested and approved
- Firewalls are configured under the “default deny” concept
 - This means that, for a service or port to be activated, it must be approved specifically for use
 - By default, the use of any service or communications port without specific approval is denied
- Only the minimum set of firewall services necessary for business operations is enabled, and only with the approval of the appropriate system security administrator
- All unused firewall ports and services are disabled
- All publicly accessible servers are located in the firewall DMZ or in an area specifically configured to isolate these servers from the rest of the infrastructure
- Firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with an internal source address, received from an external connection, are rejected
- Firewalls are located in controlled access areas
- Firewalls are configured to prohibit outbound traffic destined to inappropriate websites

9.4.5 Routers and Switches

Routers and switches provide communication services that are essential to the correct and secure transmission of data on local and wide area networks. The compromise of a router or switch can result in denial of service to the network. Compromises expose sensitive data that can lead to attacks against other networks from a particular location. Securing routers and switches is different than using routers and switches as firewalls.

The following best practice solutions should be applied to all routers and switches throughout an application environment:

- Access to routers and switches is password-protected in accordance with State guidance
- Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of the appropriate system security administrator
- All unused switch or router ports are disabled
- Routers and switches are configured to maintain audit records of all security-relevant events



- Router and switch software is kept current by installing all security-related updates, fixes, or modifications as soon as they are tested and approved for installation
- Any dial-up connection through routers must be made in a way that is approved by the appropriate system security administrator

9.4.6 Virus Protection Controls

Viruses and other malicious code (a.k.a. “malware”) have reached epidemic proportions throughout the computing world. Viruses can cause processing disruptions and loss of data, as well as significant loss of productivity while cleanup is conducted. In addition, new viruses are emerging at an ever-increasing rate.

All systems use antivirus utilities or programs to detect and remove viruses or other malicious code. This software is updated frequently to help fight new viruses and malware. In addition, to help ensure that viruses and malware are intercepted as early as possible, antivirus software is kept active on a system. It should not be used intermittently at the discretion of users.

Antivirus programs are installed on workstations to detect and remove viruses in incoming and outgoing e-mail messages and attachments. They actively scan downloaded files from the Internet and files copied from external media devices such as thumb drives, DVDs, and external USB drives. Workstation and server disk drives are routinely scanned for viruses. State agencies must decide what scanning schedule is appropriate and best for their systems. The type of scan impacts system resources, availability, capacity, and data throughput. Real-time background scans demand more computing resources than scans run every few minutes or on file intercept. Deep scans put high demands on hardware resources and can significantly impact system availability, capacity, and data throughput.

The specific restrictions outlined below should be implemented to reduce the threat of viruses on systems:

- Only authorized software is introduced on systems
- All media should be scanned for viruses before introduction to the system
 - This includes software and data from other activities and programs downloaded from the Internet
- Original software is not issued to users, but is copied for use in copyright agreements
 - At least one copy of the original software is stored according to Configuration Management controls

9.4.7 Penetration Testing

Penetration testing involves real-world hacking techniques to identify security weaknesses and validate the security posture of a network and IS. A systematic and analytical process is used to evaluate computer resources



for exploitable vulnerabilities. As part of the security assessment for IS, penetration testing is incorporated to effectively evaluate the security posture of the network and IS. The penetration test is approached from a hacker's perspective. Penetration testing is a highly specialized field and requires staff knowledgeable in testing methodologies, experienced in all levels of testing, and trained in the use of testing tools. A combination of both commercial and freeware hacking tools is used to scan the network to uncover any inherent vulnerability. Once all the vulnerabilities are found, they are documented along with the mitigation strategies to resolve all discovered vulnerabilities.

9.4.8 Audit

Auditing is maintaining a record of system activity by the system or application processes. This includes recording user activity from the time of log-in to the time of log-out, each and every time the user accesses the system. These records create an audit trail for traceability of activities in the system. In conjunction with appropriate tools and procedures, audit trails help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails allow for the investigation and detection of system misuse and aid in the conviction of individuals who illegally access a system.

Audit trails should capture the following information:

- System startup and shutdown
- Successful and unsuccessful login attempts
- User actions to access files or applications
- Actions taken by system administrators and security personnel
- All administrative actions performed on a system
- Audit trails should record the following information for each event:
 - Date and time of event
 - Type of event
 - Success or failure of an event, and
 - Name of file or application accessed

Audit trail logs are properly secured with access limited to system administrators. The audit logs should be reviewed regularly. States must establish and adhere to a policy for length of retention.

9.4.9 Internet and Web Security

The Internet is an integral part of the way business is conducted. It is critical that State agencies work in accordance with standards and mandates to secure access to the web. Hackers are constantly trying to exploit weaknesses in Internet security systems and policy to gain access to personal files and information. As people

become more reliant on modern technology, they also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media fraud. By adhering to the State agency's IS security policies and standards, agencies can reduce the risk that their system is vulnerable. Cybersecurity⁺⁺⁺⁺ encompasses the majority of topics discussed in this chapter. However, the growing use of the Internet and the World Wide Web includes some additional topics State agencies need to consider.

Key areas include:

- Basic Internet Security
- Web servers
- Web browsers
- Mobile devices

At the most basic level, the web is divided into two principal components: web servers, which are applications that make information available over the Internet (i.e., publish information), and web browsers (i.e., clients), which are used to access and display the information stored on the web servers. The web server is the most targeted and attacked host on most organizations' networks. A web server can be attacked directly or be used as a node to attack a State agency's internal networks. As a result, it is essential to secure web servers and the network infrastructure that supports them.



Refer to the [Defense Information Systems Agency \(DISA\) Security Technical Implementation Guide](#) for detailed guides on Internet and world-wide web security methods.

9.4.9.1 Basic Internet Security Issues

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes identity theft, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

More and more enterprises depend on IT systems and computer networks for essential operations. These systems face large and diverse cyber threats ranging from unsophisticated hackers to technically competent intruders

⁺⁺⁺⁺ The use of "cyber" is most frequently used in the context of Internet and World Wide Web security more than enterprise system security. However, the two are dependent on each other and it is really only a matter of semantics.



using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems.

Cyber security protects the data and integrity of computing assets belonging to or connecting to an organization's network. Its purpose is to defend those assets against all threat actors throughout the entire lifecycle of a cyber-attack. While an organization has a high level of detailed control over their own IS assets, the Internet and the World Wide Web are not so easily controlled. Nonetheless, there are actions State agencies can take to protect their IS and IT resources.

Table 50: Five Common Cyber Threats¹²¹

Threat	Description	Countermeasure
Viruses	A virus is a piece of software that can replicate itself and infect a computer without the permission or knowledge of the user. A virus can only spread when it is transmitted by a user over a network or the Internet, or through removable media such as memory sticks.	Antivirus software detects and eliminates known viruses.
Spam	SPAM is electronic junk email. The amount of spam has now reached 90 billion messages a day. Email addresses are collected from chat rooms, websites, newsgroups and by Trojans which harvest users' address books.	Controlled mostly by Internet Service Providers, State agencies can use spam filters for screening out e-mail messages with suspect titles or from suspect persons, as well email messages from blocked senders.
Spoofing, Phishing and Pharming	<u>Spoofing</u> is an attack in which a person or program masquerades as another. A common tactic is to spoof a website (see phishing). <u>Phishing</u> (pronounced "fishing") is a common form of spoofing in which a phony web page is produced that looks just like a legitimate web page. The phony page is on a server under the control of the attacker. Criminals try to trick users into thinking that they are connected to a trusted site, and then harvest user names, passwords, credit card details and other sensitive information. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging. The email message claims to be from a legitimate source but when the user clicks	As spoofing, phishing, and to a lesser extent, pharming, rely on tricking users rather than advanced technology, the best way to handle these threats is through vigilance. Don't open emails from unknown sources or click on links embedded in suspect messages. Check the security guidelines of websites such as PayPal so that users can distinguish between legitimate and bogus emails. Also, rather than clicking on the link embedded in an email, users can type the



Table 50: Five Common Cyber Threats

Threat	Description	Countermeasure
	on the link provided, he or she lands on the fake web page. <u>Pharming</u> (pronounced “farming”) is an attack in which a hacker attempts to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim’s computer or by exploitation of a vulnerability in Domain Name Systems (DNS) server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses — the servers are the “signposts” of the Internet.	general link in a web browser (e.g., http://www.usda.gov).
Spyware	Spyware is software that is secretly installed on a computer without the user’s consent. It monitors user activity or interferes with user control over a personal computer.	<u>Real-time protection</u>: these programs work just like anti-virus software. They scan all incoming network traffic for spyware software and block any threats that are detected. <u>Detection and removal</u>: users schedule daily, weekly, or monthly scans of their computer to detect and remove any spyware software that has been installed. These antispyware programs scan the contents of the Windows registry, operating system files, and programs installed on a computer. They then provide a list of threats found, allowing the user to choose what to delete and what to keep.
Denial-Of-Service Attack (DOS Attack)	As its name implies, a Denial-of-Service or DoS attack is an attempt to make a computer resource such as a website or web service unavailable to users. One of the most common methods of attack involves saturating the target (victim) machine with external communications requests. The machine then cannot	Use of firewalls, configuration of routers and switches, front-end hardware, and intrusion-prevention systems are common defenses against denial of service attacks.

**Table 50: Five Common Cyber Threats**

Threat	Description	Countermeasure
	respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable.	

When updating the security plan, State agencies can also refer to the security issues and questions in **Table 51** to assess issues related to internet security.

Table 51: Internet Security Issues Checklist

✓	INFORMATION TO BE ADDRESSED
	Describe the functions (e.g., data transfer, forms-based data entry, or browser-based interactive applications, etc.) the Internet is being used to perform.
	Describe your application categories and how they are integrated with your legacy system. For example: • information access = hypertext, multimedia, soft content and data; • collaboration = newsgroups, shared documents and videoconferencing; • transaction processing = Internet commerce and links to IT legacy applications
	What communication protocols are in use? (FTP, HTTP, telnet, or a combination?)
	How do you control access, Identification & Authorization, sensitive or private information, no repudiation, and data integrity?
	Are firewalls and/or proxy servers present? If so, describe the software used.
	Is data encryption used? If so, what level (DESII, MIME, etc.)? Is it hardware or software-based?
	What application languages are being used? (e.g., HTML, XML, JavaScript, etc.) Are these static, semi-dynamic, or dynamic?
	What database connectivity or Application Program Interfaces (API) are in place?
	Do you have separate web servers? Describe hardware and software.
	Describe what controls are in effect for shared resources, including any of the following: password protection, user groups, smartcards, biometrics, data encryption, callback systems, virus scanners, vulnerability scanners, and intelligent agents.

**Table 51: Internet Security Issues Checklist**

✓	INFORMATION TO BE ADDRESSED
	Are user logons/passwords challenged frequently and under a multilevel protection scheme? Do you allow synchronization of passwords for a single sign-on?
	Are passwords changed on a regular basis? How often? Is this system-controlled or manual?
	How many people have administrative rights to the application, telecommunications, and web servers? Are these rights separated by function, or can a single person access all of these?
	Are backups performed of Internet application files and data files? How often?
	Is a contingency plan in place? Has it been tested? How often is it updated?
	Is access by mobile devices and teleworkers subject to the same security controls as in-office users?

9.4.9.2 Web Server Security

Securing the OS that the web server runs on is the initial step in providing security for the web server. (See section **9.4.2.2 - Operating System Security**. The web server software only differs in functionality from other applications that reside on a computer. However, since the web server may provide public access to the computer as well as agency wide or Statewide access, it must be securely configured to prevent the web server and the host computer from being compromised by intruders.

One of the precautions to take when configuring a web server is to never run the web service as a root or administrative user (e.g., super user). Web services or applications should never be located at the root of a directory structure. Instead, they should be in a component-specific subdirectory to provide optimum access management. The web service should be run with the permissions of a normal user. This prevents the escalation of privilege if the web server is ever compromised. Also, the file system of the web server (directories and files) should not be configured to have write access for any users other than those internal users that require such access.

Other precautions and secure configuration issues to consider when configuring a public web server are as follows:

- The web server is on a separate local area network with a firewall configuration or demilitarized zone (DMZ) from other production systems
- The web server will never have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network



- The web server is treated as an untrusted host
- The web server is dedicated to providing web services only
- Compilers are not installed on the web server
- All services not required by the web server are disabled
- The latest contractor software is used for the web server, including all the latest hot fixes and patches

9.4.9.3 Web Browser Security

The web browser is usually a commercial client application used to display information requested from a web server. The State agency should designate a standard browser for use within the system environment. This decision includes evaluating how available browsers work with SNAP, WIC, and EBT systems at the software code and scripting language level. Scripting languages, such as JavaScript and ActiveX (Microsoft), are often very susceptible to breaches. It is recommended that all scripting languages not required for official systems operation be disabled within the web browsers.

9.4.9.4 Mobile Device Security

“Mobile devices allow employees to access information resources wherever they are, whenever they need. The constant Internet access available through a mobile device's cellular and Wi-Fi connections has the potential to make business practices more efficient and effective. As mobile technologies mature, employees increasingly want to use mobile devices to access corporate enterprise services, data, and other resources to perform work-related activities. Unfortunately, security controls have not kept pace with the security risks that mobile devices can pose.”¹²²

“If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to gain unauthorized access to that data. Even worse, a mobile device with remote access to sensitive organizational data could be leveraged by an attacker to gain access to not only that data, but also any other data that the user is allowed to access from that mobile device. The challenge lies in ensuring the confidentiality, integrity, and availability of the information that a mobile device accesses, stores, and processes. Despite the security risks posed by today's mobile devices, enterprises are under pressure to accept them due to several factors, such as anticipated cost savings and employees' demand for more convenience.”¹²³



See [NIST Special Publication 800-124](#) – “Guidelines for Managing the Security of Mobile Devices in the Enterprise” for additional details on mobile device security.

See NIST Special Publication 1800 series – “NIST Cybersecurity Practice Guides” for details on mobile device security.

9.5 Privacy Controls

“In 1974 the Privacy Act sought to balance the government's need to collect information from an individual with a citizen's right to be notified as to how that information was being used, collected, maintained, and disposed of after the requisite period of use. Privacy, with respect to personally identifiable information (PII), is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. In today's digital world, effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII and the environments in which those systems operate. Standardized privacy controls and assessment procedures (developed to evaluate the effectiveness of the controls) will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements.”¹²⁴ This is supported, in part, by designing information systems to support privacy by automating privacy controls.



Personally identifiable information (PII) is defined as information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. – OMB Memorandum 07-16 “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”

9.5.1 Authority and Purpose

The need to protect a person's privacy begins with the authority to collect personal information and the purpose for collecting that information. Without proper authority and a legitimate purpose, no organization, private sector or public sector, has the right to do so. This includes getting consent from the person on whom the information



is being collected. Once personal information is collected, privacy must be respected for PII. Government organizations must identify the legal basis authorizing them to collect particular PII and provide notices specifying what activities they engage in that may impact privacy. This includes identifying the specific program(s) and information system(s) where PII will be collected, used, maintained, and shared. The purpose for using the PII must be included in the notices. In order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

9.5.2 Accountability, Audit, and Risk Management

The accountability, auditing, and risk management controls enhance public confidence through effective controls for governance, monitoring, risk management, and assessment. These controls should be used to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk. State agencies should develop, implement, and maintain organizational governance for privacy to ensure compliance with applicable laws and regulations. This includes federal privacy laws and policy changes affecting the privacy program. Privacy impact and risk assessments should be key components of the governance. These are designed to assess individuals' privacy risks resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. Privacy Impact Assessments are conducted to identify privacy risks and identify methods to mitigate those risks. They ensure that programs or information systems comply with legal, regulatory, and policy requirements. They also serve as notice to the public of privacy practices. Contractors and service providers, along with government personnel, should be required to adhere to the relevant governance and controls. This includes providing relevant privacy awareness training. Finally, the State agency must monitor and audit privacy controls and internal privacy policy to ensure effective implementation.

9.5.3 Data Minimization and Retention

Collecting, using, and retaining PII should be kept to the minimum necessary for supporting the purpose of why it is collected in the first place. State agencies must identify the minimum PII data points needed for the purposes described in the notices and for which the individual consented.

Privacy involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. The State agency should establish a PII retention policy and adhere to it. Once the need for PII data elements passes, the State agency should not retain it any longer than legally authorized. The State agency can reduce their security and privacy risks by reducing their inventory of PII consistent with the authorized purpose. This means performing a periodic PII holding inventory to determine what PII is still needed and what can be disposed of according to record management governance.



“Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the appropriate system security administrator and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.”¹²⁵

9.5.4 Individual Participation and Redress

Good privacy protection includes making individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, these controls enhance public confidence in organizational decisions made based on the PII. People whose information has been collected must understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of their PII. It is incumbent on the State agency to support this understanding. The State agency must also obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII. The State agency may obtain consent through opt-in, opt-out, or implied consent.

Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII. One example of implied consent is by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording. Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. Consent mechanisms should include a discussion of the consequences to individuals of failure to provide PII.

The State agency must allow individuals access to their PII. Access should be based on published rules and regulations. Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors.

Likewise, State agencies must allow individuals a means to correct inaccuracies in their information (i.e., redress). Effective redress processes demonstrate organizational commitment to data quality, especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. The State agency should use discretion in determining if records are to be corrected or amended,



based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals should have a way to appeal an adverse decision and have incorrect information amended, where appropriate.

9.5.5 Transparency

This is simply providing public notice of State agency information practices and the privacy impact of their programs and activities. The State agency should provide effective notice to the public and to individuals regarding its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal. It is complementary to the notices providing the authority and purposes for collecting PII, and how the PII will be used. The consequences of individuals exercising or not exercising those choices in how PII will be collected, used, and shared must be communicated. Access to PII, and for amending or correcting PII, is also communicated. Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how the State agency uses PII generally and, where appropriate, to make an informed decision prior to providing PII to the State agency. Effective notice also demonstrates the privacy considerations that the State agency has addressed in implementing its information practices.

There are different mechanisms for informing the public about their privacy practices. These include, but are not limited to:

- Privacy Impact Assessments
- System of Records Notices
- Privacy reports
- Publicly available web pages
- E-mail distributions, blogs, and periodic publications (e.g., quarterly newsletters)

The State agency may also employ publicly facing email addresses and phone lines, or both, that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

9.5.6 Use Limitation

This set of controls ensures that the State agency only uses PII either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of these controls will ensure that the scope of PII use is limited accordingly. When the State agency needs to share PII externally for authorized purposes, it must enter into appropriate written agreements. The type of agreement might be a Memoranda of Understanding, Memoranda of Agreement, Letter of Intent, Computer Matching Agreement, or similar agreement. Such agreements must specify and enumerate the purposes for which the PII may be used.



9.6 EBT - Specific Controls

State agencies are required to implement and maintain comprehensive security programs for all information systems involved in administering SNAP. In addition to the [7 CFR 277.18\(m\)](#)¹²⁶ requirements, there are additional requirements specific to EBT systems in [7 CFR 274.8\(b\)\(3\)](#).¹²⁷ This includes “A separate EBT security component shall be incorporated into the State agency Security Program for Automated Data Processing (ADP) systems where appropriate as prescribed under §277.18(m) of this chapter.”¹²⁸

9.6.1 EBT Cards

EBT card security consists of card management functions, including the issuance and control of EBT cards. Security issues associated with EBT cards have been raised due to the high frequency of maintenance activities associated with them. These maintenance activities include whenever EBT cards are issued, activated, replaced, and destroyed. Therefore, the potential for fraud exists at many points in the lifecycle of the cards. To mitigate the risk of fraud, several security measures are included with each type of card.

Magnetic stripe cards contain information on benefit recipients (e.g., personal account number and name), which is verified by a central processor before benefit transactions are authorized. Security measures for these types of cards include requirements for conformance to International Organization for Standardization (ISO) standards, and policies for card inventory management, card activation and deactivation, PIN mailing, and card lifecycle.

Smart cards are different from magnetic stripe cards in that they contain a microprocessor and a memory chip that processes transactions offline. With smart cards, the transaction is authorized between the chip and the point-of-sale (POS) terminal. There is no online communication with a central processor at the time of transaction. Security measures for these types of cards include requirements for the operating system, the ability to disable and enable chips, key management, expiration dates, encryption, biometrics verification and security for multi-application cards.

Hybrid cards may contain a combination of different technologies, but in this document, a hybrid card is defined as a smart card with a magnetic stripe. The magnetic stripe may be used to access one type of benefit account, and the smart chip accesses another. Security measures for these types of cards include the same requirements for magnetic stripe cards and smart cards. It also includes controls to prevent security loopholes such as the ability to use the magnetic stripe to access benefits when the smart chip is not functional.

9.6.2 Encryption

Encryption is the transformation of plain text (e.g., readable data) into cipher text (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions. Encryption is implemented with either hardware or software. Software-



based encryption is the least expensive method and is suitable for applications involving low-volume transmissions. The use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved. Large volumes of data are involved in processing EBT.

9.6.3 POS Terminal and ATM Security

EBT recipients gain access to benefits through Point of Sale (POS) terminals located at authorized retailers. Benefit transactions can be performed through online processing, offline processing, and manual processing:

- **Online Processing** - uses a central processor to verify PINs and authorize transactions
 - Requirements include cashier ID and password verification, settlement controls, integrity of transmitted data, and online biometric verification
- **Offline Processing** - performs PIN verification and transaction authorization at the POS
 - Depending on how offline processing is implemented, transactions can be processed in one of two forms
 - They can either be pre-authorized at the POS (e.g., stored locally and then forwarded at a later time to the central processor for authorization), or they can be authorized at a secure POS (transactions are stored on the smart cards only and are never forwarded to a central processor)
 - Requirements for this security element include mutual authentication between the smart card and the POS terminal, non-repudiation controls for transactions, and offline biometric verification
- **Manual Processing** - involves backup procedures for online or offline processing
 - It includes paper vouchers and manual entries
 - Security requirements include policies and controls for sales vouchers (e.g., floor limits), suspense accounts, and settlement

9.6.4 EBT Security Standards

EBT security systems are designed to protect the systems and resources from unauthorized modification, disclosure, and destruction. State agencies are required to extend security provisions into their EBT systems, in addition to security provisions required under other regulations. The areas of additional security measures are storage and control measures, communications access controls, message validation, and administrative and operational procedures.



Periodic security risk analysis of the EBT system is required to address specific areas:

- Vulnerability to theft and unauthorized use
- Completeness and timeliness of the reconciliation system
- Vulnerability to tampering or creation of household accounts
- Erroneous posting of issuances
- Manipulation of retailers accounts

An EBT contingency plan must be approved by FNS prior to implementation and subsequently updated on a periodic basis. See [7 CFR 274.8](#) - Functional and Technical EBT System Requirements¹²⁹ for more information on EBT system standards.

9.7 Security Reviews and Reporting

State agencies regularly review IS security of installations involved in the administration of FNS programs according to State security policy. At a minimum, the reviews evaluate physical and data security, operating procedures, and personnel practices. State agencies are responsible for conducting the security review of systems that administer FNS programs at least biennially. State agencies must provide a written summary of their findings and determination of compliance with requirements to FNS upon request or at least biennially after completion of the Information System Security Review. The State agency includes an action plan with scheduled dates of milestones which, when completed, will correct any security weaknesses.

The reviews are designed to ensure the following:

- Sufficient controls and security measures are in place to compensate for any identified risks associated with the program/system and/or its environment
- The program/system is being operated cost-effectively and complies with applicable laws and regulations
- The program/systems' information is properly managed
- The program/system complies with management, financial, information technology (IT), accounting, budget, and other appropriate standards

9.7.1 Security Plans

The purpose of the systems security plan is to allow State agencies to comply with computer security planning activities. The plan identifies the security safeguards that are in place and planned for the IS to mitigate potential risks that could result in unauthorized disclosure, modification, or destruction of sensitive information stored and processed on a system.



Systems security plans are dynamic documents that portray an assessment of the current IS security status. The plan identifies any policies, procedures, or standards required at the local level. Systems security plans act as input to the State agencies' IS security plan. The security plan summarizes the security of all processing, including personal computers (PCs), remote access, mainframes, and related business operations.

The contents of the Systems Security Plan are outlined in **Table 52**. The objectives of the security plan are the following:

- Provide management with an assessment of security status, including future goals, training needs, and scheduled actions
- Furnish guidance to newly appointed security managers in administering the security program
- Measure progress in achieving targeted goals
- Provide FNS with an IS security status report

Table 52: Contents of the Systems Security Plan

Outline of Topics	Scope Describe the site, giving location configuration, operations, and processing supported and identification of IS units and applications covered by plan
	Definitions Explain any terms that might not be familiar to all readers
	Overall Security Assessment- Discuss State policies and practices, addressing assignment of security responsibilities, personnel security clearance policies, audit reports, and training; also assess current and planned activities for the next year
	Appendices • Site plan and equipment schematic • Sensitive application systems (obtain the following information for each system): ○ Date of last system evaluation ○ Date of last system certification or recertification ○ Date of next evaluation or recertification • Summary of the risk analysis reports • State continuity plan(s) • Summary of the security reviews for all types of processing platforms in use • Training needs with action schedule

Table 52: Contents of the Systems Security Plans

	• Other supporting documents (terminal security rules, local security procedures, user handbooks, etc.)
Policies and Procedures	• Physical security of resources • Equipment security to protect equipment from theft and unauthorized use • Software and data security • Telecommunications security • Personnel security • Continuity plans to meet critical processing needs in the event of short-or long-term interruption of service • Emergency preparedness • Designation of a State agency IS security officer/manager

9.7.2 FNS Security Plan Reviews

When reviewing security plans, FNS looks for the answers to the following questions:

- Does the plan address logical and physical security of the system?
- Does the plan identify and provide corrective actions for security compromises from interfaces with external systems?
- Does the logical security include password protection, data encryption (if applicable), access profiles, to preclude access to the data by unauthorized personnel?
- Does the logical security provide for supervisory intervention if needed (determined case by case)?
- Are negotiable documents or authorizations stored securely?
- Does the physical security address not only the security of the physical devices but also the building security?
- Does the physical security address safety and environment issues?
- Does the security plan address data and application backup procedures?
- Does the security plan include recovery procedures?
- Does the security plan include disaster preparedness and recovery procedures? (These may be in a separate plan.)
- Does the security plan cover both the State and local agencies?
- If a department or agency-wide security plan exists, is there a clear delineation of where the system security plan leaves off and the agency plan takes over or vice versa?



- Does the logical security include separation of duties between functions to prevent potential fraud situations?
- Does the plan address the process to be followed for disposal of equipment and media?

9.8 Security Summary

- The purpose of systems security is to protect a State agency's valuable information resources associated with administering information systems supporting administration of SNAP, WIC, and EBT systems. It is the State's responsibility to develop an Information System (IS) security plan
- State agencies are responsible for implementing and maintaining a program to ensure adequate security is provided for personnel, information collected, processed, transmitted, stored, or disseminated into general support systems and major applications
- Security includes protecting all projects being developed, implemented, and tested, as well as operational systems
- There are three general information technology security control groupings:
 - **Management controls** are used to address those controls that are strategic in nature
 - **Operational controls** address security controls implemented and directly supporting the technical controls and processing environment
 - **Technical controls** are security controls implemented on systems that transmit, process, and store information
 - There are two specific additional IT security controls
 - **Privacy Controls** are the administrative, technical and physical controls safeguarding the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information
 - **EBT-specific controls** are security controls that are unique to an EBT system
- Contingency plans establish recovery procedures that address specific threats. A contingency plan:
 - Documents the process to mitigate risks of business interruption and minimize any disruption of service, both large and small
 - Contains instructions for achieving a full or minimally acceptable set of business operational objectives
 - Involves preparations to respond to external circumstances that may disrupt business operations
- State agencies must regularly review IS security of installations involved in the administration of FNS programs according to State security policy



Endnotes

- ⁹¹ “Information security program”, 7 CFR 277.18 (m), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ⁹² “Information security program”, 7 CFR 277.18 (m)(2), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ⁹³ “Information system security requirements”, 7 CFR 277.18 (m)(1), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ⁹⁴ “Information system security requirements”, 7 CFR 277.18 (m)(1), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ⁹⁵ “Federal Information Security Modernization Act (FISMA)”, Department of Homeland Security <https://www.dhs.gov/fisma>
- ⁹⁶ “Managing Federal Information as a Strategic Resource”, OMB Circular A-130, <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>
- ⁹⁷ “Computer Security”, NIST Special Publication 800, 2016, <http://csrc.nist.gov/publications/PubsSPs.html#SP%20800>
- ⁹⁸ “Risk Management Framework with Cybersecurity Framework”, NIST, <http://www.nist.gov/cyberframework/>
- ⁹⁹ “Guide for Developing Security Plans for Federal Information Systems”, NIST Special Publication 800-18 (Revision 1), February 2006, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>
- ¹⁰⁰ “Guide for Conducting Risk Assessments: Information Security”, NIST Special Publication 800-30 (Revision 1), September 2012, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- ¹⁰¹ “Contingency Planning Guide for Federal Information Systems”, NIST Special Publication 800-34 (Revision 1), May 2010, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>
- ¹⁰² “Guide to Information Technology Security Services”, NIST Special Publication 800-35, October 2003, <http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>
- ¹⁰³ “Security and Privacy Controls for Federal Information Systems and Organizations”, NIST Special Publication 800-53 (Revision 5), September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- ¹⁰⁴ “Computer Security Incident Handling Guide” NIST Special Publication 800-61 (Revision 2), August 2012, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- ¹⁰⁵ “Systems Security Engineering, Volume 1”, NIST Special Publication 800-160, November 2016, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf>
- ¹⁰⁶ “National Checklist Program for IT Products – Guidelines for Checklist Users and Developers”, NIST Special Publication 800-70 (Revision 4), February 2018, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf>
- ¹⁰⁷ “Guidelines for Media Sanitization”, NIST Special Publication 800-88 (Revision 1), December 2014, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>



-
- ¹⁰⁸ “Technical Guide to Information Security Testing and Assessment”, NIST Special Publication 800-115, September 2008, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- ¹⁰⁹ “Guidelines for Managing the Security of Mobile Devices in the Enterprise” NIST Special Publication 800-124 (Revision 1), June 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
- ¹¹⁰ “Executive Order 13636, Improving Critical Infrastructure Cybersecurity”, Federal Register, February 12, 2013. <https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>
- ¹¹¹ “Security Technical Implementation Guides (STIGs)”, Defense Information Systems Agency, <https://public.cyber.mil/stigs/downloads/>
- ¹¹² “SNAP Provisions of the Agricultural Act of 2014 implementing Memorandum”, U.S. Department of Agriculture Food and Nutrition Service, March 21, 2014, <https://www.fns.usda.gov/snap/snap-provisions-agricultural-act-2014-implementing-memorandum>
- ¹¹³ “Assessing Security and Privacy Controls in Federal Information Systems and Organizations”, NIST Special Publication 800-53A (Revision 5), September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- ¹¹⁴ “Security reviews”, 7 CFR 277.18 (m)(1) and 277.18 (m)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ¹¹⁵ “Applicability”, 7 CFR 277.18 (m)(4), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8
- ¹¹⁶ “Guide for Developing Security Plans for Federal Information Systems, section 3.14 Minimum Security Controls”, NIST Special Publication 800-18 (Revision 1), February 2006, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>
- ¹¹⁷ “Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalog”, NIST Special Publication 800-53 (Revision 5), September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- ¹¹⁸ “Guidelines for Media Sanitization”, NIST Special Publication 800-88 (Revision 1), December 2014, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
- ¹¹⁹ “State Plan”, 7 CFR 246.4 (a)(26), U.S. Government, https://ecfr.io/Title-07/se7.4.246_14
- ¹²⁰ “National Checklist Program for IT Products – Guidelines for Checklist Users and Developers”, NIST Special Publication 800-70 (Revision 4), February 2018, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf>
- ¹²¹ “The 11 most common computer security threats... And what you can do to protect yourself from them”, Norton Symantec, http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx
- ¹²² “Cybersecurity Practice Guides”, NIST Special Publications 1800s, <https://csrc.nist.gov/publications/sp#SP1800>
- ¹²³ “Cybersecurity Practice Guides”, NIST Special Publications 1800s, <https://csrc.nist.gov/publications/sp#SP1800>
- ¹²⁴ “Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalog”, NIST Special Publication 800-53 (Revision 5), September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>



¹²⁵ "Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalog, Minimization Of PII Used in Testing, Training, and Research", NIST Special Publication 800-53 (Revision 5), September 2020, <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

¹²⁶ "Information system security requirements and review process", 7 CFR 277.18 (m), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8

¹²⁷ "Functional and technical EBT system requirements: System Security", 7 CFR 274.8 (b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=a18b73a0c670d409f4080b898a333f48&mc=true&node=se7.4.274_18&rgn=div8

¹²⁸ "System Security", 7 CFR 274.8(b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=a18b73a0c670d409f4080b898a333f48&mc=true&node=se7.4.274_18&rgn=div8

¹²⁹ "Functional and technical EBT system requirements", 7 CFR 274.8, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=a18b73a0c670d409f4080b898a333f48&mc=true&node=se7.4.274_18&rgn=div8



A1. Acronyms and Glossary of Terms

A1.1 Acronyms

Acronym	Meaning
ADP	Automated Data Processing
ADR	Alternative Dispute Resolution
ALCM	Acquisition Lifecycle Management
ANSI	American National Standards Institute
APD	Advance Planning Document
APDU	Advance Planning Document Update
AV	Anti-Virus
BAFO	Best and Final Offer
BCD	Business Capability Definition
BPA	Business Process Analysis
BPR/I	Business Process Reengineering/Improvement
CAP	Cost Allocation Plan
CBA	Cost Benefit Analysis
CCB	Change Control Board
CFR	Code of Federal Regulations
CIO	Chief Information Office or Chief Information Officer
CM	Configuration Management
CMOS/PROM	Complementary Metal Oxide Semiconductor / Program Read-Only-Memory
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representatives
DBMS	Database Management System
DDI	Design, Development, and Implementation
DISA	Defense Information Systems Agency



Acronym	Meaning
<i>DLCM</i>	Data Lifecycle Management
<i>DMZ</i>	Demilitarized Zone
<i>EAR</i>	Emergency Acquisition Request
<i>EBT</i>	Electronic Benefit Transfer
<i>FAR</i>	Federal Acquisition Regulation
<i>FFP</i>	Federal financial participation
<i>FFR</i>	Federal Financial Report (Form FS-425)
<i>FISMA</i>	Federal Information Security Modernization Act of 2014
<i>FM</i>	Financial Management
<i>FNS</i>	Food and Nutrition Service
<i>FRD</i>	Functional Requirements Document
<i>GCD</i>	Gold Copy Database
<i>IAPD</i>	Implementation Advance Planning Document
<i>IAPDU</i>	Implementation APDU
<i>IEEE</i>	Institute of Electrical and Electronics Engineers
<i>IP</i>	Internet Protocol
<i>IS</i>	Information System or Information Systems. Singular and plural used interchangeably.
<i>ISO</i>	International Organization for Standardization
<i>ISSO</i>	Information Systems Security Office
<i>IT</i>	Information Technology
<i>IV&V</i>	Independent Verification and Validation
<i>LAN</i>	Local Area Network
<i>M&O</i>	Maintenance and Operations
<i>MIS</i>	Management Information Systems
<i>MOU</i>	Memorandum of Understanding
<i>NASPO</i>	National Association of State Procurement Officials
<i>NIST</i>	National Institute of Standards and Technology



Acronym	Meaning
NSA	Nutrition Services and Administration
OA	Operational Adjustment Funds
OMB	Office of Management and Budget
OS	Operating System
PAPD	Planning Advance Planning Document
PAPDU	Planning APDU
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Project Manager
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMLC	Project Management Lifecycle
PMP	Project Management Professional
POAM	Plan of Actions and Milestones
PoP	Period of Performance
POS	Point of Sale (Terminal)
QA	Quality Assurance
QC	Quality Control
RACI	Responsible Accountable Consult Inform
RFI	Request for Information
RFP	Request for Proposal
RO	Regional Office
ROM	Rough Order of Magnitude
RTM	Requirements Traceability Matrix
SAE	State Administrative Expense
SAM	State Agency Model



Acronym	Meaning
<i>SDLC</i>	Systems Development Lifecycle
<i>SIRT</i>	System Integrity Review Tool
<i>SLA</i>	Service Level Agreements
<i>SNAP</i>	Supplemental Nutrition Assistance Program
<i>SOA</i>	Service Oriented Architecture
<i>SOW</i>	Statement of Work
<i>SSO</i>	State Systems Office
<i>STIGS</i>	Security Technical Implementation Guides
<i>STLC</i>	Software Testing Lifecycle
<i>T&I</i>	Transfer and Implementation
<i>T&M</i>	Time and Material Contract
<i>TANF</i>	Temporary Assistance for Needy Families
<i>UAT</i>	User Acceptance Test or User Acceptance Testing
<i>URL</i>	Uniform Resource Locator
<i>V&V</i>	Verification and Validation
<i>WAN</i>	Wide Area Network
<i>WBS</i>	Work Breakdown Structure
<i>WIC</i>	Special Supplemental Nutrition Program for Women, Infants, and Children



A1.2 Glossary of Terms

A

Acceptance Documents – Documents signed by the State agency to indicate the State’s satisfaction that a contractor has completed a phase of work in accordance with contract requirements. The information upon which and the methods by which a State agency is to base its decision, including documentation of the work product that the contractor is to furnish, should be agreed upon in advance. Acceptance documents contain information a State agency uses to base its decision that the system is the correct system for its use and performs to contract expectations. These documents include documentation of the work performed and the product the contractor provided.

Acceptance Testing – See User Acceptance Testing

Acquisition – A purchase of supplies or services through a purchase or lease, regardless of whether the supplies or services are already in existence or must be developed, created, or evaluated.

Advance Planning Document (APD) - Document used to secure funding and approval of the project to automate State processes to administer the SNAP or WIC programs. This document records information for the APD process, which is designed to: (1) describe in broad terms the State agency’s plan for managing the design, development, implementation, and operation of a system that meets Federal, State, and user needs in an efficient, comprehensive, and cost-effective manner; (2) establish system and FNS program performance goals in terms of projected costs and benefits, and (3) secure FFP for the State agency.

Advance Planning Document (APD) Process – Process used by several Federal agencies to receive and approve State agency requests for federal funding or FFP for information systems (IS). The Advance Planning Document (APD) process is a series of successive steps through which State agencies obtain federal prior approval of and Federal financial participation (FFP) in automation projects supporting Food and Nutrition Service (FNS) programs. This includes all certification and eligibility systems and Electronic Benefit Transfer (EBT) system projects.

Advance Planning Document Update (APDU) - Annual or as-needed documentation submitted by the State agency on the status of project development activities and expenditures in relation to the approved PAPD. An annual APDU is due 60 days before the anniversary of the approval date of the initial IAPD or PAPD. An APDU may also be submitted as needed to request funding approval for project continuation whenever significant project changes occur or are anticipated. Advance Planning Document Update (APDU) means a document submitted annually (Annual APDU) by the State agency to report the status of project activities and expenditures in relation to the approved Planning APD or Implementation APD or on an as needed basis (As Needed APDU) to request funding approval for project continuation when significant project changes occur or are anticipated.



Alternatives Analysis – A key part of the Feasibility Study in which alternatives for primary system requirements and resources are contrasted and compared with the aim of determining the best viable alternative. Comparative analysis includes development resources, implementation resources, functional requirements, hardware and software requirements, and M&O support and costs.

Automated Clearinghouse (ACH) – The primary system that agencies use for electronic funds transfer (EFT).

B

Benefiting Program – State or Federal public assistance program that uses some or all of the functions of a State agency's automated computer system. For example, the SNAP, Medicaid, TANF and Child Support Enforcement may all be benefiting programs in a shared State computer system that determines applicants' eligibility.

Best and Final Offer (BAFO) – Technical and cost proposal that is submitted by a vendor to a State or local agency after all negotiations are concluded and that is the offer upon which the contracting decision is made.

Black-box Testing – A software test method that checks for functions (requirements) of an application or system. The test engineer does not have to have an in-depth knowledge of the code constructs but must understand the functional specifications.

Budget – The source of the financial information needed to make valid decisions concerning cost-benefit analyses and overall cost controls and to determine funding availability. Technically, it is "aggregating the estimated costs of individual activities or work projects [establishing] an authorized cost baseline." For APD purposes, it must reflect the total anticipated project cost, including Federal and State shares. Accurate reporting of IS expenditures is also required to perform reconciliations against budgeted and approved funding levels. The Planning APD budget is designed to capture quarterly costs for the entire planning phase of the project, including all anticipated expenditures. The Implementation APD budget is designed to capture quarterly costs for the life of the project through full implementation. The APDU budget format is designed to capture actual costs quarterly throughout the life of the project and to compare them with original cost estimates as well as future estimates.

Business Rules Engine – Software that applies business rules to a decision-making process in a software application. The rules may come from legal regulation (the categories of person eligible for a program), state policy (whether and how to count certain assets), or other sources. The rules engine software, among other functions, may help classify, prioritize and manage all these rules, verify consistency of formal rules, and relate rules to multiple applications as appropriate. Business rules can also be used to detect certain favorable and unfavorable situations automatically.



C

Capacity – Measure of a State agency's output, program participation rates or other federal reporting requirements, for example.

Change Control Board (CCB) – A formally charted group responsible for reviewing, evaluating, approving, delaying, or rejecting changes to the project. The CCB records and communicates such decisions.

Central Service Cost Allocation Plan (CSCAP) – The documentation identifying, accumulating, and allocating or developing billing rates based on the allowable costs of services provided by a state, local government, or Indian tribe on a centralized basis to its departments and agencies. The costs of these services may be allocated or billed to users.

Cognizant Federal Agency – Federal agency charged with reviewing, negotiating, and approving the Cost Allocation Plan of a given State or local government agency. Cognizance is generally assigned to the federal agency that has the greatest dollar involvement with the grantee. It may differ for ongoing operational costs and for a specific project such as an APD project.

Commercial Off The Shelf (COTS) – Proprietary software products that are ready-made and available for sale to the general public at established catalog or market prices in which the software vendor is not positioned as the sole implementer or integrator of the product.

Configuration Management (CM) – Control of changes, including the recording thereof, that are made to the hardware, software, firmware, and documentation throughout the system lifecycle; a discipline applying technical and administrative controls to identifying, documenting and reporting on configuration items, their physical and functional characteristics and changes to characteristics of those configuration items throughout the system lifecycle.

Contingency Plan – A secondary or alternative course of action that can be implemented in the event the primary approach fails to function as it should. Plans of this type allow projects to quickly adapt to changing circumstances and remain active. A contingency plan specifies the risk indicator to be measured, the frequency of measurement, the problem trigger, the action plan, and the specified duration for the contingent actions to resolve the problem.

Contractor – Firm, vendor, or person that is party to a contract to furnish supplies and/or equipment or perform work at a certain price or rate in support of FNS-funded IS.

Contractor and Procurement Documentation – Collection of legal and binding documentation that has been agreed to for a specific contract.

Cost Allocation – Procedure that State agencies use to identify, measure, and equitably distribute system costs among benefiting State and public assistance programs.



Cost Allocation Methodology – Specific method or approach the State agency uses to determine each benefiting program’s portion of the shared system costs.

Cost Allocation Plan (CAP) – Documentation identifying, accumulating, and distributing allowable costs of program administration together with the allocation methods used. The two types of Cost Allocation Plan are central service cost allocation plan and public assistance cost allocation plan. A central service CAP is used when several agencies share a service such as a motor pool. The public assistance CAP is a way for State agencies carrying out federal awards to charge indirect costs to a federal agency using a specified indirect cost rate.

Cost Allocation Services (CAS) – A service providing indirect cost rate and cost allocation plan negotiation services to Federal Departments and Agencies where DHHS is designated by OMB as the Cognizant Federal Agency.

D

Data Conversion – Any activity involved in the following manipulations of data: creating a data file from existing files, either manually or through electronic means; converting during system development from an existing system, paper or automated, to the new system and testing for correctness and data integrity; changing over the caseload from the old system to the new system. This is often accomplished in phases, with different State subdivisions being converted at different stages. A conversion plan outlining the strategy, requirements, schedule and validation process for transfer of the caseload to the new system and related data conversion should be included in the IAPD.

Demilitarized Zone (DMZ) – A physical or logical subnetwork (sometimes referred to as a perimeter network in computer security) that adds an additional layer of security to an organization's local area network (LAN) when it is exposed to a large and potentially untrusted network such as the Internet. The term is derived from an area between nation states in which military operation is not permitted.

Design, Development, and Implementation (DDI) – The process of defining, designing, developing, testing, and implementing a new software application or program.

Detail System Design or Detailed Design Document – Specification of the program/file level design of a system. This document describes a software product that a software designer writes to guide a software development team in the architecture of the software project. It usually accompanies an architecture diagram and has pointers to the detailed feature specifications of smaller pieces of the design. A design document is required as a practical measure to coordinate a large team under a single vision. It needs to be a stable reference and outline all parts of the software and how they will work. The document should give a fairly complete description while maintaining a high-level view of the software. Detail System Design is a comprehensive software design model consisting of these four distinct but interrelated activities: data design, architectural design, interface design, and procedural design.



Direct Charges – Charges for costs of system capabilities that benefit only a single Federal or State program. In cost allocation methodology, direct charges are identified and then removed from the cost allocation pool.

Direct Costs – Costs for system functions benefitting only a single Federal or State program. Direct costs are those that can be identified specifically with a particular cost objective. These costs may be charged directly to the Program, contracts, or other programs against which costs are finally lodged. Direct costs may also be charged to cost objectives used for the accumulation of costs pending distribution in the course to programs and other ultimate costs objectives.

Disallowance - Recovery of funds that were inappropriately charged to an FNS grant.

E

End-to-End Testing - Testing used to demonstrate whether the flow of an application is performing as designed. This includes every step from beginning to end for the full cycle of performance. The purpose is to identify system dependencies and ensure that the correct information is passed between various system components and systems.

Enhancement - Any modification that will change the functions of software and hardware beyond their original purposes or to improve operational performance of the software or hardware, not just to correct errors or deficiencies which may have been present in the software or hardware or to improve operational performance of the software or hardware. A major enhancement is a software change that significantly increases risk, cost, or functionality of the system.

Enterprise - Whole or portion of the any State agency (or additional agencies) that is affected by change in the IT infrastructure. This scope is necessary to establish the boundaries within which the State agency decision makers can manage the interoperability and integration within and across this boundary.

Entry Criteria - The minimum set of conditions that should be completed in order to start testing.

Exit Criteria - The minimum set of conditions that should be met in order to close a particular test phase.

F

Feasibility Study (Also called feasibility analysis) – An analysis and evaluation of a proposed project to determine if it (1) is technically feasible, (2) is feasible within the estimated cost, and (3) will be profitable. Feasibility studies are almost always conducted where large sums are at stake. It is a phase of a system development lifecycle (SDLC) methodology that researches the feasibility and adequacy of resources for the development or acquisition of a system solution to a user need.



Federal Financial Participation (FFP) – The portion or amount of allowable costs (up to 100 percent) that a federal grantor agency provides through a grant, contract, or other agreement. Specifications shall be based upon a clear level of funding established through legislation or regulation. This is the net amount provided by the federal participating agency.

Financial Management Review – Reviews conducted in order to obtain reasonable assurance that the financial information reported by grantees, such as State agencies and Indian Tribal Organizations, is correct and complete; that it represents proper expenditures of federal funds made available to such organizations; and/or that such organizations have otherwise complied with applicable financial requirements.

Functional Requirements Document (FRD) – Initial definition of the proposed system, which documents the goals, objectives, and user or programmatic requirements. This document details what the new system and/or hardware should do, not how it is to do it. Specifications shall be based upon a clear and accurate description of the functional requirements for the project and shall not, in competitive procurement, lead to requirements that unduly restrict competition. The FRD specific to the WIC program includes EBT readiness and functionality.

G

General System Design – A combination of narrative and diagrams describing the generic architecture of a system, as opposed to the detailed architecture of the system, but which may also include the following details: a system's diagram; a narrative identifying overall logic flow and systems functions; a description of equipment needed (including processing, data transmission, and storage requirements); a description of other resource requirements that will be necessary to operate the system; a description of system performance requirements; and a description of the environment in which the system will operate, including how the system will function within the environment.

Go/No-Go Decision (Also known as Project Gates) – Points in time during which the project team may decide whether to move forward to the next phase of the project. It also provides stages at which all documentation should be up to date before moving forward. Go/No-Go Decision points may occur at any logical phase of a project but become increasingly important based upon how far into the SDLC a project is. These points allow the project team and manager time to analyze the current state of the project, including documentation, business needs, unresolved defects, testing results, training outcomes/feedback, and so on, to determine if the project should move forward to the next phase. Funding sources may dictate these decision points as temperature checks to determine if the project is still viable and on a realistic schedule. Go/No-Go determinations are scheduled after UAT and Pilot but may be set by FNS at any time during development.

H



I

Implementation Advance Planning Document (IAPD) – A written plan of action requesting FFP (approval to expend federal funds) to acquire and implement IS services and/or equipment. The IAPD includes the design, development, testing, and implementation phases of the project.

Independent Verification and Validation (IV&V) - Review process performed by an organization that is technically, managerially, and financially independent of the development organization. Verification uses iterative processes to determine whether the products produced fulfill the requirements placed on them by previous iterations/phases/steps and are internally complete, consistent, and sufficiently correct to adequately support the next iteration/phase/step. Validation is the process of examining and exercising the complete application (software, hardware, procedures, and all else) to determine whether all stakeholders' requirements have been met.

Information System or Information Systems (IS) – Combinations of computer hardware, software, data, and telecommunications that perform specific functions to support the State agency or other Federal, State or local organizations. Commonly used in 7 CFR 277.18 and HB901 to refer to eligibility and issuance systems.

Information System Services – Services to design, develop, or operate IS equipment, either by private sources or by employees of the State agency or by State or local organizations other than the State agency, to perform such tasks as feasibility studies, system studies, system design efforts, development of system specifications, system analysis, programming, system implementation, maintenance, operations, backup and recovery, and disposition. IS services also include system training, system development, site preparation, data entry, and personnel services related to IS development and operations.

Integration Testing - The phase of the system development lifecycle in which application programs or modules that were separately developed and tested are brought together and operated as a single system. The objective of integration testing is to ensure that all elements of a system function correctly according to specifications and defined requirements as a single entity. Integration testing ensures that data and output from one program or module that function as input to or is used by another program or module are correctly processed.

Invitation for Bid – Type of solicitation document used in formal advertising, the primary considerations of which are cost and the expectation that competitive bids will be received and an acceptance (award) issued to the low responsive, responsible bidder.

J



K

L

Legacy System – Jargon for an IS (or set of applications) currently in use that was initially deployed many years ago and that uses a computing infrastructure that is several generations old. These systems tend to be critical to the business and cannot be easily replaced or cost-effectively maintained; however, they are approaching or have reached the end of their practical operational life span.

M

Maintenance –The process of modifying a system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment with the purpose of maintaining the value of the existing system. Required activities should be undertaken to conserve, as nearly and for as long as possible, the original condition of an information system while compensating for normal updates to keep the IS operating.

N

Nutrition Services and Administration (NSA) Grant – The regular federal WIC grant covering a State's administrative expenses.

O

Operational – A concept, with both general and specific meanings in FNS programs, referring to the point in the project development at which the major functions of the automated system are functioning to support program activity. For example, the new system is being used to certify recipients and to provide benefits in local offices. An IS system may become operational before all project work included in an approved APD is completed. For example, a system may be considered operational, although there are still ancillary functions being built. A system is considered truly operational statewide once all development under the IAPD is completed, all sites are fully operational, and all work has been accepted by the State agency. Operational also signifies the point at which the reporting of costs moves from the Automated Data Processing (ADP) Development to ADP Operational on the FNS-269 (through FY 2011) or FNS-425 (beginning FY 2012) or FNS-798 documents submitted by all State agencies. The closure of an APD may occur after a system is considered fully operational statewide.



In the specific meaning, operational refers to the SNAP regulatory meaning for implementation of Food and Nutrition Act provisions for enhanced funding for development projects. For projects with phased implementation, each State subdivision (as outlined in the Case Conversion or Implementation/Rollout Plan) shall be considered operational at the time that the system produces automated application processing and/or issuance for the SNAP caseload for that subdivision.

Operational Adjustment (OA) – The limited federal funding allocated each year in the WIC Program for special projects such as computer systems.

Operations – The operating of the IS and networks. It may include the day to day procedures for operating the system, performing routine housekeeping procedures on the system, reviewing error logs and responding to any issues, and performing end of period (e.g. daily, monthly) procedures to include creating backup of key data files.

Order of Precedence – Clause or paragraph included in a contract citing the order of importance of documents to be used in the definition of terms and work, most importantly in dispute resolution should questions or challenges arise.

P

Performance Testing – The process of validating the effectiveness of computer hardware or software to ensure that a system meets performance specifications, especially under the expected workload. (See **Chapter 6 – “Test Planning”** for additional information.) Common types of performance testing include:

- Load testing
- Stress testing
- Endurance testing
- Spike testing
- Capacity testing
- Configuration testing
- Volume testing
- Scalability testing
- Response time
- Bottlenecking

Pilot – The phase of the system development lifecycle in which a fully functional prototype of the entire system is tested in a live environment before it is rolled out and implemented statewide. Pilots must operate until a state of routine operation is reached with the full caseload in the pilot area. The design of the pilot must provide the opportunity to test all components of the system as well as the data conversion process and system performance.



The duration of the pilot must be for a sufficient period of time to thoroughly evaluate the system, usually a minimum of three months. The results of Pilot testing must be provided to FNS before the system is implemented statewide.

Planning Advanced Planning Document(PAPD) – A brief written plan of action that requests FFP to accomplish the planning activities necessary for a State agency to determine the need for, feasibility of, and projected costs and benefits of an IS equipment or services acquisition, to plan the acquisition of IS equipment and/or services, and to acquire information necessary to prepare an Implementation APD.

Platform – Collection of tightly integrated computing hardware, peripherals, OS, and middleware upon which an application is built. The application provides some of its functionality by accessing services residing on the application platform through a program interface.

Program – SNAP, WIC, and Food Distribution conducted under the Food and Nutrition Act of 2008 and regulations.

Project – A related set of information technology tasks, undertaken by a State, to improve the efficiency, economy and effectiveness of administration and/or operation of its health or human services programs. A project may also be a less comprehensive activity such as office automation, enhancements to an existing system, or an upgrade of computer hardware.

Project Management – The application of knowledge, tools, skills, and techniques to project activities and teams for meeting project requirements and competing demands accomplished by integrating and applying the project management processes of initiating, planning, executing, controlling, integrating, and closing. Successful project management includes identifying requirements; establishing goals; balancing demands of quality, time, scope, and cost; and adapting the specifications, plans, and approach to meet the needs and expectations of stakeholders.

Project Management Plan - A document that defines how the project is executed, monitored, and controlled. It is detailed and composed of one or more subsidiary management plans and other planning documents. It describes the project oversight, reporting requirements for the State and contractor, and how the State will achieve professional project management.

Q

Quality Assurance (QA) – Planned and systematic set of actions to provide adequate confidence that work products and the processes used to produce them conform to established requirements.



R

Regression Testing – The process of testing a software system program that has been modified to ensure that any bugs have been fixed, that no other previously working functions have failed as a result of the modifications, and that newly added features have not created problems with previous versions of the software.

Request for Proposals (RFP) – The document used for public solicitation of competitive proposals from qualified sources as outlined in 7 CFR 277.14(g)(3). It is the solicitation document used in negotiated procurements with the expectation that proposals will be received and evaluated leading to an award without discussion, or to a revised proposal after discussion which will then lead to an award.

Risk Management Plan – Document that describes the risk analysis and management processes to be used, including a listing of current risks, their priority, and planned strategies for their mitigation.

S

Security Plan – A description of the security and interface requirements to be employed and the system failure and disaster recovery/business contingency procedures available to be implemented. It includes the approach for ensuring the physical, electronic, and operational security of the system, including hardware, software, data, communications, facilities, and goods.

Service Agreement – The document signed by the State or local agency and the State or local IT department for IT services such as telecommunications, network installation and maintenance, hardware installation, and maintenance system planning services that are to be provided to the State or local agency.

State – Any of the 50 States of the United States, the District of Columbia, Puerto Rico, Guam, the Northern Mariana Islands, the U.S. Virgin Islands, and the reservation of an Indian Tribal Organization that meets the requirements for participation as a State agency as defined by individual FNS programs.

State Agency – Any agency of State government, including the local offices thereof, which is responsible for the administration of the federally-aided public assistance programs within the State. In those States where such assistance programs are operated on a decentralized basis, this includes the counterpart local agencies which administer such assistance programs for the State agency and the Indian Tribal Organization of any Indian tribe determined by the Department to be capable of effectively administering a supplemental nutrition assistance program or a Food Distribution Program in accordance with provisions of the Food and Nutrition Act of 2008.

Status Reports – Information a contractor provides to the State agency regarding performance progress or issues for a specific contract.



Stress Testing – The phase of testing of software or hardware to determine the stability of a system and whether its performance is satisfactory outside standard usage specifications, such as under any extreme and unfavorable conditions.

Sub-agency – Any State or local government entity to which the State agency provides FNS funds in connection with the administration of FNS programs.

Subcontractor - A private, profit, or nonprofit organization that performs a portion of the services required by a State agency through a contractual agreement with the prime contractor.

System Architecture – Representation of a system in which there is a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture, and human interaction with these components. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system.

System Design – Specification of the working relations between all the parts for systems in terms of their characteristic actions.

System Development Life Cycle (SDLC) – A system development process independent of software or other Information Technology considerations. It is the development or application development process used to develop an IS, including requirements, validation, testing, training, and user ownership through investigation, analysis, design, implementation, and maintenance.

System Specifications – The exact models, brands, and suppliers for each software application and hardware device and information about the new IS system, such as workload descriptions, input data, information to be maintained and processed, data processing techniques, and output data required to determine what IS equipment and software are necessary to implement the system design.

System Study – Examination of existing information flow and operational procedures in an organization.

Systems Testing- A series of development tests leading up to the user acceptance test. Systems testing elements include unit, integration, and regression testing.

T

Test Case – A set of test inputs, execution conditions, and expected results developed for a particular objective.

Test Phase – The period of the SDLC prior to any systems test activities during which the plan is completed and submitted. This phase starts when the test plan for the systems test has been approved by FNS.

Test Plan – Description of how all system testing will be conducted, including but not limited to unit testing, integration testing, performance testing, end-to-end testing, and regression testing. At a minimum, a test plan



should address the types of testing to be performed, organization of the test team and associated responsibilities, test database generation, test case development, test schedule, pass/fail criteria, and documentation of results. As a documentation requirement, a final test plan for UAT must be submitted to FNS prior to beginning the testing phase.

Test Script – A sequence of test steps (set of instructions) that attempt to verify the system under test functions as expected. These scripts usually are automated and are written using a scripting programming language.

Training Plan – Description of how all system users will be provided with training on the IS or application.

Transfer and Implementation (T&I) – The transfer of a system, component, or data from one hardware or software environment to another. Any planned or desired modifications to the current “core” code are kept to a minimum. When a State agency is transferring a system, requirements for the T&I must include any enhancements and code modifications.

U

Unit Testing – The phase of testing individual units or components in the software application to validate that each unit of the software performs as designed. The primary goal of unit testing is to take the smallest piece of testable software in the application, isolate it from the remainder of the code, and determine whether it behaves exactly as expected.

Use Case – Technique for capturing functional requirements of systems and systems of systems. Each use case provides one or more scenarios that convey how the system should interact with the users, called actors, to achieve a specific business goal or function.

User Acceptance Testing (UAT) – The phase of the SDLC in which an application is tested, usually by or in conjunction with users, to ensure that the application is functioning according to specifications and defined requirements and is acceptable to users. Stress and performance testing is often also a part of acceptance testing.

V

W

Waiver of Depreciation – A written request to change the method of accounting and claiming for the cost of equipment. For individual items of equipment that cost more than \$25,000 per item, federal cost circulars require that depreciation must be charged over the useful life of the equipment. The written request asks for agency permission to charge the entire cost of the equipment acquisition at the time of acquisition (more commonly



known as “expensing”). Unless agency permission is received, the equipment cost must be based on depreciation over the life of the equipment, not all at once. This is not a specific form or format for this request. Waivers of depreciation are normally granted only if it is cost-beneficial to FNS.

White-box Testing - A software test method that checks internal structures and logic paths of an application or system. The test engineer must understand the design and code to use this method effectively.

X

Y

Z



A2. Regulations

Table 53: Regulations

Regulatory Citation /Program	Web link	Description
7 CFR 246.12 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=06618a8aa8a30f74b89fe73002c82d34&mc=true&node=se7.4.246_112&rgn=d_iv8	Outlines requirements for any delivery system, including EBT, and assigns FNS the oversight responsibility of ensuring that any EBT system provides adequate safeguards and adheres to all provisions.
7 CFR 272.10 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=06618a8aa8a30f74b89fe73002c82d34&mc=true&node=se7.4.272_110&rgn=d_iv8	Although the requirement for an “ADP/CIS Model Plan” is obsolete, the high level requirements in 7 CFR 272.10(b)(1), (b)(2)(vii) through (xiii), and (b)(3) remain valid.
7 CFR 277.14 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=e3ad9bf19e22de01d568e0b96ff18ffe&mc=true&node=se7.4.277_114&rgn=div_8	Specifies procurement standards
7 CFR 274.2 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=06618a8aa8a30f74b89fe73002c82d34&mc=true&node=se7.4.274_12&rgn=d_iv8	Providing benefits to participants
7 CFR 274.8 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=06618a8aa8a30f74b89fe73002c82d34&mc=true&node=se7.4.274_18&rgn=d_iv8	EBT Technical Requirements and Specifications
2 CFR 277.11 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=70303d176f61d6c16b1f9c01c4404a4f&mc=true&node=se7.4.277_111&rgn=d_iv8	Financial Reporting Requirements
2 CFR 277.18 (SNAP adopted by WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=4af6e78e46e59efd10811427496ac4c1&mc=true&node=se7.4.277_118&rgn=d_iv8	Stipulates payments of certain administrative costs of State agencies for establishment of an Automated Data Processing (ADP) and Information Retrieval System.



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
2 CFR 200.102 (All USDA)	http://www.ecfr.gov/cgi-bin/text-idx?SID=00d151a75d85c4bed76dd20ceb9e0906&mc=true&node=se2.1.200_1102&rgn=div8	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments Regulations—Additions and Exceptions
2 CFR 200.313 (All USDA)	http://www.ecfr.gov/cgi-bin/text-idx?SID=00d151a75d85c4bed76dd20ceb9e0906&mc=true&node=se2.1.200_1313&rgn=div8	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments Regulations—Equipment
2 CFR 200.448 (All USDA)	http://www.ecfr.gov/cgi-bin/text-idx?SID=d8bd8ac0ac78ebf0f7d49a4bb0f4c0b0&mc=true&node=se2.1.200_1448&rgn=div8	Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments Regulations—Copyrights



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
7 USC 51 (The Food Stamp Act (FSA) of 1977)	https://www.fns.usda.gov/farmbill	Enacted to strengthen the agricultural economy, help achieve a fuller and more effective use of food abundances, and provide for improved levels of nutrition among low-income households, including: • The Secretary's authority to issue regulations, define standards, and require corrective actions by States to achieve effective and efficient administration of the Food Stamp Program (now the Supplemental Nutrition Assistance Program (SNAP)) • The requirement that States make the program and its records available for federal inspection • The Secretary's authority to seek injunctions and financial sanctions to secure State compliance with the FSA and its regulations • Model Plan requirements for information systems • General funding provisions
42 USC 1786 (Child Nutrition Act of 1966 - WIC)	http://www.fns.usda.gov/wic/wic-laws-and-regulations	It is the purpose of the program authorized by this section to provide, up to the authorization levels set forth in subsection (g) of this section, supplemental foods and nutrition education, including breastfeeding promotion and support, through any eligible local agency that applies for participation in the program.



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
2 CFR 200.416-200.417	http://www.ecfr.gov/cgi-bin/text-idx?SID=8fc53bd6c2662141601f5431b69d96ba&mc=true&node=sg2.1.200_1415.sg14&rgn=div7	Cost Principles for State, Local, and Indian Tribal Governments (Grants and Agreements)
7 CFR 271.1 to 271.8 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=8fc53bd6c2662141601f5431b69d96ba&mc=true&node=pt7.4.271&rgn=div5	General Information and Definitions
7 CFR 272.1-272.16 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=8fc53bd6c2662141601f5431b69d96ba&mc=true&node=pt7.4.272&rgn=div5	Requirements for Participating State Agencies
7 CFR 274.1-274.8	http://www.ecfr.gov/cgi-bin/text-idx?SID=8fc53bd6c2662141601f5431b69d96ba&mc=true&node=pt7.4.274&rgn=div5	Issuance and use of program benefits
7 CFR 277.1-277.18 (SNAP)	http://www.ecfr.gov/cgi-bin/text-idx?SID=8fc53bd6c2662141601f5431b69d96ba&mc=true&node=pt7.4.277&rgn=div5	Payments of Certain Administrative Costs of State Agencies, including Establishment of an Automated Data Processing (ADP) and Information Retrieval System
7 CFR 277 Appendix (SNAP-Payments of Certain Administrative Costs)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1dd83085017f07214cdf0d65386d27e8&mc=true&node=ap7.4.277_118.a&rgn=div9	Departmental Regulation for Program Administration and Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments
7 CFR 274.1 (SNAP EBT Auditing Standards)	http://www.ecfr.gov/cgi-bin/text-idx?SID=c39e50110629edac0cc93d4b13a5f46e&mc=true&node=pt7.4.274&rgn=div5	Requires States with SNAP EBT systems to perform an examination of their EBT transaction processing is conducted at least annually.



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
7 CFR 272 (EBT Adjustments Requirements For Participating State Agencies)	http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=7:4.1.1.3.20	SNAP EBT system—State agency's ability to make adjustments to a household's account in an EBT system
7 CFR 273 (Certification of eligible households and general rules)	http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title07/7cfr273_main_02.tpl	SNAP EBT system—State agency's ability to make adjustments to a household's account in an EBT system
7 CFR 274 (Issuance And Use Of Program Benefits)	http://www.ecfr.gov/cgi-bin/text-idx?SID=5df8be3d7a83db7c9e049db60dcab102&mc=true&node=se7.4.274_13&rgn=div8	SNAP EBT system—State agency's ability to make adjustments to a household's account in an EBT system
7 CFR 274.8 (EBT Interoperability and Portability)	http://www.ecfr.gov/cgi-bin/text-idx?SID=cf94f2f7a85174974500ff0accedd988&mc=true&node=se7.4.274_18&rgn=div8	Functional and technical EBT system requirements
PL 104-193 (EBT PRWORA)	https://www.congress.gov/bill/104th-congress/house-bill/3734/text?q=%7B%22search%22%3A%5B%22PL+104-193%22%5D%7D&resultIndex=1	Mandated each State agency implement EBT for issuance of food stamp benefits no later than October 1, 2002.
7 CFR 274 (EBT Retail Food Store Provisions)	http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=f8c42cf935b087216ccce6bb71fd2e52&mc=true&n=pt7.4.274&r=PART&ty=HTML	Issuance and use of program benefits.
2 CFR 200.501-200.507 (EBT-Audits)	http://www.ecfr.gov/cgi-bin/text-idx?SID=0d07d7e7d6b15fd205ed1b928ab131dc&mc=true&node=sg2.1.200_1500.sg18&rgn=div7	Audits of States, Local Governments, and Non-Profit Organizations for Food Stamp Program



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
7 CFR 246 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1cc1da9e6e74dd01970d549f0ec7848f&mc=true&node=pt7.4.246&rgn=div5	Special Supplemental Nutrition Program for Women, Infants and Children (WIC)
7 CFR 246.2 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=6d3b88eba0210e5fd5a1b0f2af5f3027&mc=true&node=se7.4.246_12&rgn=div8	Definitions
7 CFR 246.3 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=3a05f20bb33175e79f0b4f2f32c614c7&mc=true&node=pt7.4.246&rgn=div5#se7.4.246_13	Administration
7 CFR 246.4 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=3a05f20bb33175e79f0b4f2f32c614c7&mc=true&node=pt7.4.246&rgn=div5#se7.4.246_14	State Plan
7 CFR 246.7 (WIC)	http://www.ecfr.gov/cgi-bin/text-idx?SID=3a05f20bb33175e79f0b4f2f32c614c7&mc=true&node=pt7.4.246&rgn=div5#se7.4.246_17	Certification of participants
7 CFR 264.12 (WIC-Food delivery methods)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1cc1da9e6e74dd01970d549f0ec7848f&mc=true&node=se7.4.246_112&rgn=div8	Food Delivery Systems (EBT)
7 CFR 246.12 (a) (WIC-Food delivery methods)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1cc1da9e6e74dd01970d549f0ec7848f&mc=true&node=se7.4.246_112&rgn=div8	General



Table 53: Regulations

Regulatory Citation /Program	Web link	Description
7 CFR 246.12 (h) (WIC-Food delivery methods)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1cc1da9e6e74dd01970d549f0ec7848f&mc=true&node=se7.4.246_112&rgn=div8	Retail food delivery systems: Vendor agreements
7 CFR 246.12 (w) through (cc) (WIC-Food delivery methods)	http://www.ecfr.gov/cgi-bin/text-idx?SID=1cc1da9e6e74dd01970d549f0ec7848f&mc=true&node=se7.4.246_112&rgn=div8	Electronic Benefits Transfer
2 CFR 200.501-200.507 (Audit Requirements)	http://www.ecfr.gov/cgi-bin/text-idx?SID=0d07d7e7d6b15fd205ed1b928ab131dc&mc=true&node=sg2.1.200_1500.sg18&rgn=div7	PART 200—Uniform Administrative Requirements, Cost Principles, And Audit Requirements For Federal Awards Subpart F—Audit Requirements

A3. Regional Office Information

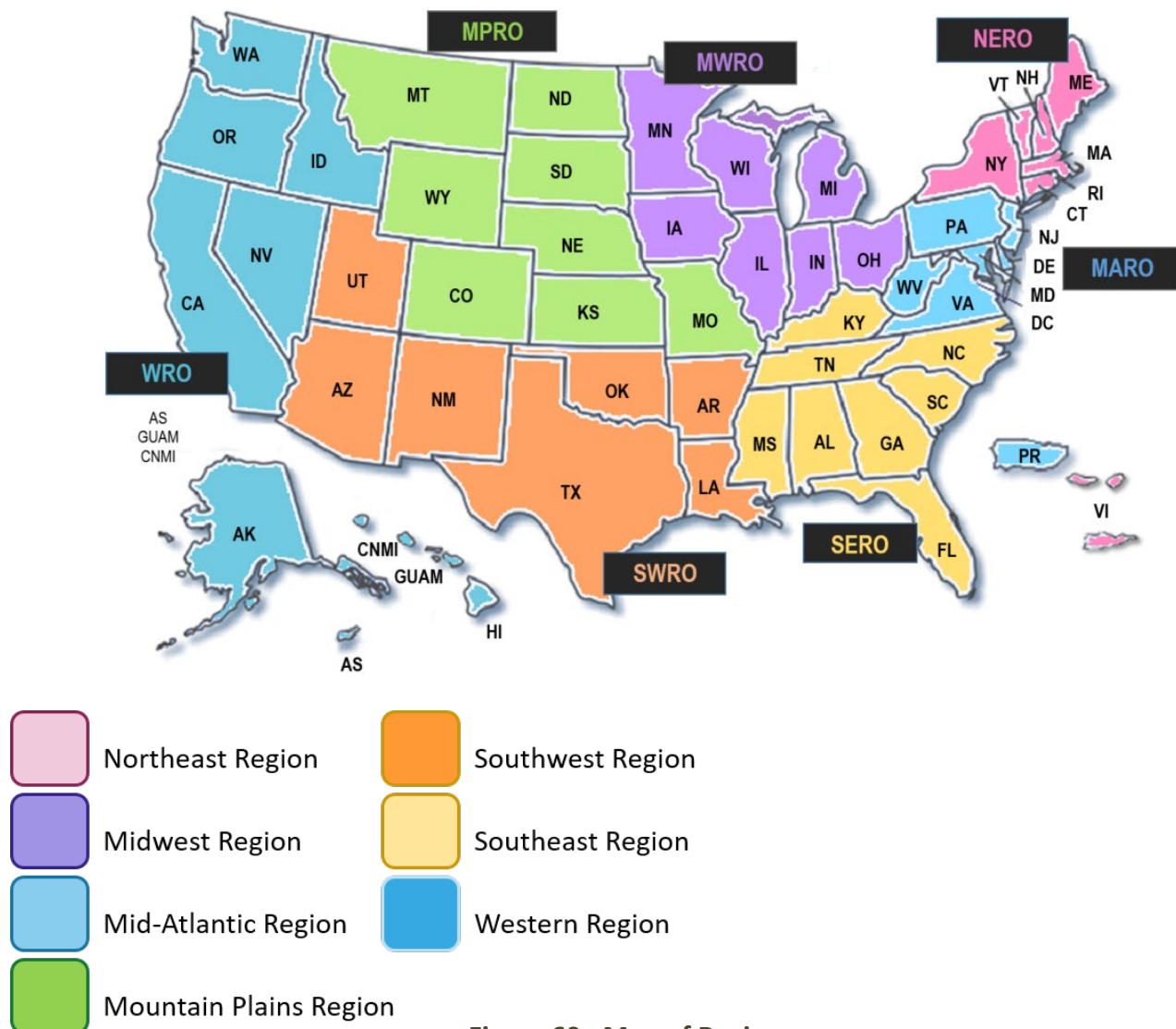


Figure 60: Map of Regions



Northeast Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Northeast Region USDA/FNS/NERO 10 Causeway Street, Room 501 Boston, Massachusetts 02222-1069 Tel: 617-565-6370	Connecticut Indian Township Passamaquoddy Reservation, ME Maine Massachusetts New Hampshire New York Pleasant Point Passamaquoddy Reservation, ME Rhode Island Seneca Nation, NY Vermont Virgin Islands
Mid-Atlantic Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Mid-Atlantic Region USDA/FNS/MARO Mercer Corporate Park 300 Corporate Boulevard Robbinsville, New Jersey 08691-1518 Tel: 609-259-5025	Delaware District of Columbia Maryland New Jersey Pennsylvania Puerto Rico Virginia West Virginia
Southeast Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Southeast Region USDA/FNS/SERO 61 Forsyth St., Room 8T36 Atlanta, Georgia 30303-3427 Tel: 404-562-1801	Alabama Band of Choctaw Indians, MS Eastern Band of Cherokee Indians, NC Florida Georgia Kentucky Mississippi North Carolina South Carolina Tennessee



Midwest Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Midwest Region USDA/FNS/MWRO 77 West Jackson Boulevard - 20th Fl. Chicago, Illinois 60604-3507 Tel: 312-353-6664	Illinois Indiana Iowa Michigan Minnesota Ohio Wisconsin
Southwest Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Southwest Region USDA/FNS/SWRO 1100 Commerce St. Room 555 Dallas, Texas 75242-1005 Tel: 214-290-9800	Acoma, Canoncito, and Laguna (ACL), NM Arizona Arkansas Cherokee Nation of Oklahoma, OK Chickasaw Nation, OK Choctaw Nation of Oklahoma, OK Citizen Potawatomi Nation, OK Eight Northern Pueblos Council, NM Five Sandoval Pueblos, Inc., NM Inter-Tribal Council of Oklahoma, OK Louisiana Muscogee (Creek) Nation, OK New Mexico Oklahoma Osage Tribal Council, OK Otoe-Missouria Tribe, OK Pueblo of Isleta, NM Pueblo of San Felipe, NM Pueblo of Zuni, NM Santo Domingo Tribe, NM Utah Texas Wichita, Caddo, and Delaware Tribes (WCD Enterprises, Inc.), OK



Mountain Plains Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Mountain Plains Region USDA/FNS/MPRO 1244 Speer Boulevard, Room 903 Denver, Colorado 80204-3581 Tel: 303-844-0300	Cheyenne River Sioux Tribe, SD Colorado Eastern Shoshone Tribe, WY Kansas Missouri Montana Nebraska North Dakota Northern Arapaho, WY Omaha Tribe, Nebraska Rosebud Sioux Tribe, SD Santee Sioux Nation, NE South Dakota Standing Rock Sioux Tribe, ND Three Affiliated Tribes, ND Ute Mountain Ute Tribe, CO Winnebago Tribe, NE Wyoming
Western Regional Office	States, ITOS, and Territories SNAP or WIC Programs
Western Region USDA/FNS/WRO 90 Seventh Street Suite 10-100 San Francisco, California 94103 Tel: 415-705-1310	Alaska American Samoa California Guam Hawaii Idaho Inter-Tribal Council of Arizona (ITCA), AZ Inter-Tribal Council of Nevada (ITCN), NV Navajo Nation, AZ Nevada Commonwealth of Northern Marianas Islands (CNMI) Oregon Washington



A4. System Type and Acquisition Selection Tool

A4.1 Introduction

Organizations looking to refresh their IT systems to garner more efficiency and cost effectiveness face many daunting and complex decisions. The purpose of this tool is to provide a broad and simplified overview of important considerations which will have sweeping impacts on the types of systems which are best suited for an organization and the acquisition process to obtain them.

A4.2 Using this Tool

A collection of key terms are presented as a preface to this tool to help establish a base line vocabulary. Please review it before going further into the tool or use it as a reference source should you find a topic confusing.

While reading through flowcharts, any element which is outlined in yellow indicates that it hyperlinks to another chart. If you follow a hyperlink and wish to return to the previously viewed slide then right click and choose 'Last Viewed'

A4.3 References

This tool assumes a basic working knowledge of the mentioned topics. However if more information is required or desired please see the below references for further reading.



For more information on the acquisition process please refer to chapter **4.0 Procurement**.

Table 54: Key Terms and References

Term	Acronym	Definition
Public Cloud		The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Private Cloud		The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and



Table 54: Key Terms and References

Term	Acronym	Definition
		operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community Cloud		The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Hybrid Cloud		The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Software-as-a-Service	SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. A prime example of a SaaS would be Microsoft Online Services and Google products such as Gmail and Google Docs.
Platform-as-a-Service	PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. A prime example of a PaaS would be a web hosting company such as Amazon or Go Daddy.
Infrastructure-as-a-Service	IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). A data center such as a state IT shop is a prime example of an IaaS.
Enterprise Architecture	EA	Enterprise architecture is being used in this connotation to refer to the base network, servers, and clients internal to an organization. They are generally based on service oriented architecture (SOA) design principles and provide the base upon which systems



Table 54: Key Terms and References

Term	Acronym	Definition
		run. For instance an acquired COTS-based or traditional transfer system would be placed on top of an agency's enterprise architecture. Throughout this document EA may be used to refer to a internally hosted system or solution and may or may not include COTS-based components.
Commercial-off-the-Shelf	COTS	In general, COTS products are characterized by the following: IT solutions, systems, and/or software supplied from the private sector; offered and sold competitively in substantial quantities in the commercial marketplace; and prepared with the sole or chief emphasis on salability, profit, or success to yield or make a profit. Comprised of a broad spectrum of functionality to meet requirements for a domain (e.g., financial management, case management, benefits and compensation management). Is configured, rather than constructed from scratch, in order to implement a particular function or business solution. Does not require customization through reprogramming to satisfy a particular functional capability; configuring software properties and options does not constitute programming. Is not synonymous with proprietary software. Not all COTS is proprietary and not all proprietary software is COTS.
Traditional Transfer	Transfer	This refers to an instance where an agency owns a system or application which is currently capable of being copied and distributed to another agency. Throughout this document the term transfer will be used to indicate a solution which has been deemed to be stable and capable which is own by an agency who has consented to its the duplication and distribution.
System upgrade	Upgrade	This is used to refer to instances where an agency already owns a system or application and it is capable of being modified.
Cloud computing		Generally speaking, cloud computing is a broad term used to describe the delivery of computing needs and data storage capacity to a heterogeneous community of end-users, primarily delivered through networked systems. Cloud computing uses a collection of services, applications, information, and infrastructure comprised of pools of computing, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down. Cloud computing provides for an on-demand, utility-like model of allocation and consumption.

A4.4 System Type Selection

A4.4.1 Taking Stock

The first basic step in refreshing an IT system is to take stock of what you have currently. You need to determine if there is an application already in place and if you own it. If you have nothing in place and are doing a clean acquisition, then this phase is very straight forward. If, however, you already have a system in place it becomes more complicated. The current system needs to be evaluated to determine if it is a viable option to keep in place. You must consider if it can either have its life extended either through upgrades or if it needs to be supplemented with additional applications or systems. Should the current system be deemed too deprecated to keep in service, then you can move forward as if it's a completely new acquisition, but data conversion from the old system to the new one becomes a major concern.

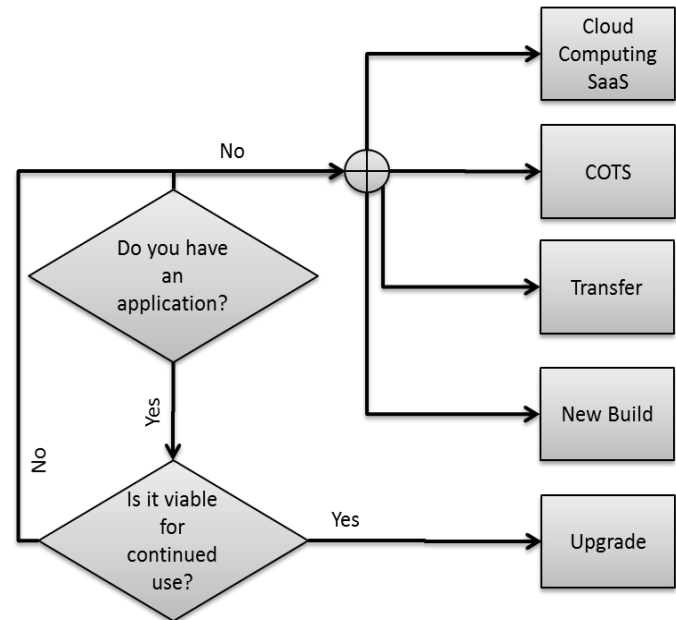


Figure 61: Taking Stock of Current Applications

A4.4.2 System Ownership

Many government agencies have concerns over which aspects of a system they own when they make a purchase. Some organizations feel that actually owning their systems, or at least parts of their system, is very important to meeting security demands and their financial obligations to show a return on investment. For these organizations, it's important to see a tangible good for their money or to insure full control over certain aspects of operations. There is a big distinction, however, between owning an application in its entirety and simply owning the right to use it. Your agency's stance on this will determine how limited or open your solution selection is. In all cases the data associated with a system is owned by the organization.

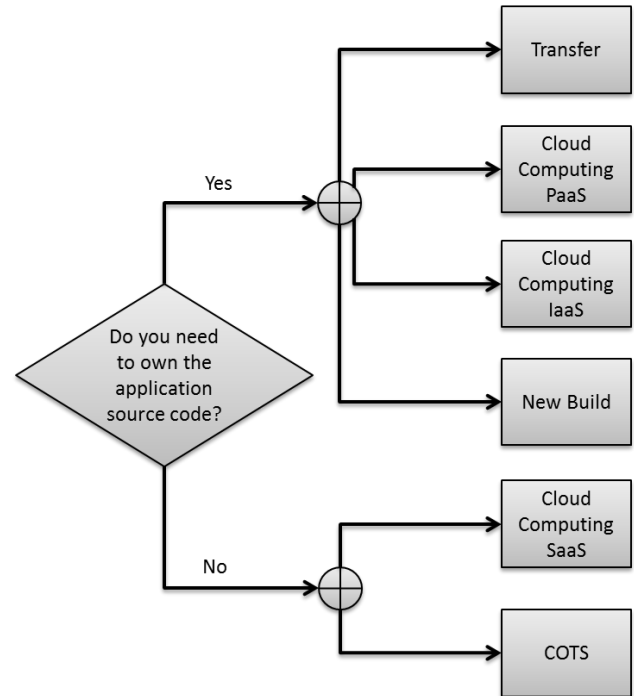


Figure 62: Application Ownership

A4.4.3 Resources

Another major consideration is how much and what kinds of resources are available during all phases of the process. All systems will require major resources during the acquisition, deployment, implementation, and migration stages. Depending on what system type is selected, you may also have to add development on top of that. Once a system is in place, however, the day to day operational

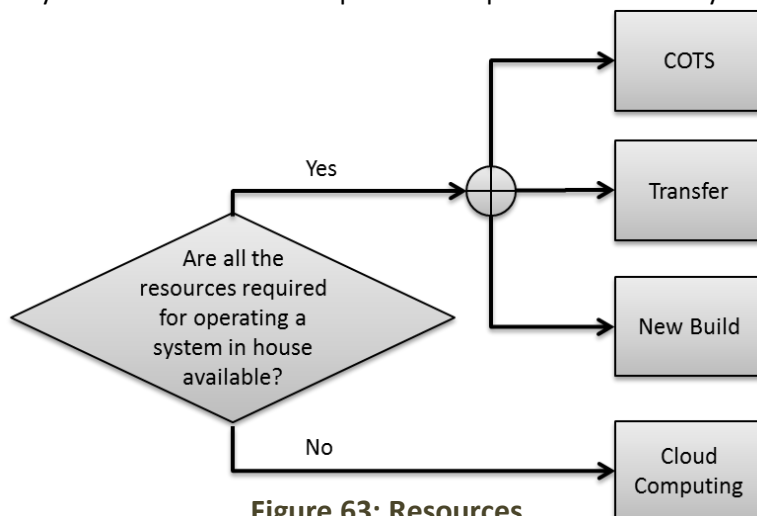


Figure 63: Resources

consumption of resources becomes a major consideration. Depending on the system type selected, these operation costs may be burdensome or insignificant when compared to the initial costs. In most all cases, externally hosted solutions have a far lower resource cost associated with them than internally hosted systems.

A4.4.4 Customization

Customization is also a big consideration. To some organizations the rights to some aspects of a system is very important:

- The right to alter the source code
- The ability to make customizations to the functionality of applications
- The rights to manage other low level technical components

This ensures that the organization has the ability to add functionality as necessary and extend the life of a system. These types of operations require more resources. Organizations must find the proper balance which suits their circumstances.

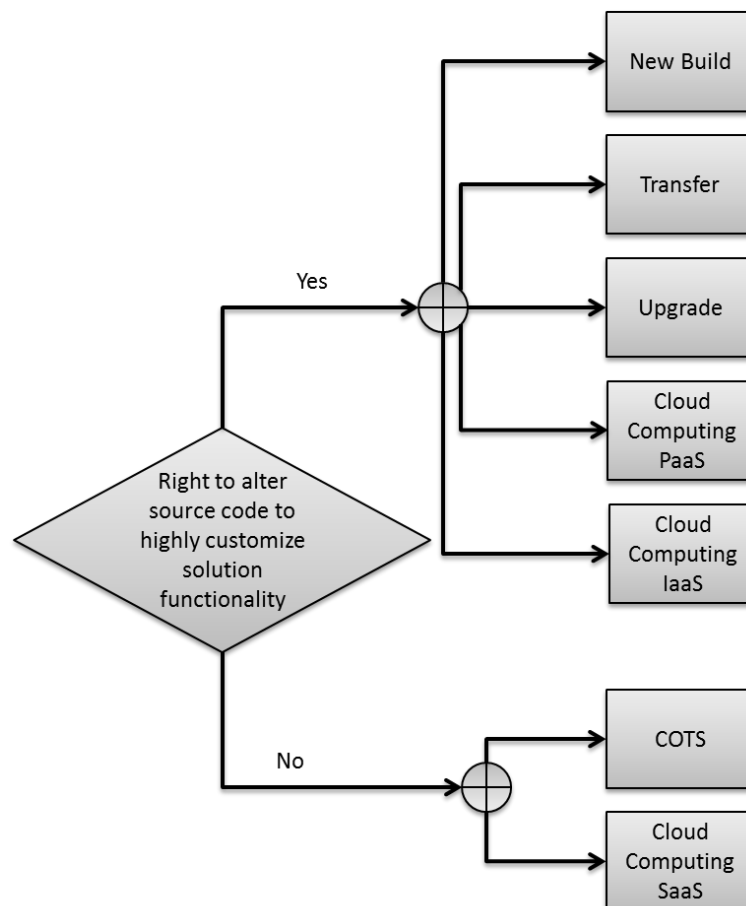
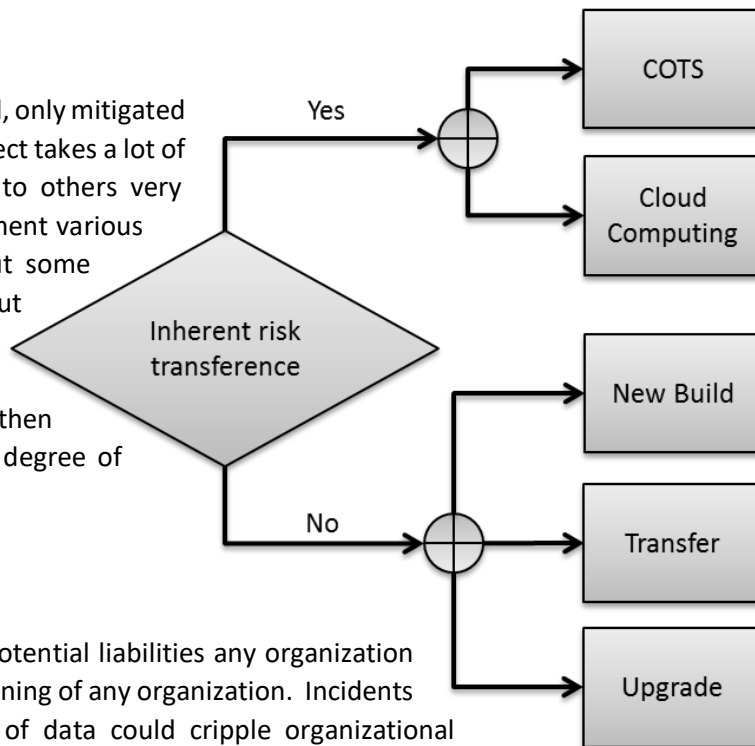


Figure 64: Application Customization

A4.4.5 Risk

It is well known that risk can never be eliminated, only mitigated or transferred. Managing risk to mitigate its effect takes a lot of resources, which makes transferring the risk to others very appealing. There are countless ways to implement various forms of risk transference and mitigation, but some system types naturally transfer some risk without the need for additional services or considerations. If reducing the resources consumed by risk management is a goal, then picking the system type with the appropriate degree of inherent risk transference will be important.



A4.4.6 Data

One of the most valuable assets, and largest potential liabilities any organization holds is data. Data is instrumental to the functioning of any organization. Incidents which affect the consistency and availability of data could cripple organizational operations. Organizations have legal obligations and standards that they must meet and comply with to insure that their data is appropriately protected. Failing to do

Figure 65: Risk

so opens the organization to litigation from clients and possible sanctions from the government. This makes picking a system that has an appropriate security structure in place paramount. Different system types allow for different degrees of granular security control as well as shifting different responsibilities to different parties. Organizations need to assess if they have the proper in-house staff to meet their security responsibilities, or if there is an external trustworthy entity to whom it could be outsourced and then pick an appropriate system accordingly. Organizations must understand how much control they must maintain internally and how much may be outsourced before determining the best system type.

Table 55: System Type Selection Based on Security to Responsibility

Level of Security Control	Responsible Party	
	In-House	Out sourced
Application Security	PaaS, IaaS, Enterprise Architecture	SaaS
Platform Security	IaaS, Enterprise Architecture	SaaS, PaaS



Table 55: System Type Selection Based on Security to Responsibility

Level of Security Control	Responsible Party	
	In-House	Out sourced
Hardware Security	Enterprise Architecture	SaaS, PaaS, IaaS
Data Security	Enterprise Architecture, SaaS, PaaS, IaaS (Private and hybrid cloud deployment)	SaaS, PaaS, IaaS (Public, Community, and hybrid cloud deployment)

A4.4.7 Standards

It's also very important to be aware of the standards a system is based upon, especially if it involves cloud-based elements. There are standards for every functional level and component of a system. There are standards from the high-level overall architecture of the system down to the way data itself is handled and stored, and every level of interface and manipulation in between. Each segment of the system should be investigated to see what kind of standard it is associated with.

There are two basic types of standards:

5. An open standard which is developed by many people from many organizations working in combination to produce a standard that is freely available and transparent.
6. A proprietary standard is the other form which is generally developed by a single organization who obfuscates the details of the standard in such a way to make it only useable by the developing organization. Failure to understand the standards being accepted when acquiring a system could lead to vendor lock-in.

When investigating a standard, make sure to research how the standard was developed, how well it's used in the industry, and what the future plans for the standard are. Highly utilized proprietary standards may be an indication of best practices. In rare circumstances, proprietary standards have been converted into open standards. A standard with very little to no future development plans could either indicate a mature stable standard or could be a warning sign of impending obsolescence. The world of standards is usually very much in flux and must be considered on a case-by-case basis which can lead to some difficulty. It is, however, still a very important consideration which could have long lasting impacts on the operation and life expectancy of a system.



A4.4.8 Decision Matrix

The topics mentioned here are very broad with many important details. All of which will need to be considered in tandem and addressed fully and appropriately before a system type can be selected. The following decision matrix is a combination of the previously mentioned factors combined to easily compare the different system types and the implications they have on the broad topics discussed. A system type's handling of a topic, as related in this matrix (and in this document as a whole), is not prescriptive. Any combination of additional services and/or contract negotiations can come into play to dramatically alter the outcomes.

Table 56: Decision Matrix

	New Build	Upgrade	Transfer	COTS	Cloud	Cloud (SaaS)	Cloud (PaaS)	Cloud (IaaS)
Application Ownership	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes
Supplement Existing System	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Limited in-house resource usage during implementation	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Limited in-house resource usage during operation	No	No	No	Yes	Yes	Yes	Yes	Yes
Risk transference by default	No	No	No	Yes	Yes	Yes	Yes	Yes
Add custom functionality	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes



Table 56: Decision Matrix

	New Build	Upgrade	Transfer	COTS	Cloud	Cloud (SaaS)	Cloud (PaaS)	Cloud (IaaS)
Application Security (Default In-house responsibility)	Yes	Yes	Yes	No	Yes/No	No	Yes	Yes
Application Security (Default outsourced responsibility)	No	No	No	Yes	Yes/No	Yes	No	No
Platform Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes/No	No	No	Yes
Platform Security (Default outsourced responsibility)	No	No	No	No	Yes/No	Yes	Yes	No
Hardware Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes/No	No	No	No
Hardware Security (Default outsourced responsibility)	No	No	No	No	Yes/No	Yes	Yes	Yes
Data Security (Default In-house responsibility)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Security (Default outsourced responsibility)	No	No	No	No	Yes	Yes	Yes	Yes

A4.4.9 Types of Systems

Custom Built System

A custom built system is the most expensive way to obtain a system; however, it allows for the highest degree of business process to technology matching while also providing all features and functionality demanded from the system.

Custom Built System

Traditional Transfer

A transfer system is a good choice if another agency already has a system in-place that matches your requirements. Cost savings can be realized by not having to reinvent the system making migration, customization, and infrastructure the major concerns.

Traditional Transfer

Upgrade Existing System

If you already have a functional system in place, perhaps the most cost effective option would be simply to maintain the current system. Utilizing internal resources or hiring third-party contractors to write updates and upgrades may be a much more viable option than acquiring a new system.

Upgrade Existing System

Purchase COTS

If you need an entirely internally supported system (an enterprise architecture) but can't deal with the overhead generated by system development, maintenance, and upgrades, COTS may be best for you. COTS solutions transfer the lifecycle management for software to the vendor, but at the cost of ownership and control of functional enhancement or changes.

Purchase COTS

Cloud Computing

Cloud computing is a scalable solution which can provide a complete system from hardware to application or just portions of a solution. This flexibility may provide tight control of resources and costs without sacrificing operations. At the very least, cloud computing can provide stability to costs and other resource utilization.

Cloud Computing

Figure 66: Types of Systems

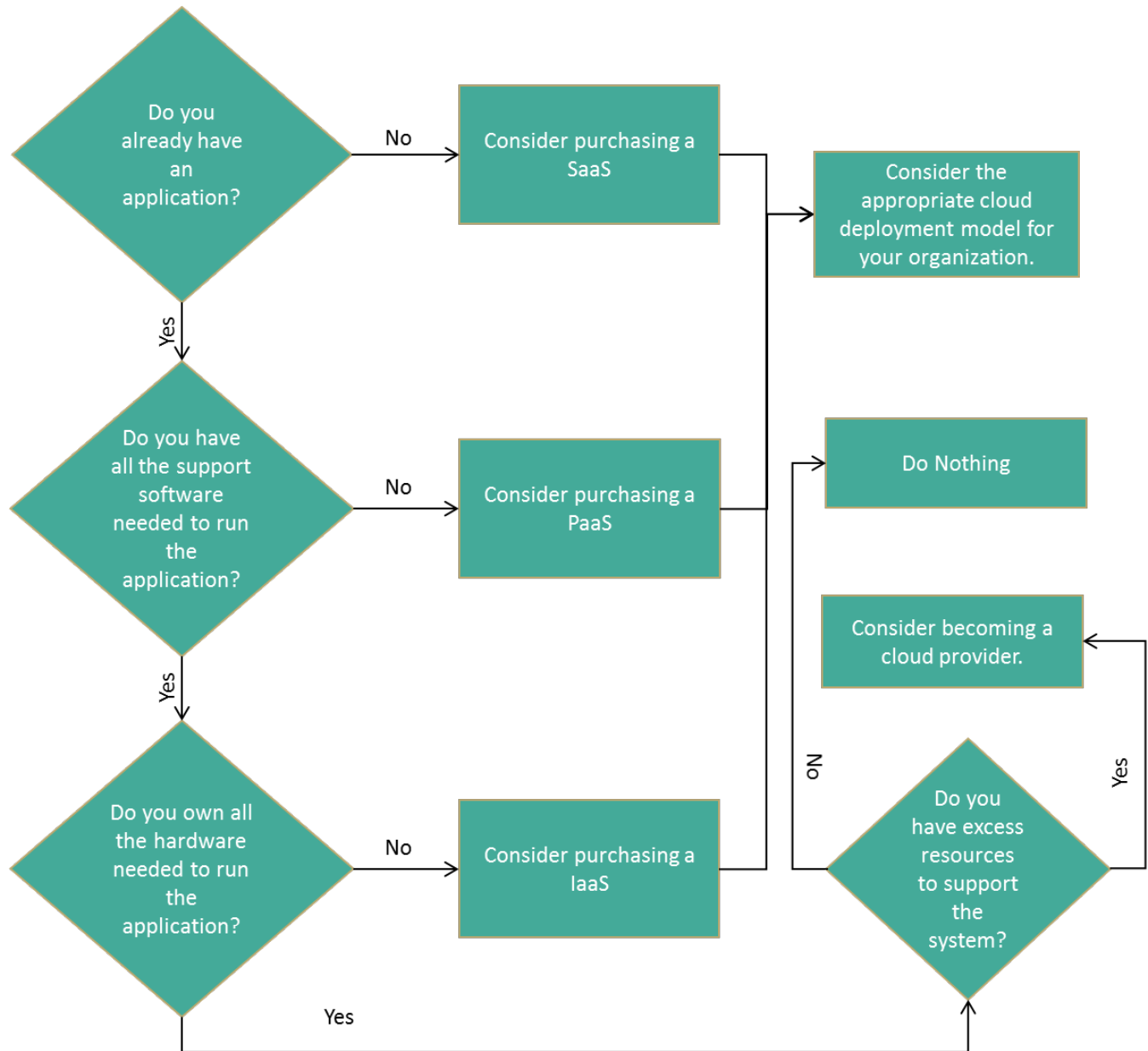


Figure 67: Cloud Service Selection

A4.5 Becoming a Cloud Provider

If an organization has a highly mature and stable IT solution in place which is based on an EA with ample resources, then it may be possible for the organization to reconfigure those assets in such a way that the organization may become a cloud provider itself. Becoming a cloud provider would allow the organization to spread the costs of its infrastructure in the same way that commercial vendors do, giving them a source of revenue to dramatically lower overhead expenses.

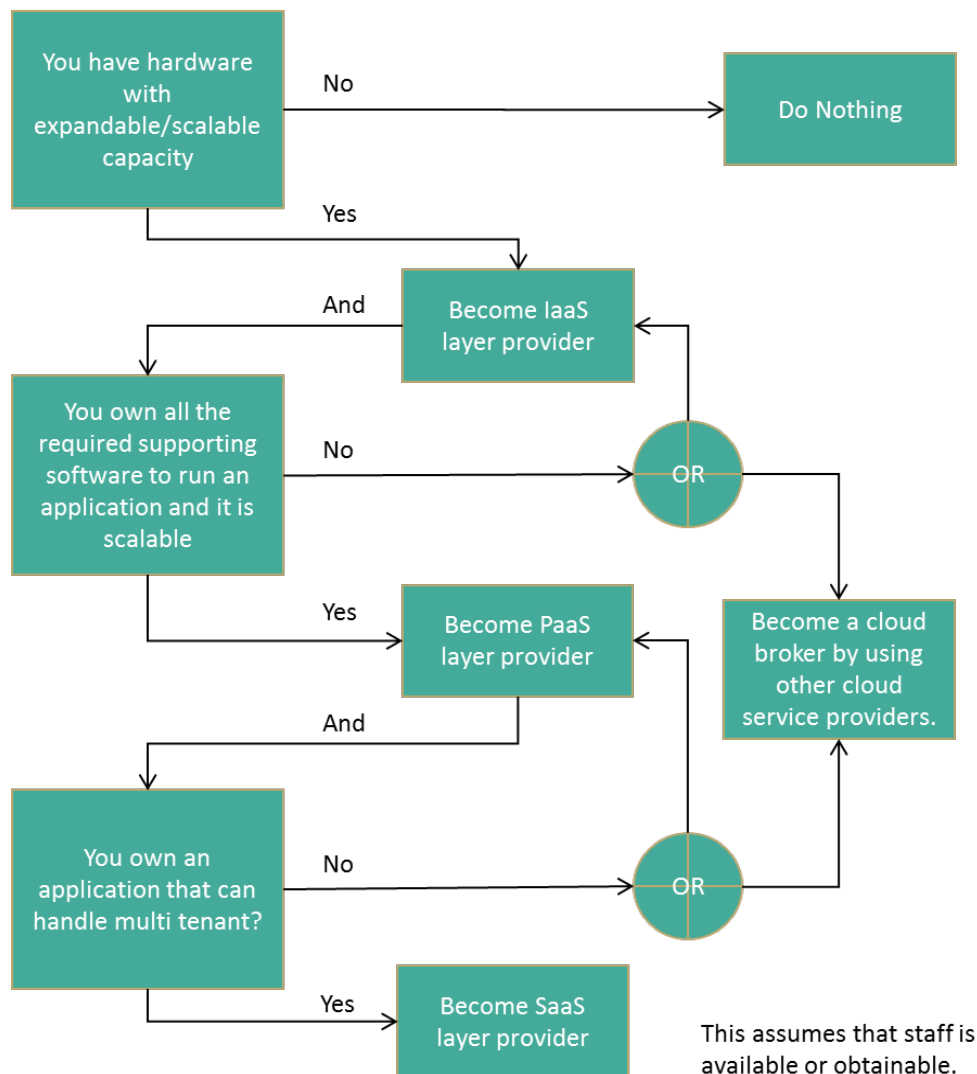


Figure 68: Becoming a Cloud Provider

A4.5.1 Cloud Broker

An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers. The integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. Cloud brokers typically do not own the assets or services they are providing.

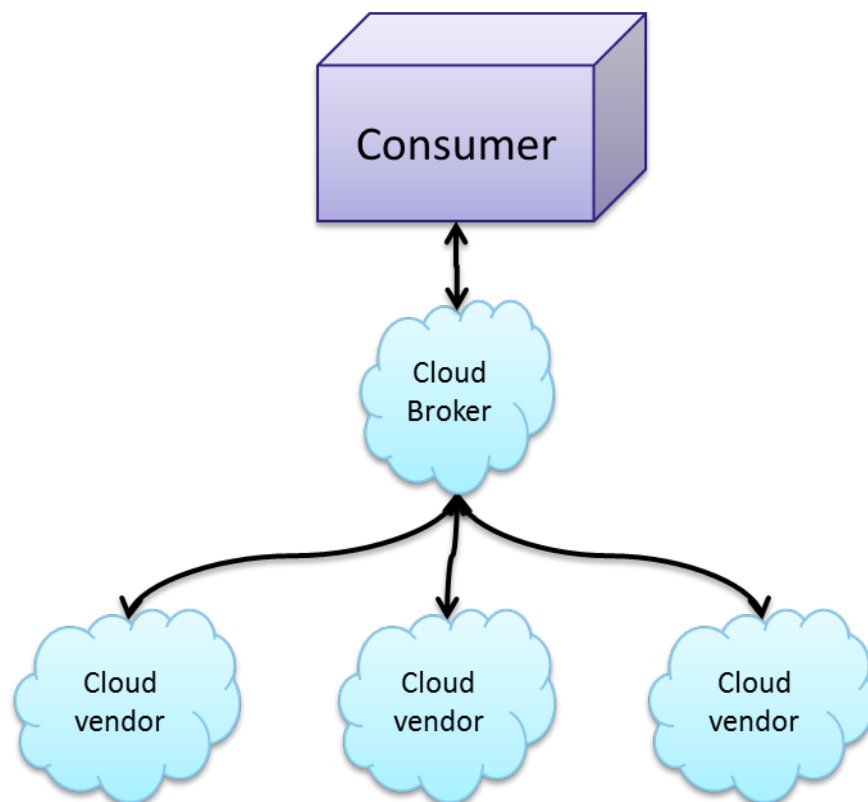


Figure 69: Cloud Broker

A4.6 Cloud Deployment Selection

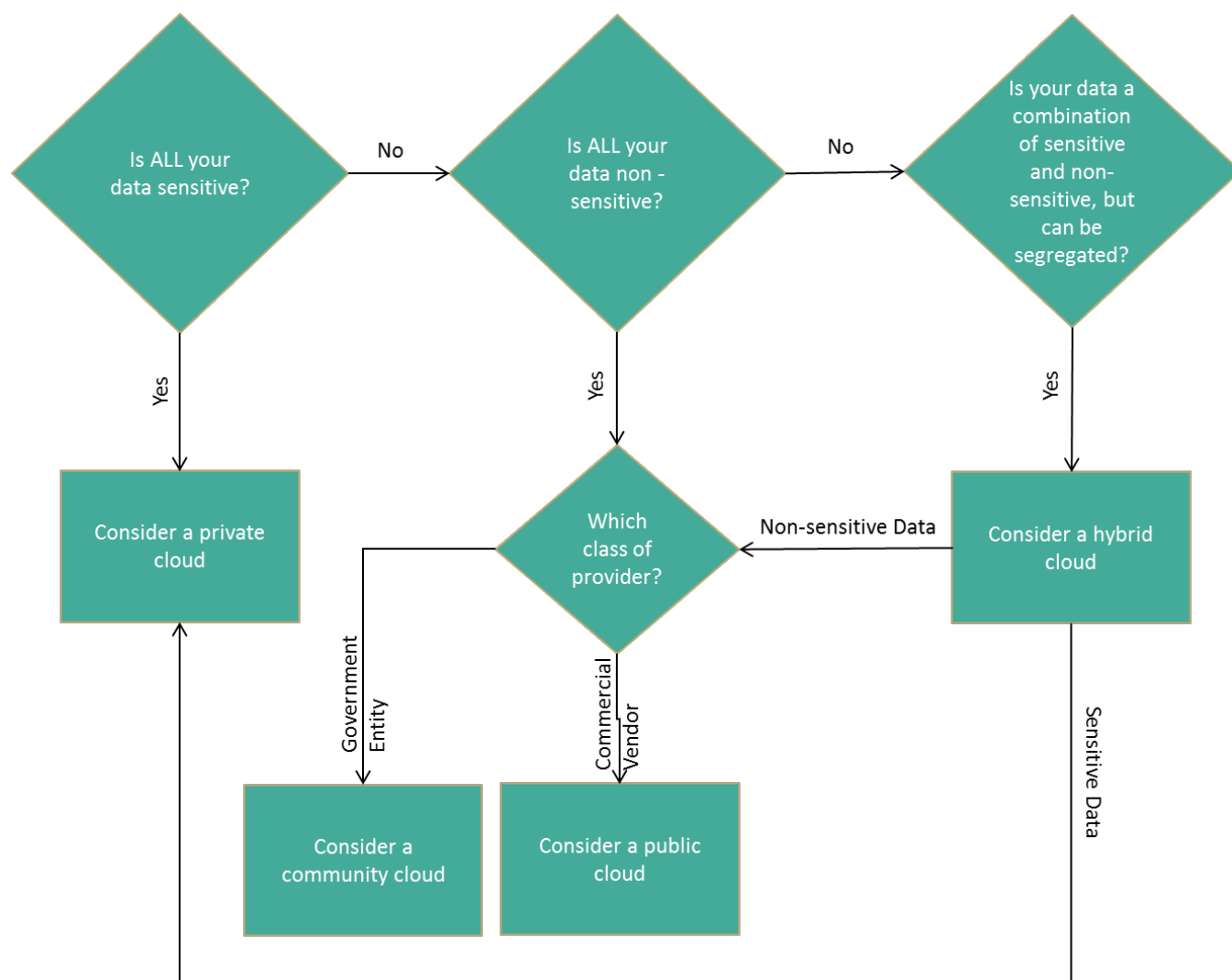


Figure 70: Cloud Deployment Selection

A4.6.1 Public Cloud

In a public cloud, the cloud provider's assets are readily consumable by any organization or individual. A public cloud has the largest potential set of users and thus can achieve the highest degree of cost savings. This larger user-base, however, also translates into a higher security threat. This is because public clouds are designed so that many organizations and/or large groups of individual users make use of the same application and/or set of hardware at the same time. This is known as a multi-tenant instance.

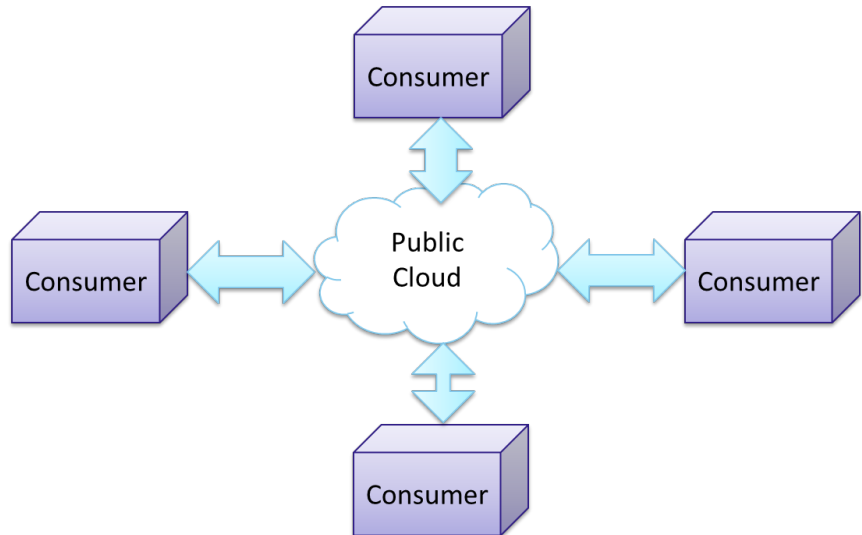


Figure 71: Public Cloud

A4.6.2 Private Cloud

A private cloud is designed to support only one consumer or limited user community, which lowers the cost saving strategy of cloud computing by cost distribution when compared to a public cloud. A private cloud can be internal or external to an organization. In an internal private cloud, the organization provides all the hardware and software itself which it houses in a facility controlled entirely by the organization. This gives the organization greater control over the security of the system. Even though the system is housed inside the organization, third party contractors and vendors may be hired to help manage the system. In an external private cloud, an organization enters into a contract with a third party contractor to build a cloud from scratch, hardware to software, which is housed in the contractor's facility, but can only be used by the soliciting organization. While this is more costly for contractors to construct, they are willing to engage in these arrangements because it ensures long term management contracts from the organization to maintain the systems. Private clouds can be the most costly form of cloud deployment, but also the most secure.

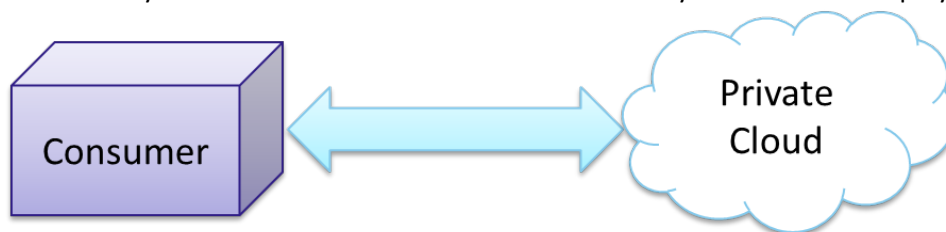


Figure 72: Private Cloud

A4.6.3 Hybrid Cloud

A hybrid cloud is a combination of the two other types of cloud. Hybrid clouds can be used in a multitude of ways. For instance, a hybrid cloud could be used to segregate data based on sensitivity. In such a case, non-sensitive data could be placed in public clouds to realize costs savings while sensitive data is placed in private clouds for security purposes. A hybrid cloud may also be utilized to overcome bandwidth issues. In cases where large amounts of data are being transferred or queried back and forth from the organization's facility to the cloud providers' location, limitations on internet connections between the two locations may cause performance to degrade. Appliances may be placed in the consumer's location creating a kind of mini-private cloud which performs caching and batch processing functions to the external cloud in order to keep performance within acceptable levels. Hybrid clouds may also be used for redundancy purposes. For example, an organization may make use of a local/onsite private cloud in conjunction with a public or community cloud to ensure continuity of operations during an internet outage which disables communications to the public/community cloud.

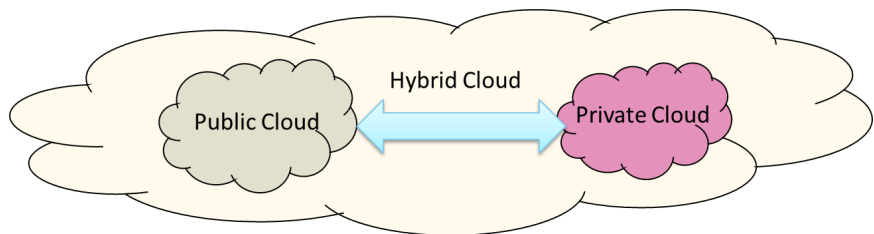


Figure 73: Hybrid Cloud

A4.6.4 Community Cloud

A community cloud is a middle ground between a public cloud and a private cloud. In a community cloud, the cloud provider has configured its assets in such a way as to cater to a more select niche of consumers who have the same operational needs and/or requirements. In some instances, vendors create a specialized cloud which is targeted at a specific industry, such as the medical or legal industry, by insuring that the security features and performance metrics are in-line with the industry norms.

A community cloud may also be a consortium of consumers who have teamed together for the sole purpose of cost sharing to reduce the overhead associated with clouds. In these ways, the community cloud offers increased security by limiting the user base to something much smaller than a public cloud and yet increased cost efficiency by spreading costs over a larger user base than a private cloud.

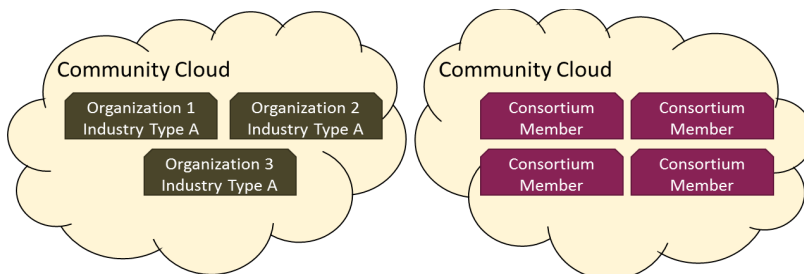


Figure 74: Community Cloud

A4.6.5 Bridging Resource Gaps with Cloud

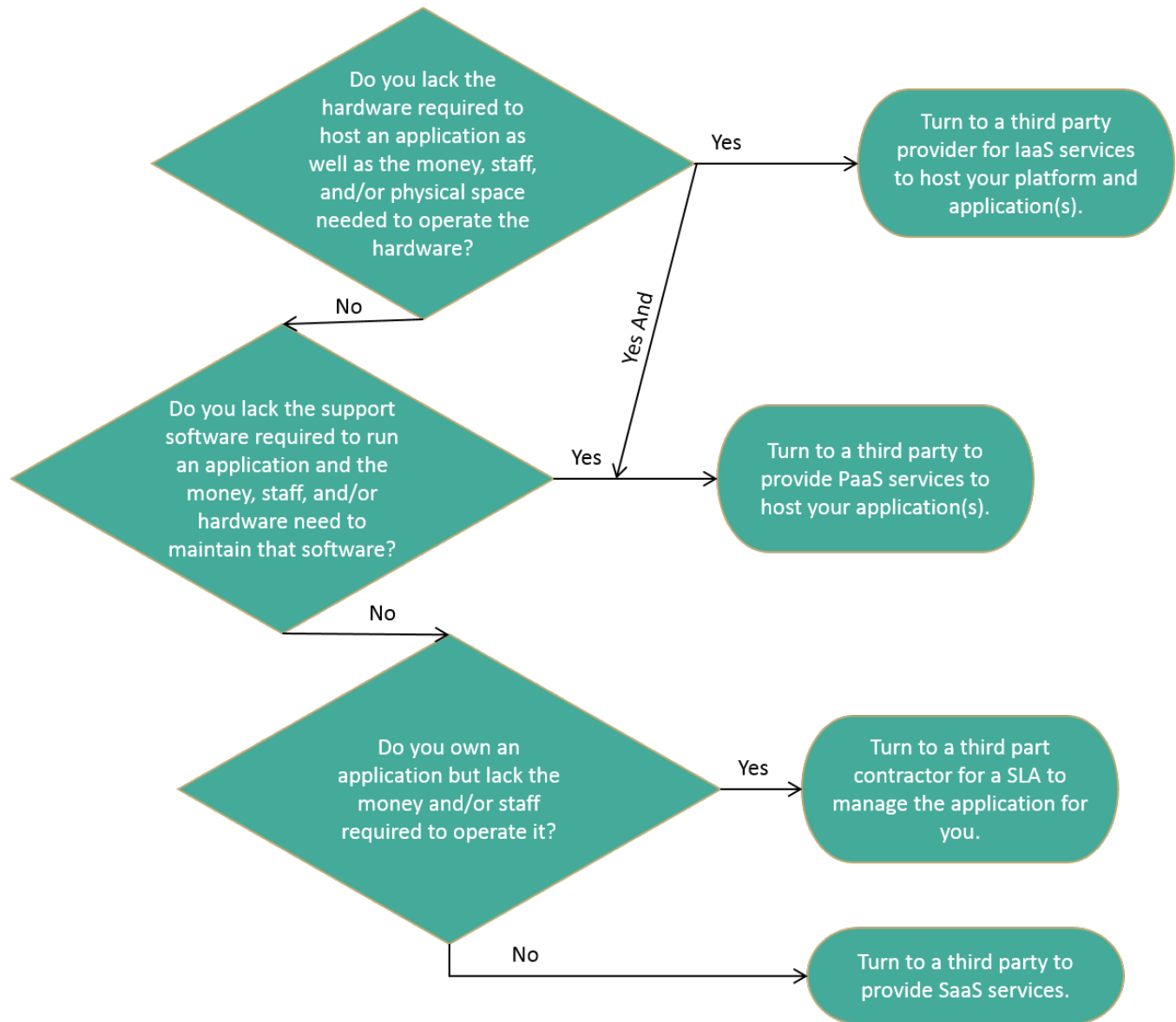


Figure 75: Bridging Resource Gaps with Cloud

A4.6.6 Cloud Security Control Level

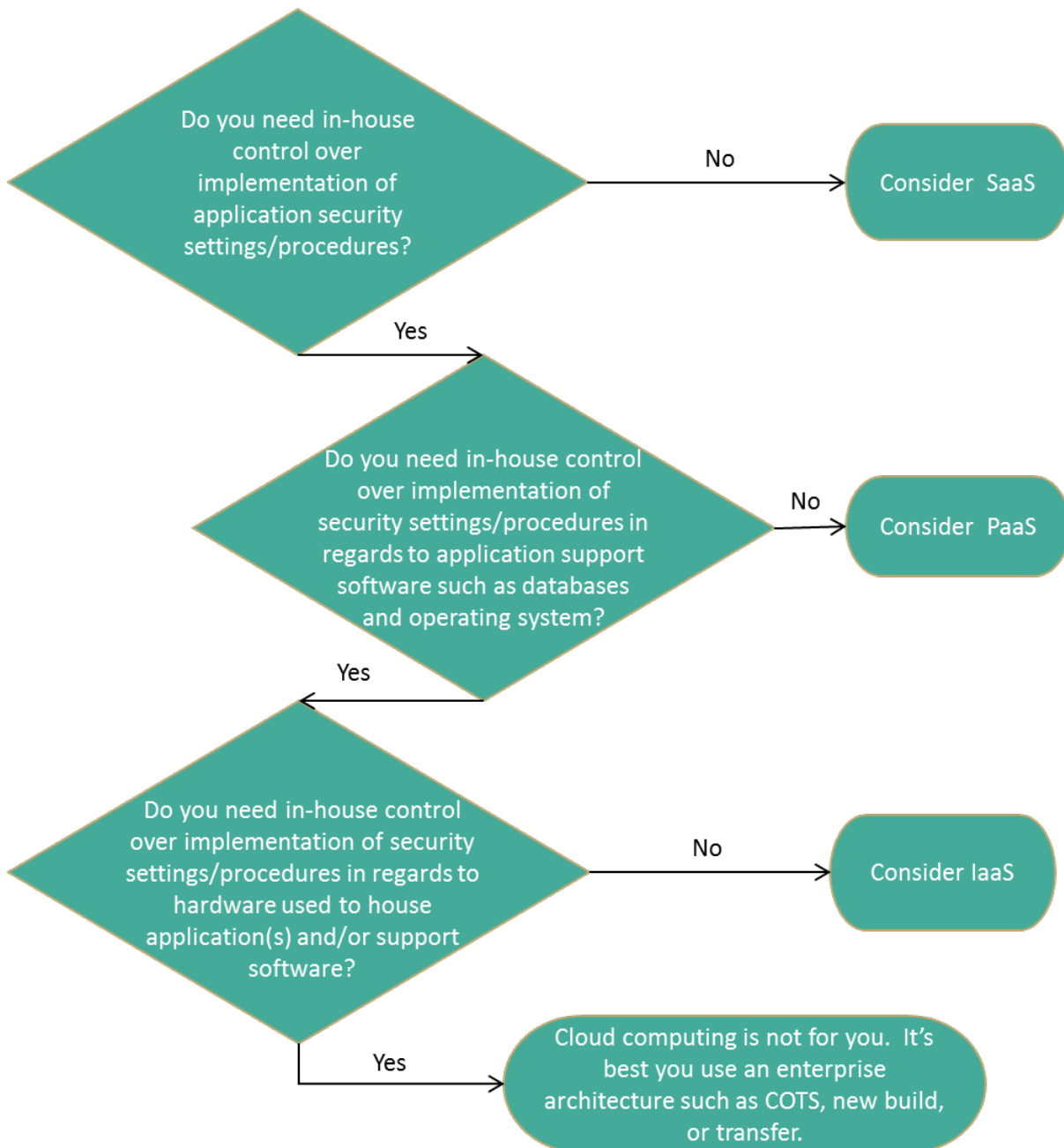


Figure 76: Cloud Security Control Level

A4.6.7 Purchasing SaaS

SaaS, sometimes referred to as “on-demand software,” is a software delivery model where a business application is hosted. The consumer provides and owns only the data. SaaS products are meant to support multiple tenants (consumers) with a single instance of an application.

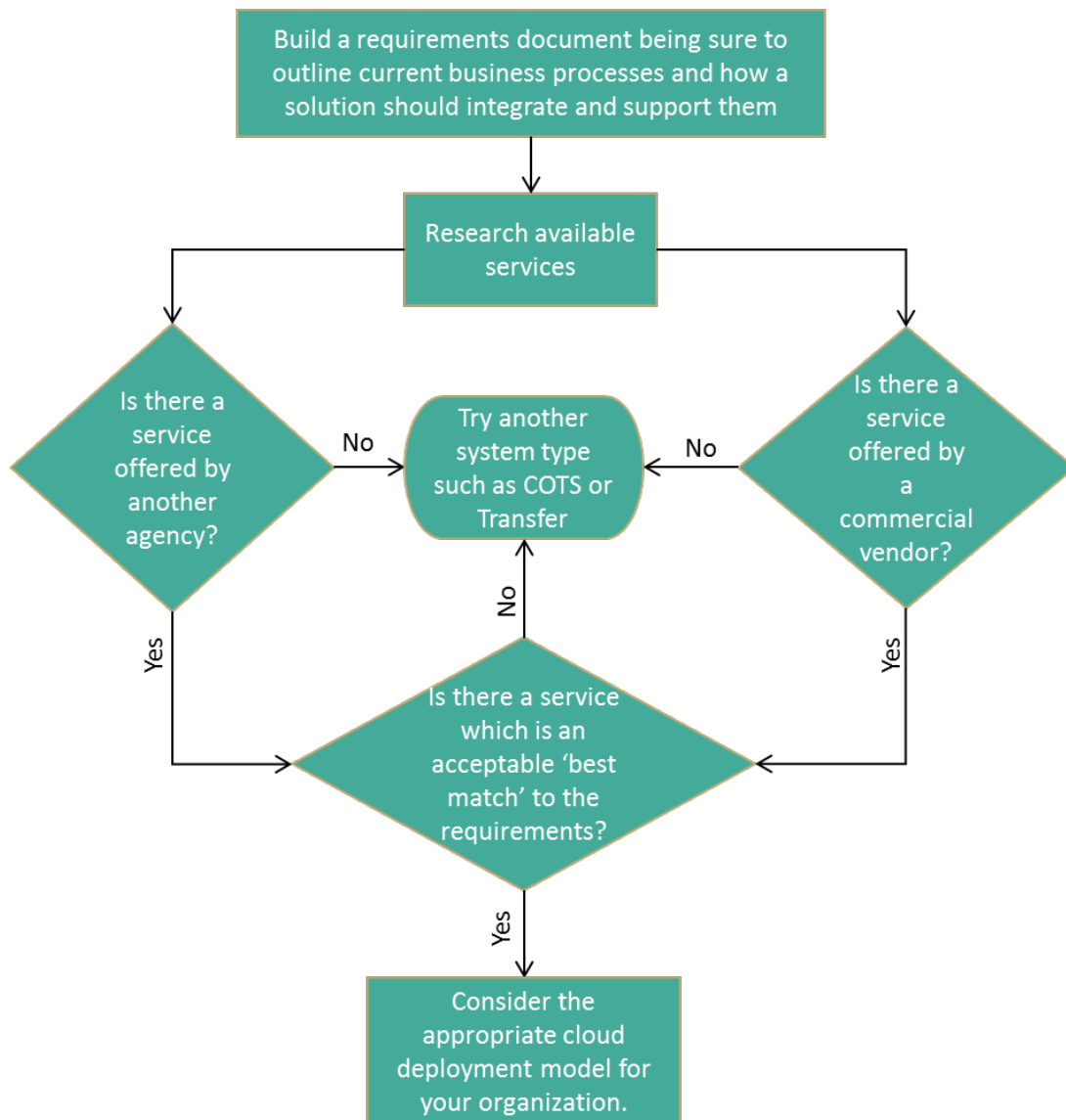


Figure 77: Purchase SaaS

A4.6.8 Purchasing PaaS

In Platform as a Service (PaaS) the cloud provider supplies the hardware as well as the basic software, such as the operating system and other basic libraries needed to host and execute applications. The PaaS model allows the burden of providing and managing basic IT overhead to be carried by the cloud provider while still giving the consumer the flexibility to design, build, and deploy their own applications. PaaS services are ideal for organizations which have an application they have purchased or had custom developed, but do not have the resources to purchase or maintain the hardware and base software needed to host the application.

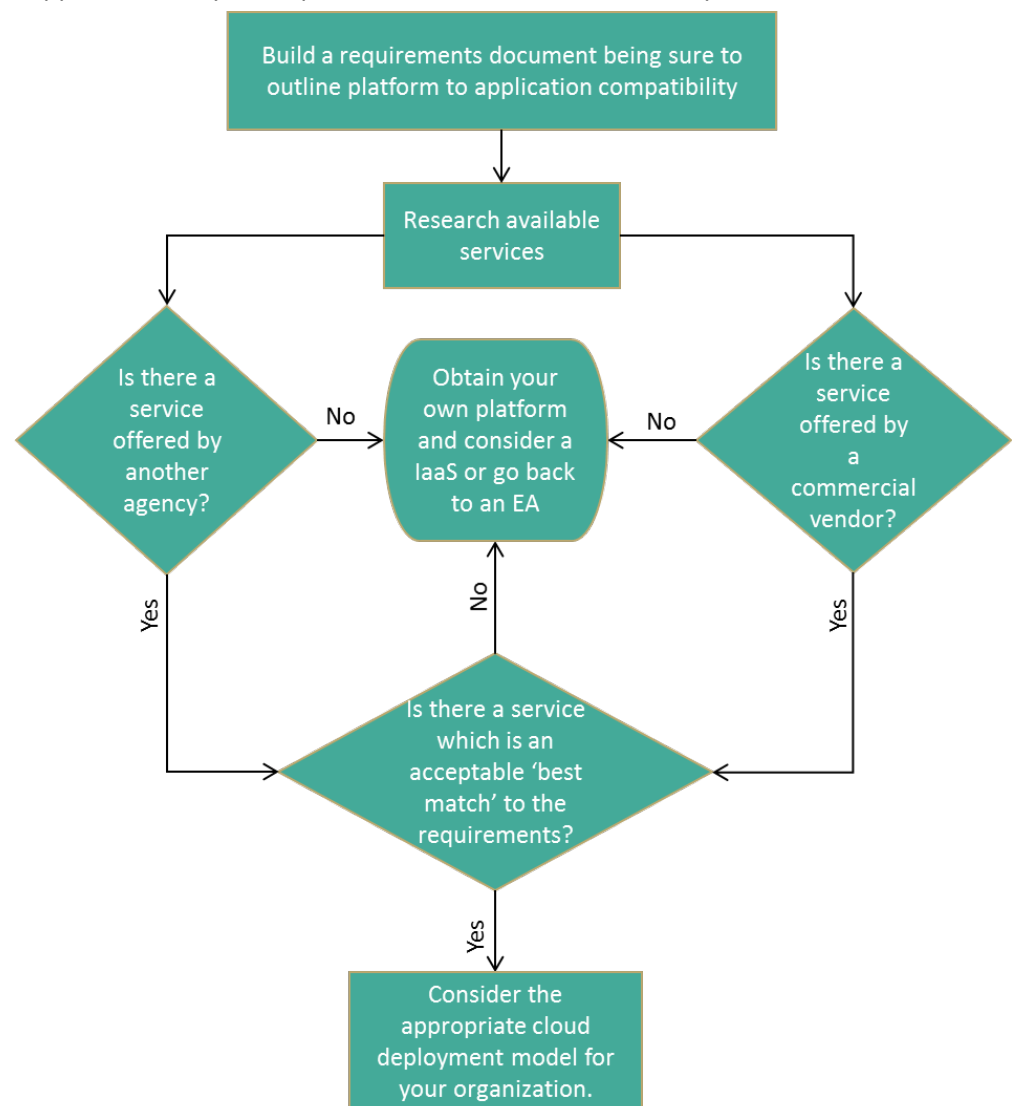


Figure 78: Purchase PaaS

A4.6.9 Purchasing IaaS

In IaaS, a cloud provider primarily supplies the use of hardware with no software. It is up to the consumer to acquire, install, and maintain any software to run on the hardware. IaaS services are great for organizations that want to maintain full control over all software aspects of their system but do not have the resources to meet the electrical, physical storage space, internet connection, and/or other requirements or perhaps cannot afford to purchase and maintain such systems.

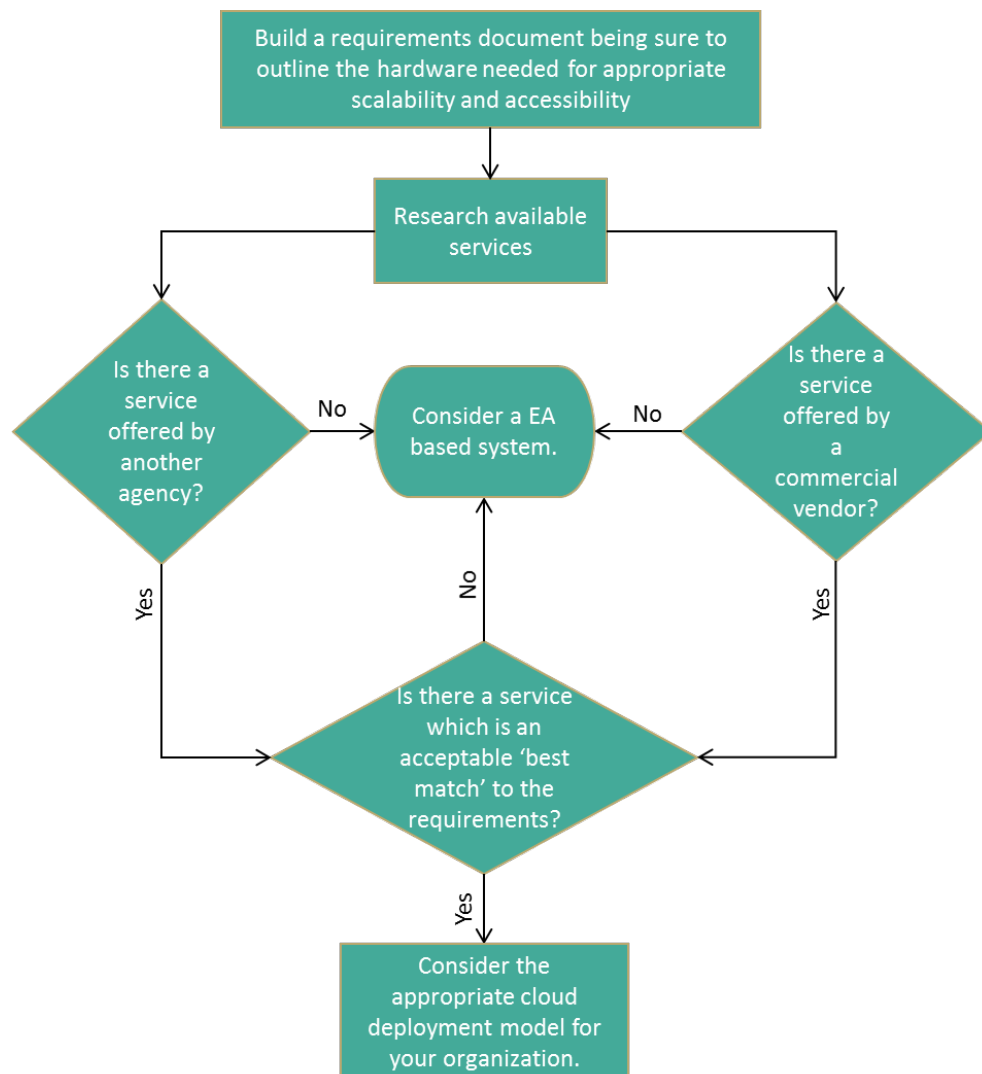


Figure 79: Purchase IaaS

A4.7 Purchasing COTS

If you need an internally supported system (such as an Enterprise Architecture) but can't deal with the overhead generated by system development, maintenance, and upgrades then COTS may be best for you. COTS solutions transfer the lifecycle management for software to the vendor but at the cost of ownership and control.

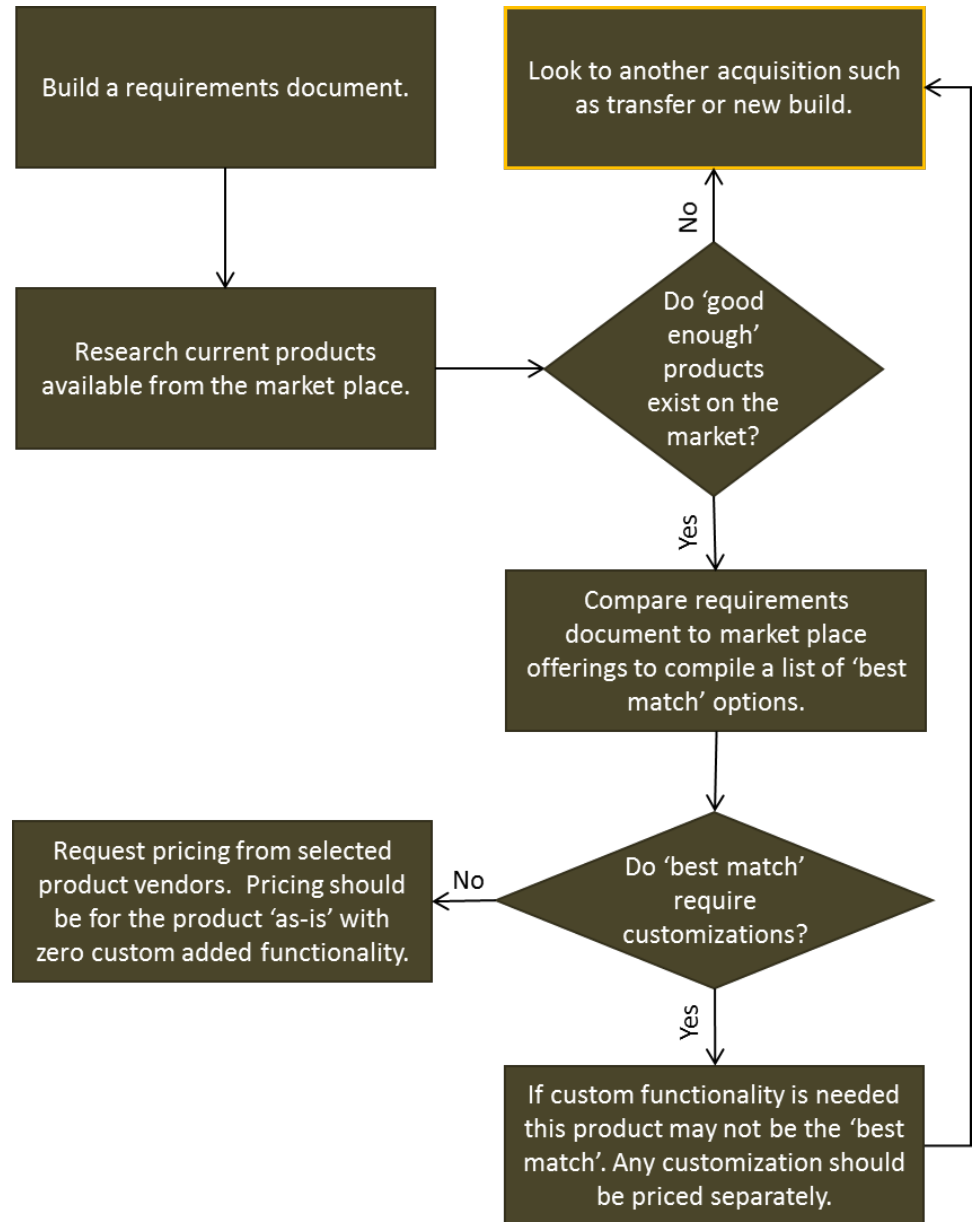


Figure 80: Purchase COTS

A4.8 Upgrade Current System

If you already have a functional system in-place, perhaps the most cost effective option would be to simply maintain the current system. Utilizing internal resources or hiring third-party contractors to write updates and upgrades may be a much more viable option than acquiring a new system.

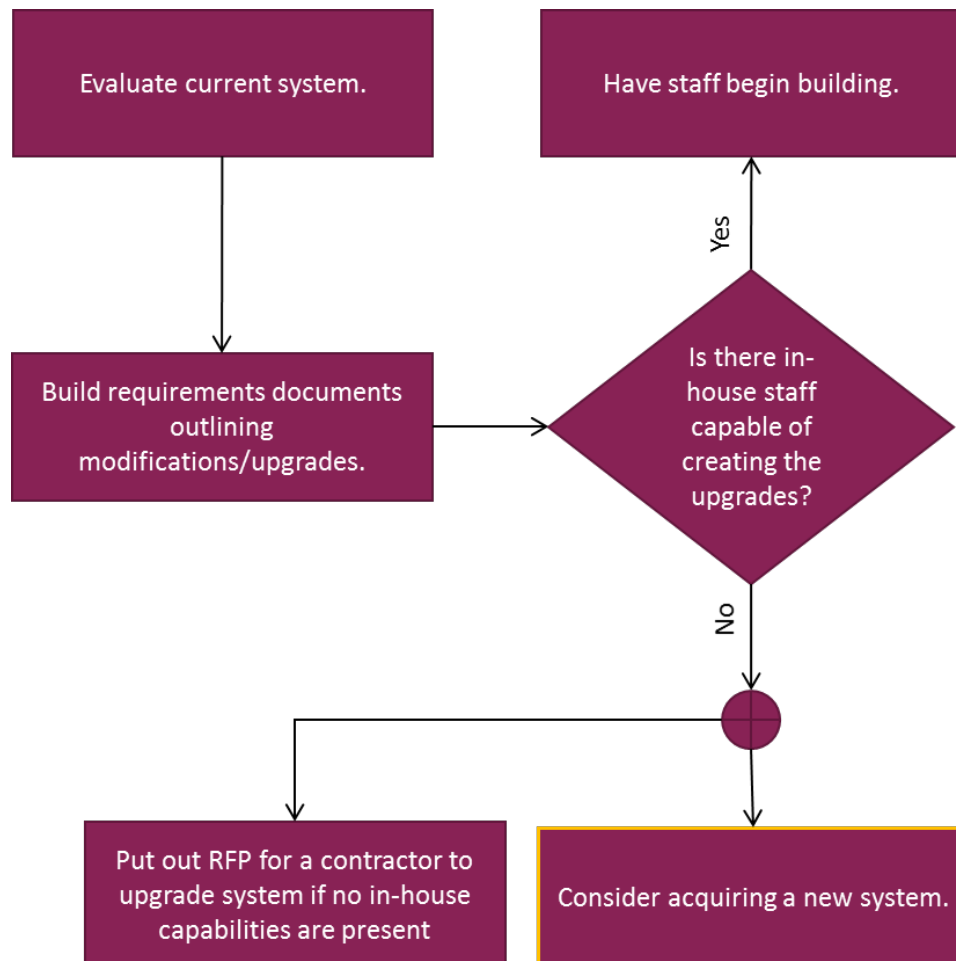


Figure 81: Upgrade Current System

A4.9 Transfer an Existing System

A transfer system is a good choice if another agency already has a system in-place that matches your requirements. Cost savings can be realized by not having to reinvent the system making migration, customization, and infrastructure the major concerns. If infrastructure and other operating resources are a major concern, it is possible to obtain a transfer but deploy it to the cloud instead of internally to an Enterprise Architecture.

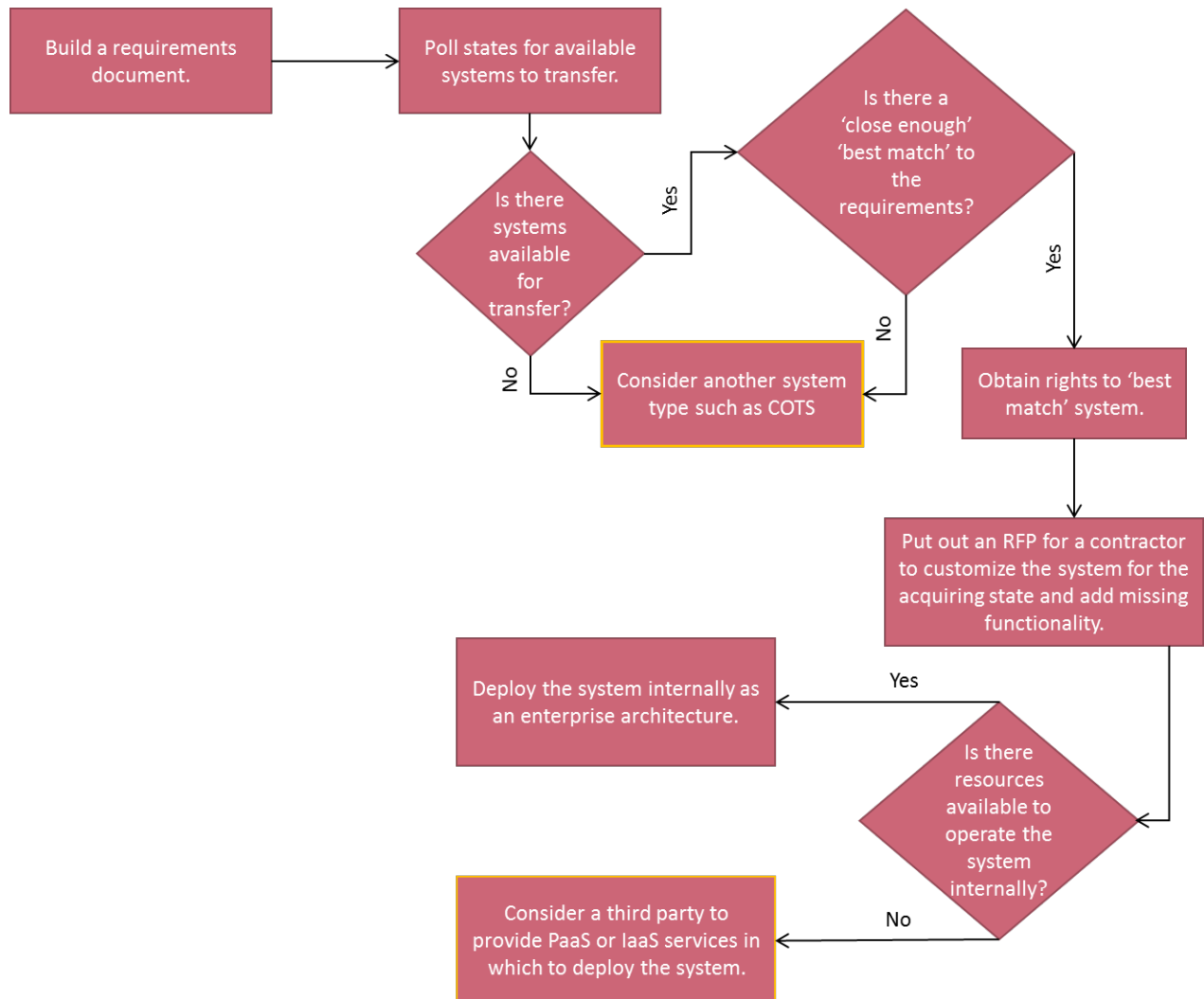


Figure 82: Transfer Existing System

A4.10 Custom Built System

A custom built system is the most expensive way to obtain a system, however it allows for the highest degree of business process to technology matching while also providing all features and functionality demanded from the system.

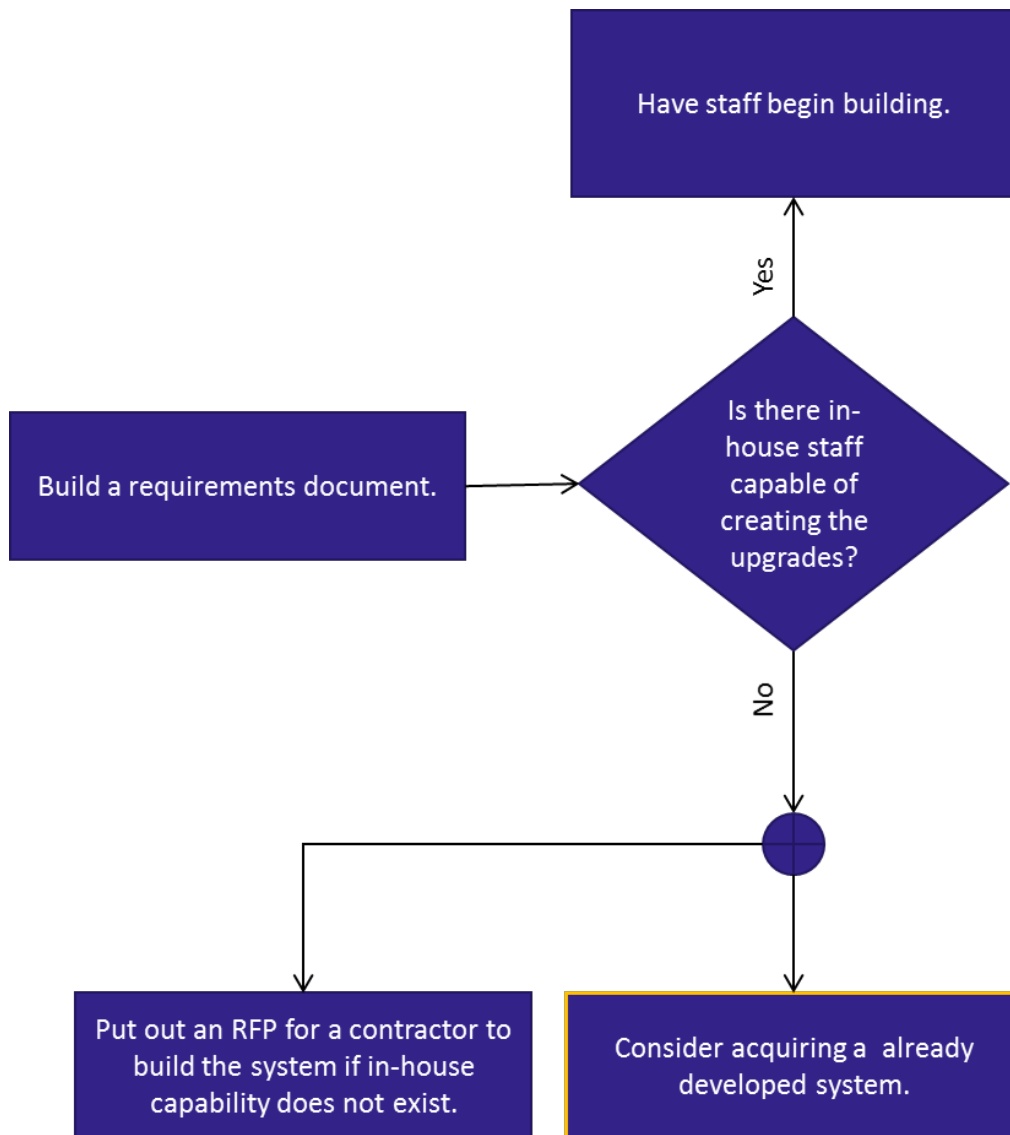


Figure 83: Custom Built System



A5. Feasibility Study Worksheet

Justification: Based on your comparison and your evaluation criteria, how do the systems compare?

Which one(s) merit further consideration of their costs and benefits? Why?

FEASIBILITY STUDY

	SYSTEM NAME			
Requirement	Current System	Alternative 1	Alternative 2	Alternative 3
Objectives				
Requirements				
Assumptions and constraints				
Technical maturity of solution				
Compatibility of this system with state standards for hardware, architecture or environment				



FEASIBILITY STUDY

	SYSTEM NAME			
Requirement	Current System	Alternative 1	Alternative 2	Alternative 3
Compatibility of this system with other necessary software or applications				
Organizational impacts of this system				
Facility/site impacts				
Operational impacts*				
Fiscal impacts**				
*(e.g., user operating procedures, data center procedures, source data management, data entry procedures, data retention requirements, plans for system support, archiving, etc.)				
**(e.g., cost factors related to the design, development, or transfer and operation of this system)				



A6. Cost Benefit Analysis Worksheet

A6.1 Costs

Directions: Use the following tables to identify and outline the nonrecurring (design, development, and implementation) and recurring, (operations and maintenance) costs for the current system. Add a similar detailed narrative for each alternative system being considered before starting the Cost Benefit Analysis (CBA).

Nonrecurring Costs (Design, Development, Implementation)

Costs	Current System	Alternative 1	Alternate 2	Alternate 3
Capital Investment Costs				
Site And Facility				
IT Equipment				
Data Communications Equipment				
Environmental Conditioning Equipment (Central Processing Site)				
Security and Privacy Equipment				



Nonrecurring Costs (Design, Development, Implementation)

Costs	Current System	Alternative 1	Alternate 2	Alternate 3
Capital Investment Costs				
Database				
Other Nonrecurring Costs				
Database Preparation				
Data Conversion				
Training, Travel, And Other Personnel-Related Costs Of Development And Installation				
Contractual, Interagency, Or Other Direct Support Services				



Recurring Costs (M&O)

Costs	Current System	Proposed System	Alternate 1	Alternate 2
Software, Lease, Rentals, And Maintenance				
Data Communications Lease, Rentals, And Maintenance				
Personnel Salaries And Fringe Benefits				
Equipment, Lease, Rentals, And Maintenance				
Personnel Salaries And Fringe Benefits				
Direct Support Services*				



Recurring Costs (M&O)

Costs	Current System	Proposed System	Alternate 1	Alternate 2
Travel And Training				
Space Occupancy				
Supplies And Utilities				
Security And Privacy				
Other Costs That Are Unique To Current System Or Alternative				
*(e.g., Help Desk, Central Processing Site Operations)				



A6.2 Benefits

Directions: Similar to assessing costs, use the following table to identify the quantifiable and non-quantifiable benefits that could be attained through the development of each proposed alternative. Only 'Cost Reduction' and 'Value Enhancement' are categories of benefit. The rest are just costs as listed above.

Quantifiable Benefits

Benefits	Current System	Alternative 1	Alternative 2	Alternative 3
Cost Reduction*				
Value Enhancement**				
Equipment Lease, Rentals, and Maintenance				
Software Lease, Rentals, and Maintenance				
Data Communications Lease, Rentals, and Maintenance				



Quantifiable Benefits

Benefits	Current System	Alternative 1	Alternative 2	Alternative 3
Personnel Salaries and Fringe Benefits				
Direct Support Services				
Travel and Training				
Space Occupancy				
Security and Privacy				
Contractual and Interagency Services				
Cost Avoidance of Future Costs that Would be Incurred if the Best Alternative were Chosen				
*(e.g., resulting from improved data entry, storage, and retrieval techniques)				
**(e.g., improved resources use, reduced error rates)				



Non-quantifiable Benefits

Costs	Current System	Alternative 1	Alternative 2	Alternative 3
Ease Of Use				
Information Can Be Shared Efficiently				
Increased Cross Functional Communications				
Better Performance Of Business Processes				



A7. Sample Transmittal Letter

A7.1 Transmittal Letter Template

This sample letter in this appendix is a suggested guideline, and models the Transmittal Letter Template Checklist found below. The sample letter begins in section **A7.2** on page **516**.

The following text styles are used throughout this sample letter:

- **Guidance Text** - *Descriptions, guidance, information, and suggestions of what to include in a particular section of the letter.*
- Sample Text - An example or concept that applies to the section and could be used with minor updates.
- **<<“Fill-In” Data>>** – **Information or data the State agency needs to “fill-in” based on their requirements.**

Transmittal Letter Template Checklist

✓	ITEM	COMMENT
	Agency Letterhead	
	Date	Letter date should not be significantly earlier than the actual date of transmittal.
	Federal Addressee(s)	Signed letter should be scanned and sent electronically rather than by hardcopy delivery.
	Salutation	May be: “Dear Mr/Ms (Name)” if single addressee or “Dear Colleagues” if multiple addressees.
	Purpose of Letter (introductory paragraph)	Request for review and approval of (type(s) of document(s)) relating to (project name). Any urgent/time critical issue to be discussed further in letter.
	Summary of Document Purpose/Main Content/Significant Issues (body of letter)	May use a combination of narrative paragraph and bullet/numerical item formats.
	Extracts or References to Major Points (body of letter)	Goals, Objectives, Time Period Covered, Cost Estimate, etc.



Transmittal Letter Template Checklist

✓	ITEM	COMMENT
	Summary of Next Steps/Future Efforts (closing paragraph)	Provide larger perspective and/or activity to be taken on project in near future.
	Closing	Contact information for questions, etc.
	Signature	Responsible official with authority to make commitments for agency.
	Attachment(s)/Enclosure(s)	May simply indicate that there are items included with the cover letter or may list the actual items.
	Addressee Copies	List of others copy of document to be sent.



A7.2 Sample Transmittal Letter

<<Your State>>
<<Office of the Department>>
<<123 Your Street
Your City, State 12345>>

<<Month 00, Year>>

<<Mr./Ms. Smith>>

Regional Administrator

<<XXXXXX>> Regional Office

Food and Nutrition Service

U.S. Department of Agriculture

<<Address

City, State 12345>>

<<Dear Mr./Ms. Smith>>,

Enclosed for your agency's approval is the Quality Assurance (QA) Services Request for Proposal (RFP) to procure services from a third-party vendor for QA oversight of several critical technology solutions and projects as well as modernization planning efforts. The State has employed Quality Assurance throughout the Systems Development Lifecycle for major application development and planning projects. The current engagement for QA services ends <<Month, Day, Year>>. In order to ensure continuity of QA services, the State is seeking to execute a contract resulting from this procurement no later than Month and Year.

The selected vendor will provide quality assurance reviews, project risk analysis, and assistance with planning and setting of quality goals and objectives for the following projects and activities:

- Functional Roadmap Project
- Imaging/Enterprise Document Repository and On-site Scanning
- State Support Enforcement and Tracking System
- Enterprise Architecture, IT Governance and Outcome Management Office activities
- myBenefits/myWorkspace
- Open Systems Disaster Recovery Procedures

The State is also seeking pricing within the RFP for QA for projects that may be initiated during the duration of the contract resulting from this RFP. At this time those costs are not part of the project budgets nor are the activities



included in the QA RFP work plans. In the event these projects are initiated, the State will seek prior federal approval of QA activities, deliverables, and associated costs.

The contract term is three years with two extensions of up to twelve months each. Please note at this time the State is not seeking approval of possible contract extension periods. The State will seek prior federal approval should the contract extensions be necessary.

The estimated acquisition cost is \$6 million over the three-year contract term. Actual contract costs may vary based on pricing received as a result of the bid process. The following chart depicts estimated contractual costs for each project:

PROJECT	YR 1	YR 2	YR 3	EXTENDED COST
Functional Roadmap Project	\$252,845	\$252,845	\$252,845	\$758,536
Imaging/Enterprise Document Repository and On-site Scanning	\$217,599	\$217,599	\$217,599	\$652,796
State Support Enforcement and Tracking System	\$275,854	\$275,854	\$275,854	\$827,561
Enterprise Architecture/Outcome Management Office	\$565,659	\$565,659	\$565,659	\$1,696,977
MY BENEFIT/WORKSPACE	\$541,917	\$541,917	\$541,917	\$1,625,750
Open Systems Disaster Recovery	\$146,127	\$146,127	\$146,127	\$438,380
TOTAL	\$2,000,000	\$2,000,000	\$2,000,000	\$6,000,000

Exhibits A-G of this document allocate projected QA contract costs by federal and state benefitting programs based on the approved federal cost allocation plans.

Thank you for your continued support and cooperation. If you require any additional information, please contact <<State Person>> at <<123-456-7890>>, or by email at <<state.person@xx.state.us>>

Sincerely,

Signed by an official authorized to commit State resources

<<Your Name>>

<<Your Title>>

Enclosures

cc: Regional Office Program Director
State Systems Office Contact person



A8. Sample Budgets

A8.1 Sample PAPD Budget

Task/Line Item		Fiscal Year (FY)				FY Total	Fiscal Year (FY)				FY Total	Project Total
		Q1	Q2	Q3	Q4		Q1	Q2	Q3	Q4		
State Costs	State Travel	\$3,926	\$5,526	\$3,035	\$5,252	\$17,739	\$6,852	\$0	\$0	\$0	\$6,852	\$24,591
	Local Travel	\$100	\$325	\$225	\$225	\$875	\$50	\$50	\$200	\$200	\$500	\$1,375
	Staff Time	\$2,596	\$3,289	\$2,397	\$3,108	\$11,390	\$4,720	\$1,284	\$1,284	\$985	\$8,273	\$19,663
	LA Staff Time	\$200	\$298	\$189	\$144	\$831	\$200	\$128	\$128	\$128	\$584	\$1,415
	Equipment	\$0	\$0	\$0	\$0		\$6,809	\$3,732	\$0	\$0	\$10,541	\$10,541
	IT Support	\$0	\$0	\$698	\$1,290	\$1,988	\$7,890	\$698	\$328	\$0	\$8,916	\$10,904
	Indirect	\$779	\$220	\$515	\$4,389	\$5,903	\$5,423	\$4,708	\$4,730	\$30	\$14,891	\$20,794
	State Subtotal	\$7,601	\$9,658	\$7,059	\$14,408	\$38,726	\$31,944	\$10,600	\$6,670	\$1,343	\$50,557	\$89,283
Contractor Costs	Travel	\$0	\$0	\$21,520	\$22,450	\$43,970	\$10,500	\$13,830	\$1,500	\$0	\$25,830	\$69,800
	Site Survey	\$0	\$0	\$48,480	\$47,550	\$96,030	\$0	\$0	\$0	\$0	\$0	\$96,030
	Develop RFP	\$0	\$0	\$0	\$0	\$0	\$5,800	\$10,550	\$650	\$0	\$17,000	\$17,000
	Develop IAPD	\$0	\$0	\$0	\$0	\$0	\$25,786	\$22,654	\$2,460	\$0	\$50,900	\$50,900
	Contr. Subtotal	\$0	\$0	\$70,000	\$70,000	\$140,000	\$42,086	\$47,034	\$4,610	\$0	\$93,730	\$233,730
Total		\$7,601	\$9,658	\$77,059	\$84,408	\$178,726	\$74,030	\$57,634	\$11,280	\$1,343	\$144,287	\$323,013

Date Submitted:



A8.2 Sample IAPD/U Budget

Contains actuals to date.

A8.2.1 Year One

Year One

Months	Apr-Jun	Apr-Jun	Jul-Sept	Jul-Sept	Total	Total
	Projected	Actual	Projected	Actual	Projected	Actual
	3rd Quarter	3rd Quarter	4th Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers						
<i>DDI Contractor</i>	\$150,000	\$78,944	\$750,000	\$724,323	\$900,000	\$803,267
<i>QA Contractor</i>	\$20,000	\$27,500	\$30,000	\$30,000	\$50,000	\$57,500
<i>Direct Personnel</i>	\$25,000	\$26,512	\$25,000	\$26,512	\$50,000	\$53,024
<i>Equipment</i>	\$0	\$0	\$0	\$0	\$0	\$0
<i>Travel</i>	\$0	\$0	\$0	\$3,695	\$0	\$3,695
<i>Training</i>	\$0	\$0	\$0	\$0	\$0	\$0
<i>Indirect Costs</i>	\$10,000	\$11,253	\$10,000	\$11,253	\$20,000	\$22,506
Total	\$205,000	\$144,209	\$815,000	\$795,783	\$1,020,000	\$939,992
						Program Allocation
TANF Portion 4.56%	\$9,348	\$6,576	\$37,164	\$36,288	\$46,512	\$42,864



Year One

Months	Apr-Jun	Apr-Jun	Jul-Sept	Jul-Sept	Total	Total
	Projected	Actual	Projected	Actual	Projected	Actual
	3rd Quarter	3rd Quarter	4th Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers						
State (0%)	\$0	\$0	\$0	\$0	\$0	\$0
Federal (100%)	\$9,348	\$6,576	\$37,164	\$36,288	\$46,512	\$42,864
FNS Portion 37.51%	\$76,896	\$54,093	\$305,707	\$298,498	\$382,602	\$352,591
State (50%)	\$38,448	\$27,046	\$152,853	\$149,249	\$191,301	\$176,295
Federal (50%)	\$38,448	\$27,046	\$152,853	\$149,249	\$191,301	\$176,295
Medicaid Portion 57.7%	\$118,285	\$83,209	\$470,255	\$459,167	\$588,540	\$542,375
State (10%)	\$11,829	\$8,321	\$47,026	\$45,917	\$58,854	\$54,238
Federal (90%)	\$106,457	\$74,888	\$423,230	\$413,250	\$529,686	\$488,138
State Only Portion 0.23%	\$472	\$332	\$1,875	\$1,830	\$2,346	\$2,162
Total Federal Share	\$154,252	\$108,510	\$613,247	\$598,787	\$767,499	\$707,297
Total State Share	\$50,748	\$35,699	\$201,753	\$196,996	\$252,501	\$232,695
Total	\$205,000	\$144,209	\$815,000	\$795,783	\$1,020,000	\$939,992



A8.2.2 Year Two

Year Two

Months	Oct-Dec	Oct-Dec	Jan-Mar	Jan-Mar	Apr-Jun	Apr-Jun	Total	Total
	Projected	Actual	Projected	Actual	Projected	Projected	Projected Remaining	Actual
	1st Quarter	1st Quarter	2nd Quarter	2nd Quarter	3rd Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers								
<i>DDI Contractor</i>	\$1,250,000	\$1,375,000	\$1,250,000	\$1,250,000	\$1,250,000	\$1,250,000	\$2,500,000	\$2,625,000
<i>QA Contractor</i>	\$30,000	\$30,000	\$30,000	\$30,000	\$30,000	\$30,000	\$60,000	\$60,000
<i>Direct Personnel</i>	\$25,000	\$26,512	\$25,000	\$17,501	\$25,000	\$25,000	\$50,000	\$44,013
<i>Equipment</i>	\$0	\$34,268	\$750,000	\$789,666	\$750,000	\$850,000	\$1,600,000	\$823,934
<i>Travel</i>	\$10,000	\$8,544	\$10,000	\$13,877	\$10,000	\$10,000	\$20,000	\$22,421
<i>Training</i>	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
<i>Indirect Costs</i>	\$10,000	\$11,253	\$10,000	\$8,553	\$10,000	\$10,000	\$20,000	\$19,806
Total	\$1,325,000	\$1,485,577	\$2,075,000	\$2,109,597	\$2,075,000	\$2,175,000	\$4,250,000	\$3,595,174
Program Allocation								
<i>TANF Portion</i>	\$60,420	\$67,742	\$94,620	\$96,198	\$94,620	\$99,180	\$193,800	\$163,940
<i>State (0%)</i>	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
<i>Federal (100%)</i>	\$60,420	\$67,742	\$94,620	\$96,198	\$94,620	\$99,180	\$193,800	\$163,940
<i>FNS Portion 37.51%</i>	\$497,008	\$557,240	\$778,333	\$791,310	\$778,333	\$815,843	\$1,594,175	\$1,348,550



Year Two

Months	Oct-Dec	Oct-Dec	Jan-Mar	Jan-Mar	Apr-Jun	Apr-Jun	Total	Total
	Projected	Actual	Projected	Actual	Projected	Projected	Projected Remaining	Actual
	1st Quarter	1st Quarter	2nd Quarter	2nd Quarter	3rd Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers								
<i>State (50%)</i>	\$248,504	\$278,620	\$389,166	\$395,655	\$389,166	\$407,921	\$797,088	\$674,275
<i>Federal (50%)</i>	\$248,504	\$278,620	\$389,166	\$395,655	\$389,166	\$407,921	\$797,088	\$674,275
<i>Medicaid Portion 57.7%</i>	\$764,525	\$857,178	\$1,197,275	\$1,217,237	\$1,197,275	\$1,254,975	\$2,452,250	\$2,074,415
<i>State (10%)</i>	\$76,453	\$85,718	\$119,728	\$121,724	\$119,728	\$125,498	\$245,225	\$207,442
<i>Federal (90%)</i>	\$688,073	\$771,460	\$1,077,548	\$1,095,514	\$1,077,548	\$1,129,478	\$2,207,025	\$1,866,974
<i>State Only Portion 0.23%</i>	\$3,048	\$3,417	\$4,773	\$4,852	\$4,773	\$5,003	\$9,775	\$8,269
<i>Total Federal Share</i>	\$996,996	\$1,117,822	\$1,561,334	\$1,587,366	\$1,561,334	\$1,636,579	\$3,197,913	\$2,705,189
<i>Total State Share</i>	\$328,004	\$367,755	\$513,666	\$522,231	\$513,666	\$538,421	\$1,052,088	\$889,985
Total	\$1,325,000	\$1,485,577	\$2,075,000	\$2,109,597	\$2,075,000	\$2,175,000	\$4,250,000	\$3,595,174



A8.2.3 Year Three

Year Three

Months	Oct-Dec	Jan-Mar	Apr-Jun	Jul-Sept	Total	Total
	Projected	Projected	Projected	Projected	Projected	Actual
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers						
<i>DDI Contractor</i>	\$1,250,000	\$1,250,000	\$1,250,000	\$1,250,000	\$5,000,000	\$0
<i>QA Contractor</i>	\$30,000	\$30,000	\$30,000	\$30,000	\$120,000	\$0
<i>Direct Personnel</i>	\$75,000	\$75,000	\$75,000	\$75,000	\$300,000	\$0
<i>Equipment</i>	\$150,000	\$125,000	\$75,000		\$350,000	\$0
<i>Travel</i>	\$10,000	\$10,000	\$40,000	\$80,000	\$140,000	\$0
<i>Training</i>			\$200,000	\$400,000	\$600,000	\$0
<i>Indirect Costs</i>	\$25,000	\$25,000	\$25,000	\$25,000	\$100,000.00	\$0
Total	\$1,540,000	\$1,515,000	\$1,695,000	\$1,860,000	\$6,610,000	\$0
Program Allocation						
TANF Portion	\$70,224	\$69,084	\$77,292	\$84,816	\$301,416	\$0
<i>State (0%)</i>	\$0	\$0	\$0	\$0	\$0	\$0
<i>Federal (100%)</i>	\$70,224	\$69,084	\$77,292	\$84,816	\$301,416	\$0
FNS Portion 37.51%	\$577,654	\$568,277	\$635,795	\$697,686	\$2,479,411	\$0
<i>State (50%)</i>	\$288,827	\$284,138	\$317,897	\$348,843	\$1,239,706	\$0



Year Three

Months	Oct-Dec	Jan-Mar	Apr-Jun	Jul-Sept	Total	Total
	Projected	Projected	Projected	Projected	Projected	Actual
	1st Quarter	2nd Quarter	3rd Quarter	4th Quarter	FFY 20xx	FFY 20xx
Cost Centers						
<i>Federal (50%)</i>	\$288,827	\$284,138	\$317,897	\$348,843	\$1,239,706	\$0
Medicaid Portion 57.7%	\$888,580	\$874,155	\$978,015	\$1,073,220	\$3,813,970	\$0
<i>State (10%)</i>	\$88,858	\$87,416	\$97,802	\$107,322	\$381,397	\$0
<i>Federal (90%)</i>	\$799,722	\$786,740	\$880,214	\$965,898	\$3,432,573	\$0
<i>State Only Portion 0.23%</i>	\$3,542	\$3,485	\$3,899	\$4,278	\$15,203	\$0
<i>Total Federal Share</i>	\$1,158,773	\$1,139,962	\$1,275,403	\$1,399,557	\$4,973,695	\$0
<i>Total State Share</i>	\$381,227	\$375,038	\$419,597	\$460,443	\$1,636,306	\$0
Total	\$1,540,000	\$1,515,000	\$1,695,000	\$1,860,000	\$6,610,000	\$0

**A8.2.4 Year Four**

Months	Oct-Dec	Jan-Mar	Apr-Jun	Total	Total
	Projected	Projected	Projected	Projected	Actual
	1st Quarter	2nd Quarter	3rd Quarter	FFY 20xx	FFY 20xx
Cost Centers					
DDI Contractor	\$1,250,000	\$1,250,000	\$1,250,000	\$3,750,000	\$0
QA Contractor	\$30,000	\$30,000	\$30,000	\$90,000	\$0
Direct Personnel	\$75,000	\$75,000	\$75,000	\$225,000	\$0
Equipment	\$0	\$0	\$0	\$0	\$0
Travel	\$80,000	\$80,000	\$80,000	\$240,000	\$0
Training	\$400,000	\$400,000	\$400,000	\$1,200,000	\$0
Indirect Costs	\$25,000	\$25,000	\$25,000	\$75,000	\$0
Total	\$1,860,000	\$1,860,000	\$1,860,000	\$5,580,000	\$0
Program Allocation					
TANF Portion	\$84,816	\$84,816	\$84,816	\$254,448	\$0
State (0%)	\$0	\$0	\$0	\$0	\$0
Federal (100%)	\$84,816	\$84,816	\$84,816	\$254,448	\$0
FNS Portion 37.51%	\$697,686	\$697,686	\$697,686	\$2,093,058	\$0
State (50%)	\$348,843	\$348,843	\$348,843	\$1,046,529	\$0
Federal (50%)	\$348,843	\$348,843	\$348,843	\$1,046,529	\$0



Months	Oct-Dec	Jan-Mar	Apr-Jun	Total	Total
	Projected	Projected	Projected	Projected	Actual
	1st Quarter	2nd Quarter	3rd Quarter	FFY 20xx	FFY 20xx
Cost Centers					
Medicaid Portion 57.7%	\$1,073,220	\$1,073,220	\$1,073,220	\$3,219,660	\$0
State (10%)	\$107,022	\$107,022	\$107,022	\$321,966	\$0
Federal (90%)	\$965,898	\$965,898	\$965,898	\$2,897,694	\$0
State Only Portion 0.23%	\$4,278	\$4,278	\$4,278	\$12,834	\$0
Total Federal Share	\$1,399,557	\$1,399,557	\$1,399,557	\$4,198,671	\$0
Total State Share	\$460,443	\$460,443	\$460,443	\$1,381,329	\$0
Total	\$1,860,000	\$1,860,000	\$1,860,000	\$5,580,000	\$0



A8.2.5 Total Summary Budget

Budget Total – All Years

Federal Fiscal Year	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	ALL FFYs		
	Year One	Year Two	Year Two	Year Three	Year Four	Grand Totals		
	Actual	Actual 1st & 2nd Qtrs	Projected 3rd & 4th Qtrs	Projected	Projected	Total Projected Remaining	Actuals to Date	Total Projected Remaining + Actuals to Date
Cost Centers								
<i>DDI Contractor</i>	\$803,267	\$2,625,000	\$2,500,000	\$5,000,000	\$3,750,000	\$11,250,000	\$3,428,267	\$14,678,267
<i>QA Contractor</i>	\$57,500	\$60,000	\$60,000	\$120,000	\$90,000	\$270,000	\$117,500	\$387,500
<i>Direct Personnel</i>	\$53,024	\$44,013	\$50,000	\$300,000	\$225,000	\$575,000	\$97,037	\$672,037
<i>Equipment</i>	\$0	\$823,934	\$1,600,000	\$350,000	\$0	\$1,950,000	\$823,934	\$2,773,934
<i>Travel</i>	\$3,695	\$22,421	\$20,000	\$140,000	\$240,000	\$400,000	\$26,116	\$426,116
<i>Training</i>	\$0	\$0	\$0	\$600,000	\$1,200,000	\$1,800,000	\$0	\$1,800,000
Indirect Costs	\$22,506	\$19,806	\$20,000	\$100,000	\$75,000	\$195,000	\$42,312	\$237,312



Budget Total – All Years

Federal Fiscal Year	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	ALL FFYs		
	Year One	Year Two	Year Two	Year Three	Year Four	Grand Totals		
	Actual	Actual 1st & 2nd Qtrs	Projected 3rd & 4th Qtrs	Projected	Projected	Total Projected Remaining	Actuals to Date	Total Projected Remaining + Actuals to Date
Cost Centers								
<i>Total Computable</i>	\$939,992	\$3,595,174	\$4,250,000	\$6,610,000	\$5,580,000	\$16,440,000	\$4,535,166	\$20,975,166
Program Allocation								
TANF Portion 4.56%	\$42,864	\$163,940	\$193,800	\$301,416	\$254,448	\$749,664	\$206,804	\$956,468
<i>State (0%)</i>	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
<i>Federal (100%)</i>	\$42,864	\$163,940	\$193,8000	\$301,416	\$254,448	\$749,664	\$206,804	\$956,467
FNS Portion 37.51%	\$352,591	\$1,348,550	\$1,594,175	\$2,479,411	\$2,093,058	\$6,166,644	\$1,701,141	\$7,867,785
<i>State (50%)</i>	\$176,295	\$674,275	\$797,088	\$1,239,706	\$1,046,529	\$3,083,322	\$850,570	\$3,933,892
Federal (50%)	\$176,295	\$674,275	\$797,088	\$1,239,706	\$1,046,529	\$3,083,322	\$850,570	\$3,933,892



Budget Total – All Years

Federal Fiscal Year	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	FFY 20xx	ALL FFYs		
	Year One	Year Two	Year Two	Year Three	Year Four	Grand Totals		
	Actual	Actual 1st & 2nd Qtrs	Projected 3rd & 4th Qtrs	Projected	Projected	Total Projected Remaining	Actuals to Date	Total Projected Remaining + Actuals to Date
Cost Centers								
<i>Medicaid Portion 57.70%</i>	\$542,375	\$2,074,415	\$2,452,250	\$3,813,970	\$3,219,660	\$9,485,880	\$2,616,791	\$12,102,671
<i>State (10%)</i>	\$54,238	\$207,442	\$245,225	\$381,397	\$321,966	\$948,588	\$261,679	\$1,210,671
<i>Federal (90%)</i>	\$488,138	\$1,866,974	\$2,207,025	\$3,432,573	\$2,897,694	\$8,537,292	\$2,355,112	\$10,892,404
<i>State Only Portion 0.23%</i>	\$2,162	\$8,269	\$9,775	\$15,203	\$12,834	\$37,812	\$10,431	\$48,243
<i>Total Federal Share</i>	\$707,297	\$2,705,189	\$3,197,913	\$4,973,695	\$4,198,671	\$12,370,278	\$3,412,485	\$15,782,763
<i>Total State Share</i>	\$232,695	\$889,985	\$1,052,088	\$1,636,306	\$1,381,329	\$4,069,722	\$1,122,680	\$5,192,402
<i>Total</i>	\$939,992	\$3,595,174	\$4,250,000	\$6,610,000	\$5,580,000	\$16,440,000	\$4,535,166	\$20,975,166



A8.3 Total Summary Budget

	Year One		Year Two		Year Three		Year Four		Grand Total	
Cost Centers	Projected	Actual	Projected	Actual	Projected	Actual	Projected	Actual	Projected	Actual
<i>DDI Contractor</i>	\$900,000	\$803,267	\$5,000,000	\$2,625,000	\$5,000,000	\$0	\$3,750,000	\$0	\$14,650,000	\$3,428,267
<i>QA Contractor</i>	\$50,000	\$57,500	\$120,000	\$60,000	\$120,000	\$0	\$90,000	\$0	\$380,000	\$117,500
<i>Direct Personnel</i>	\$50,000	\$53,024	\$100,000	\$44,013	\$300,000	\$0	\$225,000	\$0	\$675,000	\$97,037
<i>Equipment</i>	\$0	\$0	\$2,350,000	\$823,934	\$350,000	\$0	\$0	\$0	\$2,700,000	\$823,934
<i>Travel</i>	\$0	\$3,695	\$40,000	\$22,421	\$140,000	\$0	\$240,000	\$0	\$420,000	\$26,116
<i>Training</i>	\$0	\$0	\$0	\$0	\$600,000	\$0	\$1,200,000	\$0	\$1,800,000	\$0
<i>Indirect Costs</i>	\$20,000	\$22,506	\$40,000	\$19,806	\$100,000	\$0	\$75,000	\$0	\$235,000	\$42,312
Total Computable	\$1,020,000	\$939,992	\$7,650,000	\$3,595,174	\$6,610,000	\$0	\$5,580,000	\$0	\$20,860,000	\$4,535,166
Program Allocation										
TANF Portion	\$46,512	\$42,864	\$348,840	\$163,940	\$301,416	\$0	\$254,448	\$0	\$951,216	\$206,804
<i>State (0%)</i>	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
<i>Federal (100%)</i>	\$46,512	\$42,864	\$348,840	\$163,940	\$301,416	\$0	\$254,448	\$0	\$951,216	\$206,804
FNS Portion	\$382,602	\$352,591	\$2,869,515	\$1,348,550	\$2,479,411	\$0	\$2,093,058	\$0	\$7,824,586	\$1,701,141
<i>State (50%)</i>	\$191,301	\$176,295	\$1,434,758	\$674,275	\$1,239,706	\$0	\$1,046,529	\$0	\$3,912,293	\$850,570
<i>Federal (50%)</i>	\$191,301	\$176,295	\$1,434,758	\$674,275	\$1,239,706	\$0	\$1,046,529	\$0	\$3,912,293	\$850,570



	Year One		Year Two		Year Three		Year Four		Grand Total	
Cost Centers	Projected	Actual	Projected	Actual	Projected	Actual	Projected	Actual	Projected	Actual
Medicaid Portion	\$588,540	\$542,375	\$4,414,050	\$2,074,415	\$3,813,970	\$0	\$3,219,660	\$0	\$12,036,220	\$2,616,791
<i>State (10%)</i>	\$58,854	\$54,238	\$441,405	\$207,442	\$381,397	\$0	\$321,966	\$0	\$1,203,622	\$261,679
<i>Federal (90%)</i>	\$529,686	\$488,138	\$3,972,645	\$1,866,974	\$3,432,573	\$0	\$2,897,694	\$0	\$10,832,598	\$2,355,112
State Only Portion	\$2,346	\$2,162	\$17,595	\$8,269	\$15,203	\$0	\$12,834	\$0	\$47,978	\$10,431
Total Federal Share	\$767,499	\$707,297	\$5,756,243	\$2,705,189	\$4,973,695	\$0	\$4,198,671	\$0	\$15,696,107	\$3,412,486
Total State Share	\$252,501	\$232,695	\$1,893,758	\$889,985	\$1,636,306	\$0	\$1,381,329	\$0	\$5,163,893	\$1,122,680
Total	\$1,020,000	\$939,992	\$7,650,000	\$3,595,174	\$6,610,000	\$0	\$5,580,000	\$0	\$20,860,000	\$4,535,166



A8.4 WIC EBT/MIS Funding Sources Table

PROJECT FUNDING SOURCES

STATE AGENCY NAME:					
SOURCE OF FUNDING	Source Year	Amount	Received? ✓	Spent? ✓	Requesting? ✓
A	XXXX	\$	-	-	-
B	XXXX	\$	-	-	-
C	XXXX	\$	-	-	-
D	XXXX	\$	-	-	-
E	XXXX	\$	-	-	-
F	XXXX	\$	-	-	-
TOTAL PROJECT BUDGET		\$	-	-	-

*Funding sources could be technology (National Office), infrastructure (National Office/Regional Office), operational adjustment, nutrition services and administration, ½ % spendforward, cost sharing (with approved cost allocation plan), State funds.

**Expand table as necessary to include all sources of funding.



A9. State Sole Source Exception Request

PROCUREMENT

STATE NAME:	
PROGRAM:	☐ SNAP ☐ WIC
PROJECT DESCRIPTION (BRIEF):	
CHECK ONE OF THE FOLLOWING:	☐ NEW PROCUREMENT ☐ EXTENSION TO EXISTING PROCUREMENT
DATE CURRENT CONTRACT ENDS:	
REFERENCE TO STATE PROCUREMENT RULE WHICH ALLOWS EXTENSIONS IF NOT PROVIDED BY CONTRACT/RFP:	
TYPE OF CONTRACT/SERVICES:	
☐ DEVELOPMENT	☐ Planning
☐ EBT Transaction Processor	☐ Project Management
☐ Enhancement	☐ Quality Assurance
☐ Hardware	☐ Software
☐ Independent Validation And Verification	☐ System Integrator
☐ Maintenance And Operations	☐ Transfer And Implementation
☐ OTHER (SPECIFY):	
PROPOSED CONTRACTOR/VENDOR:	
CURRENT AND/OR PREVIOUS RELATIONSHIP(S) WITH CONTRACTOR/VENDOR:	
PROPOSED SCOPE OF WORK AND RESPONSIBILITIES:	
PROPOSED CONTRACT AMOUNT:	PROPOSED CONTRACT TERM:



JUSTIFICATION

REASONABLE JUSTIFICATIONS INCLUDE SNAP: (7 CFR SECTIONS 277.14(G)(4) AND 277.18(C)); WIC: 2 CFR PART 200):

- VENDOR IS THE ONLY SOURCE OF THIS SERVICE
- PUBLIC EXIGENCY OR EMERGENCY SITUATION EXISTS, SUCH AS A NATURAL DISASTER
- FNS AUTHORIZES NON-COMPETITIVE PROCUREMENT
- AFTER SOLICITATION OF A NUMBER OF SOURCES, COMPETITION IS DETERMINED INADEQUATE

JUSTIFICATION FOR REQUEST (EXPLAIN):

WRITTEN ASSURANCE THAT STATE PROCUREMENT RULES SUPPORT SOLE SOURCE ACTION AND/OR STATE AUTHORITIES HAVE OR WILL APPROVE THIS ACTION:



A10. Request for Proposal Template

Contents

A10.1	Introduction.....	537
A10.1.1	How to Use this Template	537
A10.1.2	RFP and Contract Organization.....	538
A10.2	Template Contents	539
A10.2.1	Part I—The Schedule	540
A10.2.1.1	Section A – Solicitation/contract form.....	540
A10.2.1.2	Section B – Supplies or services and prices/costs	544
A10.2.1.3	Section C – Description/specifications/SOW	546
A10.2.1.4	Section D – Packaging and marking	554
A10.2.1.5	Section E – Inspection and acceptance.....	554
A10.2.1.6	Section F – Deliveries or performance	555
A10.2.1.7	Section G – Contract administration data.....	557
A10.2.1.8	Section H – Special contract requirements	557
A10.2.2	Part II—Contract Clauses	561
A10.2.2.1	Section I – Contract clauses	561
A10.2.3	Part III—List of Documents, Exhibits, and Other Attachments	565
A10.2.3.1	Section J – List of attachments	565
A10.2.4	Part IV—Representations and Instructions	566
A10.2.4.1	Section K – Representations, certifications, and other statements of offerors or respondents	566
A10.2.4.2	Section L – Instructions, conditions, and notices to offerors or respondents.....	566
A10.2.4.3	Section M – Evaluation factors for award	572
A10.3	Alternative RFP and Contract Formats.....	577



A10.3.1	RFP and Contract Format Alternative - Example One	578
A10.3.2	RFP and Contract Format Alternative - Example Two.....	580



A10.1 Introduction

The Food and Nutrition Service (FNS) Handbook 901 chapter **4.0 Procurement** provides the minimum required information and guidance for procurement planning. Appendix **A12 RFP and Contract Review Checklist** provides a checklist of items FNS will look for in requests for proposals (RFPs) and contracts. This appendix provides a suggested template for required content for RFP and contracts.

The RFP is not a legally binding document for procuring goods and services in the same way as a contract. It does not obligate either the State agency or the respondents to complete the proposed project. However, the contents of the RFP should reflect what the intended contract will bind both parties to once it is signed. In this sense, the composition, content, and layout of the RFP should correspond to that of the subsequent contract.

The purpose of this template is to assist the State agency in drafting an RFP and contract for their IS project(s). In no way do the examples provided constitute a complete RFP. They are for guidance only. All data provided in this template is an example of the content that could be included in an RFP and contract. However, it should not be used “as-is.” Information and data in any RFP and contract should only be used after proper procurement planning. Many of the examples are precursors to a more defined and in-depth document. The State agency must submit its RFP and resulting contract to FNS for review and approval prior to release and execution, based on applicable thresholds.



State agencies should ensure their RFPs and contracts include the same information as used in this template, taking into account your State policies and guidelines.

Refer to chapter **4.0 Procurement**, and appendix **A12 RFP and Contract Review Checklist**, along with this appendix, to build an RFP and contract compliant with FNS requirements.

A10.1.1 How to Use this Template

Beginning with section **A10.2 - Template Contents**, there will be three text styles used throughout the template. Each style communicates different elements of the template and are to be used in different ways.

1. *Guidance Text – Calibri font, Bold, Italic, Blue*

- a. *This style represents descriptions, instructions, guidance, information, and suggestions made to state agencies of what to include in a particular section of the RFP and contract.*
- b. *This text is not to be included in an RFP and contract.*



2. Fill-In Data –Calibri font, Bold, Plum

- a. This style represents Information or data the State agency needs to “fill-in” based on its procurement requirements.
- b. The data presented in this style is generic. Numbers are presented as <#>, proper nouns are presented in descriptive terms (e.g. <City Name, State Name>), and dates are presented as <MM/DD/YYYY> or <Date>.
- c. All individual fill-in data elements are separated by <brackets>.

3. Sample Text – Times New Roman font, Black

- a. This style represents example language or concepts that apply to the section. Examples are derived from real-life procurement documents. Common terms and processes may vary.
- b. While this is language that would normally be included in an RFP and contract, it should be updated or changed to correct information representative of the State agency’s procurement planning and procedures.
- c. In some cases the **<fill-in data style>** will be used concurrently within sample text.



This appendix provides a template only; it is not an RFP and/or contract. All data and examples should be replaced by data from decisions made after the appropriate procurement planning process for your project.

A10.1.2 RFP and Contract Organization

FNS does not prescribe a specific RFP or contract format for State agencies. Each State has its own procurement policies, regulations and forms. However, FNS does have expectations of what must and should be included in RFPs and contracts. The following example is based on the Uniform Contract Format (UCF) from the Federal Acquisition Regulations (FAR).¹³⁰ See section **A10.3.1 RFP and Contract Format Alternative - Example One** and section **A10.3.2 RFP and Contract Format Alternative - Example Two** for examples of other formats.



The Federal Acquisition Regulation (FAR) establishes a basic acquisition process for the Federal government. Because State agencies have their own acquisition policies, HB901 describes acquisitions and procurements based on the FAR as a common point of reference.

A basic format for State contracts is outlined in **Table 57**. A similar format is used to issue the RFP as is used to award a contract.

Table 57: Uniform Contract Format

Section	Title
Part I—The Schedule	
A	Solicitation/contract form
B	Supplies or services and prices/costs
C	Description/specifications/SOW
D	Packaging and marking
E	Inspection and acceptance
F	Deliveries or performance
G	Contract administration data
H	Special contract requirements
Part II—Contract Clauses	
I	Contract clauses
Part III—List of Documents, Exhibits, and Other Attachments	
J	List of attachments
Part IV—Representations and Instructions	
K	Representations, certifications, and other statements of offerors or respondents
L	Instructions, conditions, and notices to offerors or respondents
M	Evaluation factors for award

A10.2 Template Contents



In some cases, two examples are provided for a given topic. Once example is in narrative form and the other is form-driven. Select the format that is most appropriate for your needs.



A10.2.1 Part I—The Schedule

A10.2.1.1 Section A – Solicitation/contract form

Section A is typically the first section and first page of the RFP. It may be a standard form or cover letter that gives the RFP number, explains what type of solicitation it is (Sealed Bid or Negotiated Bid), who issued the solicitation, the address of the interested party receiving the solicitation, where proposals or bids are to be delivered, closing date and time, the contractor's name and address, and a brief description of the items or services to be performed. This will be signed by the contractor and returned with the proposal.

Example One Content:

1. INTRODUCTION

The purpose of this document is to provide interested parties with information to enable them to prepare and submit a proposal for the **<System Name> <Type of Service>** contract. The State, as represented by the **<State Agency Name>** intends to use the results of this solicitation to award a contract for **<System Name> <Type of Service>** employed to determine eligibility for programs under its purview within **<State Agency Name>** and the **<Other State agency, if joint or on behalf of>**.

Activities solicited through this RFP include, but are not limited to **<services to be provided>** of the **<System Name>** system and the **<services to be provided>** of the connection and integration of **<System Name>** with other supporting enterprise systems.

2. SUBMISSION OF PROPOSALS

Sealed Proposals will be received for implementation and integration of **<programs to be included>** eligibility and enrollment modules into the **<System Name>** for the State of **<State Name>**, **<State Agency Name>** by the **<State Name> <Department Name>**, **<Address>** until **<Date>**, **<#:## P.M (Time Zone)>** at which time they will be publicly opened.

Questions may be sent via E-MAIL to the Contract Manager at: **<firstname.lastname@statename.gov>**. The **<State Agency Name>** assumes no liability for assuring accurate/complete E-MAIL transmission/receipt.

The Contract Manager will respond to all substantive questions received. Only those answers issued in writing will be considered binding. Any information given to bidders concerning the RFP, including written questions and answers, will be furnished in writing to all bidders who have received a copy of the RFP from the Contract Manager. Questions and answers will be posted on the appropriate RFP page located at **<website>**.



All information received in response to this RFP, all information received in this RFP may be deemed public information and will be made available for public viewing and copying shortly after the time for receipt of proposals has passed,, unless the bidder has requested an exception and the state has approved the exception.

Sealed Proposals must include the following items:

Technical Proposal: **<Quantity (#)>** original and **<Quantity (#)> hard copies and/or** electronic copies must be submitted in an acceptable format.

Cost Proposal: **<Quantity> (#)** original and **<Quantity> (#)hard copies and/or** electronic copies must be submitted in an acceptable format.

3. KEY ACQUISITION EVENTS

Event Description	Date	Time
RFP Released	<MM/DD/YYYY>	<#:## P.M. (Time Zone)>
Initial Submission of Questions	<MM/DD/YYYY>	<#:## P.M. (Time Zone)>
Closing Date for Questions	<MM/DD/YYYY>	<#:## P.M. (Time Zone)>
Response to Questions Posted	<MM/DD/YYYY>	<#:## P.M. (Time Zone)>
Proposal Submission Due Date	<MM/DD/YYYY>	<#:## P.M. (Time Zone)>
Contract Award Date (Estimated)	<MM/DD/YYYY>	<N/A>
Design/Development/Implementation Work Begins Date (Estimated)	<MM/DD/YYYY>	<N/A>
Maintenance/Support Begins Date (Estimated)	<MM/DD/YYYY>	<N/A>

4. COST OF PREPARING PROPOSALS

All costs incurred for the preparation of this proposal and for other procurement related activities are solely the responsibility of the bidder. The **<State Name>** will not provide reimbursement for



such costs. The interested party is responsible for the cost of copies and for providing personnel to do the copying.

5. SUMMARY OF SERVICES

The **<State Name> <State Agency Name>** is currently implementing **<System Name>**, a modular, Web- and rules-based enterprise system that is scalable to allow the State to meet current and future State and Federal requirements. The State envisions expanding core functionality of **<System Name>** and allowing other State agencies to leverage the enterprise system. **<System Name>** was designed and developed using a Service-Oriented Architecture (SOA) approach. This will allow the State to integrate complex programs and systems while supporting the unique needs of each program. The eligibility system modules to be developed and implemented in **<System Name>** are for the **< list programs to be included>**.

6. PERIOD OF PERFORMANCE

The period of performance will include one base period of **<#> years**, with **<#>** option periods for **<#> year/months** each.

Performance Period	Start Date	End Date	Duration
Base Period	<MM/DD/YYYY>	<MM/DD/YYYY>	## months
Option Period One	<MM/DD/YYYY>	<MM/DD/YYYY>	## months
Option Period Two	<MM/DD/YYYY>	<MM/DD/YYYY>	## months
Option Period Three	<MM/DD/YYYY>	<MM/DD/YYYY>	## months

7. CONTRACT TYPE

The **<State Name>** plans to execute a Firm Fixed Price (FFP) contract, administered by the **<State Agency Name>** as a result of this RFP. All Contract awards must be approved by the U.S. Department of Agriculture, Food & Nutrition Service (FNS), **<by other federal partners (name)>**, and by **<state entities>** of the state of **<State Name>**.

The Provider shall not publish any statement, news release, or advertisement pertaining to this Contract without the prior written approval of the Contract Administrator. Should this Contract be funded, in whole or in part, by federal funds, then in compliance with the Stevens Amendment the following will be clearly stated when issuing statements, press releases, requests for proposals, bid

solicitations, and other documents: (1) the percentage of the total cost that was financed with federal moneys and (2) the dollar amount of federal funds.

Example Two Content:

This is an example form for an RFP and contract. Many States have their own forms with much the same information. This may be used in lieu of the Example One Content.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NUMBER	PAGE 1 OF
2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE	
7. FOR SOLICITATION INFORMATION CALL:			b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/ LOCAL TIME	
9. ISSUED BY		CODE	10. THIS ACQUISITION IS ☐ UNRESTRICTED OR ☐ SET ASIDE: _____ % FOR ☐ SMALL BUSINESS ☐ WOMEN-OWNED SMALL BUSINESS ☐ HUBZONE SMALL BUSINESS ☐ (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: _____ ☐ SERVICE-DISABLED ☐ EDWOSB _____ ☐ VETERAN-OWNED SMALL BUSINESS ☐ 8 (A) _____ SIZE STANDARD: _____		
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) ☐		
☐ SEE SCHEDULE		13b. RATING _____ 14. METHOD OF SOLICITATION ☐ RFQ ☐ IFB ☐ RFP			
15. DELIVER TO		CODE	16. ADMINISTERED BY		
CODE		CODE			
17a. CONTRACTOR/ OFFEROR		CODE	18a. PAYMENT WILL BE MADE BY		
FACILITY CODE		CODE			
TELEPHONE NO.		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 15a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM			
☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER					
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY	22. UNIT	23. UNIT PRICE
					24. AMOUNT
(Use Reverse and/or Attach Additional Sheets as Necessary)					
25. ACCOUNTING AND APPROPRIATION DATA			26. TOTAL AWARD AMOUNT (For Govt. Use Only)		
☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED ☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED			☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: _____		
☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED					
30a. SIGNATURE OF OFFEROR/CONTRACTOR			31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)		
30b. NAME AND TITLE OF SIGNER (Type or print)		30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (Type or print)		31c. DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION
 PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
 Prescribed by GSA - FAR (48 CFR) 53.212

**A10.2.1.2 Section B – Supplies or services and prices/costs**

Section B is a listing of the deliverables to be provided. There is a brief description of the supplies or services, the quantities, and costs of the items. Deliverables can be hardware, software, data, labor, or a combination of any or all of these items. At the solicitation stage, Section B will have blanks for the cost; the contractors will fill in their proposed costs and profits when sending their offers to the State. A provision for labor category rates should also be included for tasks which might be covered by Time and Materials later.

For an RFP, this is a blank form or table illustrating the State agency's desired format. The offerors should be instructed to provide pricing as a separate volume from the technical approach volume when submitting proposals. When a contract is awarded, this section is usually incorporated into the contract document.

Example Content:**1. EXAMPLE ONE - ITEMIZED DELIVERABLES BY CONTRACT LINE ITEM NUMBER (CLIN)**

Provide all costs for **<services to be provided>** for the **<System Name>** system and its environments, if applicable. The Price must be divided by each contract year (total of **<Quantity (#)>** years).

Itemized Deliverable Price/Costs		
Base Period (# years)	CLIN001	\$
(<MM/DD/YYYY> to <MM/DD/YYYY>)		
Option Period One (# Year/Months)	CLIN002	\$
(<MM/DD/YYYY> to <MM/DD/YYYY>)		
Option Period Two (# Year/Months)	CLIN003	\$
(<MM/DD/YYYY> to <MM/DD/YYYY>)		
Option Period Three (#Year/Months)	CLIN004	\$
(<MM/DD/YYYY> to <MM/DD/YYYY>)		
Travel – (Cost Reimbursable)	CLIN005	\$
TOTAL ALL INCLUSIVE PRICE/COST (Sum of all CLINs)		\$



2. EXAMPLE TWO - ITEMIZED DELIVERABLES

Deliverable	CLIN	Price
<System Name> Design	CLIN001	\$
<System Name> Development	CLIN002	\$
<System Name> Demonstration	CLIN003	\$
<System Name> Documentation	CLIN004	\$
<System Name> User Acceptance Testing	CLIN005	\$
<System Name> User Training	CLIN006	\$
<System Name> Pilot	CLIN007	\$
<System Name> Deployment	CLIN008	\$
<System Name> Maintenance & Upgrade Support	CLIN009	\$
<System Name> Enhancements	CLIN010	
<System Name> Maintenance & Operations Support	CLIN011	
Travel Expenses	CLIN012	\$
TOTAL of All CLINS		\$



The State agency may include a not to exceed (NTE) value for items such as travel. Occasionally, some State agencies include an NTE for the contract value as an estimate of expected costs to which offerors' bids should be within range.



A10.2.1.3 Section C – Description/specifications/SOW

Section C outlines to the contractor the actual tasks or outcomes to be performed. Depending on the acquisition, this section may be a Performance Work Statement (PWS), or Statement of Work (SOW). If the acquisition requires a SOW or a PWS, the document may contain a Work Breakdown Structure (WBS). See chapter 4.0 Procurement for explanations of the differences between, PWS, and SOW.

Example Content One – PWS ATTACHMENT:

1. PWS ATTACHMENT

The Contractor shall perform the work specified in the Performance Work Statement (PWS) or other Attachments and Exhibits in Section J of this contract. The Contractor shall provide all necessary materials, labor, equipment and facilities incidental to the performance of this requirement.

2. FUNCTIONAL REQUIREMENTS

The **<System Name>** shall be designed, developed, and implemented in accordance with the functional and technical requirements included as Attachments and Exhibits in Section J of this contract. The Contractor shall provide all necessary materials, labor, equipment and facilities incidental to the performance of this requirement.

Example Content Two – PWS STATEMENTS:

1. INTRODUCTION AND BACKGROUND

The **<State Name>**'s eligibility determinations for **<State Agency Name>** programs are processed by the **<describe information about existing system(s) to be included: system type, originating transfer State/System, year implemented, programs supported, reason for planned replacement/upgrade, system limitations/deficiencies, etc.>**

<State Name> plans to replace **<existing systems>** in an effort to modernize and streamline the eligibility processes for **<State Agency Name>** programs and leverage the modular, Web- and rules-based enterprise system that is scalable. The **<System Name>** was designed and developed using a Service-Oriented Architecture (SOA).

The State's vision is to provide seamless coordination of benefits, and increased efficiency in eligibility and enrollment, for the benefit specialists and clients. **<State Agency Name>** would like to leverage the functionality such as that provided in **<System Name>** as it will provide an enterprise system with a flexible SOA to allow **<State Agency Name>** to develop and define specific business needs, functionality, and modules for **<State agency>**. The **<State>** envisions



that replacement applications will be built on a modernized, flexible platform that will be scalable to easily integrate with **<System Name>** as well as other State and federal programs.

2. PURPOSE AND INTENT

The purpose of this Request for Proposal (RFP) is to solicit competitive proposals to implement and integrate the eligibility modules listed below into **<System Name>** and to meet **<State Agency Name>** needs and expectations as described within this RFP. A Contractor will be selected for the **<services to be provided>** of the eligibility applications. These applications include the following programs:

- **<List programs to be included in bullet list>**

The primary focus of the procurement is to select a Contractor with the appropriate program knowledge or experience with comparable programs and requirements, technology-specific expertise, enterprise implementation experience, and proven success to develop programmatic business rules and functionality specific or comparable to each program's eligibility and enrollment processes. There may be advantages to leverage Commercial Off The Shelf (COTS) products for one or more of the programs. These applications will be implemented and integrated into **<System Name>** and will be built onto the existing **<System Name>** enterprise. Prior to the system's going into production, **<the full range of testing as identified in section 4>** will be required in connection with the **<System Name>** vendor and the customer.

<State Agency Name> is migrating away from a legacy system to a web-based system leveraging enterprise services and an SOA. The SOA is supported by a Client Web Portal and a Worker Portal. The new eligibility applications should leverage the technical components of **<System Name>** and share a large number of functional commonalities for the program eligibility systems. Leveraging development work completed in **<System Name>** will reduce the amount of time needed to develop the **<State Agency Name>** eligibility applications because much of the underlying architecture is already in place.

The following objectives related to **<System Name>** can be leveraged by **<State Agency Name>**:

- Implement a new system to better support the Agency and its clients' needs
- Secure a flexible system with an open architecture that other agencies and programs can connect to for their eligibility needs in the future
- Comply with new federal requirements for processing and security
- Implement a new centralized service delivery model

The Agency would like the Contractor to design, develop, and implement functionality that leverages the enterprise system and includes the following System and Functional Scope:



- System scope:
 - Service-Oriented Architecture (SOA)
 - Application hardware and software
 - Benefit Management System (worker portal)
 - Public-facing Client Web Portal, mobile enabled
 - Workflow Management Tool
 - Reporting Engine
 - Electronic Document Management System (EDMS)
 - Business Rules Engine
 - System Interfaces and Interoperability
 - Database Management Software
 - Business Continuity and Disaster Recovery
- Functional scope:
 - Program screening
 - Application/Intake
 - Eligibility determination
 - Case management
 - Workflow management
 - Document management
 - Policy management
 - Program and management reporting
 - Quality Assurance/Quality Control
 - Client correspondence and notifications

3. PROGRAM STATISTICS

Table <#.#> includes a brief summary of each assistance program as well as basic program statistics. Policies, procedures and supplementary information can be found in the online manuals located at: <www.website.com>.



Table <#.#>: Program and Policy Summary		
PROGRAM	DESCRIPTION	PROGRAM STATISTICS
Supplemental Nutrition Assistance Program (SNAP)	Provides crucial support to needy households and to those moving from welfare to work. SNAP benefits are distributed electronically through the <State Name> Card. SNAP supports better nutrition for low-income households.	Highest monthly number of eligible recipients and households for FY <Year> • Recipients <###,###> • Households <###,###>
Temporary Assistance for Needy Families (TANF)	A time-limited pay-after-performance program, the Personal Opportunities with Employment Responsibilities assures that families with a dependent child(ren) are working to become self-sufficient through employment, child support and other resources. The program is funded with state and federal dollars through the Temporary Assistance for Needy Families (TANF) block grant.	Average monthly number of eligible recipients and households for FY <Year>: • Recipients <###> • Households <###> Highest monthly number of eligible recipient and households for FY <Year>: • Recipients <###> • Households <###>



Table <#.#>: Program and Policy Summary

PROGRAM	DESCRIPTION	PROGRAM STATISTICS
Child Care Subsidy	A benefit provided under the Early Childhood Division based on collaboratively delivering services in the most effective manner to: Ensure that children are cared for in safe, developmentally appropriate child care environments; Ensure that youth in out-of-home placement facilities are cared for in safe and healthy environments; Ensure that low income families receive assistance to pay for the cost of child care while they are working to achieve self-sufficiency; Ensure that child care providers receive training and supports necessary to improve the quality of their early care and education programs.	Highest monthly number of eligible recipients and households for FY <Year>: • Recipients <#,> • Households <#,> Monthly payments processed for FY <Year>: • <\$#,>



Table <#.#>: Program and Policy Summary		
PROGRAM	DESCRIPTION	PROGRAM STATISTICS
Title IV-E (Foster Care program)	The Foster Care Program helps States to provide safe and stable out-of-home care for children until the children are safely returned home, placed permanently with adoptive families or placed in other planned arrangements for permanency. The Adoption Assistance Program provides funds to States to facilitate the timely placement of children whose special needs or circumstances would otherwise make it difficult to place with adoptive families. The Foster Care and Adoption programs are authorized under title IV-E of the Social Security Act.	Average monthly number of placements for FY <Year>: - Foster placement <###> - Adoptions <###> Highest monthly number of placements for FY <####>: - Foster placement <###> - Adoptions <####> https://docs.google.com/a/wyo.gov/file/d/0B6DSpyyE-UESdkZ0dEFLVnJ2QTg/edit

4. FULL SYSTEM TESTING

This section should describe the expectations of full end to end internal testing, User Acceptance Testing, full regression testing and live pilot testing. It is important to convey this element to the prospective bidder, as testing has inherent go/no-go points in the system development lifecycle (SDLC) when the State and Federal staff must evaluate whether a system is meeting expectations.

During the testing phase, the contractor is responsible for the conduct of unit, system, integration, and fixes to defects found in user acceptance testing to ensure that all of the enterprise architecture, shared fiscal services, and <System Name> system requirements are satisfied. The contractor will test the software and hardware of the architecture and application to evaluate eligibility determination accuracy and the systems' compliance with defined requirements. The contractor will perform unit and integrated system testing. The contractor will support the Department in conducting user acceptance testing. The contractor will use State's testing environment for integration and UAT.

Although testing is described as a separate phase for this project, the contractor should coordinate the establishment of testing strategies during the construction phase, to ensure that the flow of testing from unit testing to acceptance testing is cohesive. The construction phase will include unit



testing to verify that each basic component of the system architecture is constructed correctly in accordance with the design specifications.

Bidders must include in their approach a detailed description for how the contractor will conduct conversion testing as well as their approach to supporting the User Acceptance Testing and Pilot. Include a discussion of project tracking tools and issue tracking methods. A description of disaster recovery and contingency planning should be included in the acceptance test activity. The plan includes, but is not limited to these items:

- Introduction – overview, purpose, objectives
- Scope/conversion test – inclusions, exclusions
- Approach for conversion test
- Test data
- Data validation, both manual and automated
- Testing process
- Test phases and cycles
- Conversion test entrance/exit criteria
- Conversion test schedule
- Resources
 - People
 - Hardware
 - Software
- Roles and responsibilities
- Issue tracking management
- Communication
- Prioritization activities
- Severity levels
- Tools
- Reporting
- Issues/risks/assumptions
- Signoff sheet
- Any appropriate appendices

5. TRAINING

The Contractor must train designated Agency staff and necessary Contractor staff in order to achieve a successful implementation of <System Name> applications. Users must be proficient in



using **<System Name>** applications in order to ensure effective and efficient business operations and service delivery in **<State Name>**.

The Contractor is responsible for developing and implementing a training program. The Contractor will be expected to travel throughout the State to complete the training initiative. The following locations will be designated as training sites and may change at the discretion of the Agency: **<Training Location One>**, **<Training Location Two>**, **<Training Location Three>**, **<Training Location Four>**, **<Training Location Five>**. The goal is to equip the State-designated trainers to be able to successfully deliver the information necessary for Agency staff to effectively use **<System Name>** applications so they can efficiently and accurately service Agency clients. The training program needs to be based on the principles of adult learning and utilize a model of coaching designed to elicit high performance. The training program should reflect two key elements of adult learning: 1) adult learners integrate new knowledge, skills and behaviors when it is conducted within the framework of life experiences; and 2) motivation for learning is enhanced by linking change with increased personal success and fulfillment.

The Contractor's proposed training program must utilize a variety of delivery methods to best meet the training objectives. Examples include computer-based training, classroom lectures, written material, and demonstrations. The Agency will provide details to the Contractor on program and policy training as appropriate.

In addition to the general responsibilities the Agency anticipates that the Contractor will provide training to appropriate Agency staff in order to conduct User Acceptance Testing and Pilot Testing and when new application features or updates have presented a significant change. The Contractor must provide training for the appropriate State staff at least two (2) weeks prior to the release of the functionality.

6. MAINTENANCE AND UPGRADE SUPPORT

The contractor will continue to maintain the eligibility systems and enterprise architecture for **<Time Period>** (e.g., *periods of performance, number of years*). The contractor will be responsible for maintaining and upgrading the software as part of the maintenance responsibilities, and for providing operational support to be performed during the contract term. The State will operate the hardware, but the contractor remains responsible for the software, which is the platform for eligibility determination. The contractor is responsible for ensuring that eligibility determination functionality remains accurate throughout the maintenance period. Operational support involves all processes necessary to meet the requirements outlined throughout this RFP. The contractor must perform all operations maintenance and support as a routine activity during this phase. Maintenance and support as a routine activity will be provided at no additional cost to the Department. The contractor will charge for approved modifications to **<System Name>** based on a contractually agreed approach and amount.



A10.2.1.4 Section D – Packaging and marking

If there are any packaging and marking requirements, they are outlined in Section D. This section describes delivery information, such as where products will be sent, delivery destinations, how packaging will be accomplished and what markings must be included for deliverables. It may also define who is responsible for shipping fees, if applicable.

Example Content:

Technical data items shall be preserved, packaged, packed, and marked in accordance with the best commercial practices to meet the packaging requirements of the carrier and insure safe delivery at destination.

All Contractor documentation that is proprietary and protected by copyright law will be marked in accordance with the following standards:

- 1) For documents created for this project in accordance with this RFP, “Company Proprietary” will be marked at the top and bottom of the front cover of a publication or the cover page of other documentation. The same will be marked at the top and bottom of the back cover of a publication or the cover page of other documentation.
- 2) For documents created for this project in accordance with this RFP, each page will be marked with the title of the document in the header.
- 3) For documents existing prior to the start of the project in the RFP, the bidder will provide a list of all “Company Proprietary” documents, their publication dates, and copyright years.

A10.2.1.5 Section E – Inspection and acceptance

Requirements for inspection, acceptance, quality assurance and reliability are explained in Section E. This often includes an inspection schedule, where inspections will occur, and acceptance criteria for each contract line item number (CLIN). Testing is part of inspection and would be appropriate for this section. Inspection can be either at the origin or destination; this should be specified in the contract.

Example Content:

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	<Destination>	State	<Destination>	State
0002	<Destination>	State	<Destination>	State
0003	<Destination>	State	<Destination>	State



CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0004	<Destination>	State	<Destination>	State
0005	<Destination>	State	<Destination>	State

A10.2.1.6 Section F – Deliveries or performance

Section F specifies the requirements for place and method of delivery or performance. Delivery schedules for hardware and services may be described in terms of calendar dates or in specified periods of time from contract award date. The place of performance may also be included here (e.g., contractor facilities, State on-site, etc.).

Note: The following is Example Content. States should follow their own procurement regulations and IT requirements for the systems' performance expectations and data.

Performance Standard	Benchmark/ Threshold Measurement and Frequency	Liquidated Damages / Calculations
1. System Availability (Uptime): <##> hours a day, <#> days a week, <###> days a year, except for scheduled downtime, measured per month.	• ## hour threshold • <##.#>% • <Recurring interval of time>	1st outage- <##.#>% of monthly bill. For each additional hour segment an additional <##.#>% will be added. 2nd outage- <##.#>% of monthly bill. For each additional hour segment an additional <##.#>% will be added. An additional <##.#>% for each subsequent outage >2 will be added.
1. Client Web Portal Availability (Uptime): <##> hours a day, <#> days a week, <###> days a year, except for scheduled downtime.	• <##.#>% • <Recurring interval of time>	\$<#,<###> for each whole % point below standard, except for scheduled down time.
2. Support Communication Availability: <##> hours a day, <#> days a week, <###> days a year, except for scheduled downtime.	• <##.#>% • <Recurring interval of time>	\$<#,<###> for each whole % point below the standard, except for scheduled down time.
3. Administrative System Availability (Uptime): <##> hours a day, <#> days a week, <###> days a year, except for scheduled downtime.	• <##.#>% • <Recurring interval of time>	\$<#,<###> for each whole % point below standard, except for scheduled down time.



Performance Standard	Benchmark/ Threshold Measurement and Frequency	Liquidated Damages / Calculations
4. Data File Processing: All data file records, including but not limited to Benefit Files and Batch Update Files received via SFTP or any other means.	• <##.#>% of files are processed within <##> hours of receipt • <Recurring interval of time>	\$<#,<###> for each whole % point below standard.
5. Data File Transmission: Data files are sent according to the daily/ monthly schedule as defined in Section <#.#> of the RFP.	• <##.#>% of data files are sent within <##> day(s) of schedule defined in this RFP. • <Recurring interval of time>	\$<#,<###> for each whole % point below standard.
6. Data File Transmission Accuracy: Data files are accurately formatted and data is accurate.	• <##.#>% of data files are accurate. • <Recurring interval of time>	\$<#,<###> for each whole % point below standard.
7. Continuation of Business Testing: Test conducted annually on mutually agreed upon date.	Continuation of Business testing is conducted on annual scheduled date.	\$<#,<###> per month delayed from scheduled date.
8. Continuation of Business Reporting: Complete reporting as described in this RFP.	Received within <##> days of completion of test.	\$<#,<###> per month if delayed beyond the <##> days of completion.
9. Call Center Wait Period: Cardholder or retailer calls answered by live operator.	• <##.#>% answered by live operator within <##> minutes. • <Recurring interval of time>	\$<#,<###> per month.
10. Incident/Problem Management Response Time: The Contractor is to document and submit an impact statement to incidents/problems reported by the State or Contractor.	Within <##> hours for State and Contractor detected/reported incidents/problems.	Reports of events, incidents or problems identified by the State must also adhere to the following standards and must be addressed by the Contractor with the same expectations specified in Section <#.#> of the RFP. In the event the Contractor fails to comply with the specified requirements, the State reserves the right to withhold <##.#>% of the most current monthly invoice per delayed response.



Performance Standard	Benchmark/ Threshold Measurement and Frequency	Liquidated Damages / Calculations
Other Performance Standards as appropriate and as applicable.	Benchmark/Threshold as appropriate and as applicable.	Calculations and statistics as appropriate and as applicable.

A10.2.1.7 Section G – Contract administration data

Section G relays accounting, appropriation data, and funding source data. It includes any required contract administration information or instructions other than those on the solicitation form. It also includes a statement that the offeror should include the payment address in the proposal if it is different from that shown for the offeror.

Example Content:

1. PAYMENT SCHEDULE

Bidders may suggest a payment schedule which mirrors specific deliverables in meeting the requirements of this RFP. Payment schedules based on time and materials only will not be acceptable nor will a flat per-hour rate. Payment will be made at the completion and acceptances of the individual deliverables, as defined in the Scope of Work.

2. PAYMENT NEGOTIATIONS

The **<State Agency Name>** will negotiate payment terms based upon a schedule to be determined by the Bidder and the **<State Agency Name>**. Payments of invoices will be based upon the Bidder successfully completing the deliverables within the stated deadlines and upon the written acceptance of the deliverables and/or services by the **<State Agency Name>**.

3. STATUS REPORTING

The Contractor is required to regularly submit status reports outlining the project's progress and compliance with milestones and delivery dates. Each report will be verified by a **<State Agency Name>** representative to ensure that all contract requirements have been met to date.

Note: Frequency of status report submissions are established by the State or negotiated by the State and Contractor.

A10.2.1.8 Section H – Special contract requirements

Section H conveys any unique or special contract requirements such as options, warranties, State-furnished equipment and incentives. These special clauses must be clear and concise. Because these are not standard



clauses, the information is written in full text and not incorporated into the RFP by reference. Other elements may include key personnel provisions, option terms, economic price adjustment provisions, multiyear provisions, limitations on State obligations, and payment of fees withheld as a performance incentive.

Involving key stakeholders, such as the agency's legal and procurement staffs, as well as whomever will be reviewing and evaluating the proposal will help in constructing this section. The Contract Clauses are vital to a solid RFP and resulting contract. Offerors will be bound by clauses in this section.

Example Content:

1. CONTRACTUAL TERMS & CONDITIONS

The terms and conditions herein constitute the entire contract and understanding of the parties and shall supersede all other communications, negotiations, arrangements and agreements, either oral or written, with respect to the subject matter hereof. All proposal documentation including, but not limited to, red line contract terms and conditions, red line statements of work and/or ground rules and assumptions are hereby void and carry no force or affect as it pertains to the interpretation or operation of the language of the instant contract nor should such language be used to provide meaning to any of the terms or conditions contained herein.

No modification or change of any provision in the contract shall be made, or be construed to have been made, unless such modification is mutually agreed to in writing by the provider and the State of **<State Name>**. The contract modification will be incorporated as a written amendment to the contract. Memoranda of understanding and correspondence shall not be construed as amendments to the contract.

The requirements appearing in this RFP shall become a part of the terms and conditions of the contract. Any deviations from the RFP requirements must have been specifically defined by the provider in its proposal and if accepted by the State of **<State Name>**, must become part of the contract, but such deviations must not have been in conflict with the basic nature of this offer.

2. CONTRACTOR DEFAULT

Unless otherwise provided in the Contract, the State shall provide the Vendor written notice of default, and the Vendor must cure the default within thirty (30) days, unless otherwise indicated within by the State ("Cure Period"). If the Vendor fails to cure the default within the Cure Period, the State may terminate the Contract, at its sole discretion, and pursue its remedies at law or in equity or both.



3. CONTRACT TERMINATION

Upon termination of the Contract, the State, in addition to any other rights provided in the Contract, may require the Vendor to deliver to the State any property including, without limitation, Software and Written Deliverables for such part of this Contract as has been terminated.

4. FORCE MAJEURE

Neither the contractor nor the State shall be responsible for delays or failures in performance resulting from events beyond the control of such party and without fault or negligence of such party. Such events shall include, but not be limited to, acts of God, strikes, block outs, riots, and acts of War, epidemics, acts of State, fire, power failures, nuclear accidents, earthquakes, and unusually severe weather.

5. PERFORMANCE BONDS

Excessive terms and conditions such as large performance bonds, unlimited liability and large holdbacks on payments may limit competition. Performance bonds in particular are costly to the bidder and can increase the cost of the bid price and project. These types of terms and conditions can deter potential bidders and inhibit competition and are strongly discouraged.

The Vendor is required to include the price of a performance bond or irrevocable bank letter of credit with the RFP proposal. If required, the cost of the bond or letter of credit must be shown as a separate line item in the Cost Information Submission. The performance bond or letter of credit must be procured at the Vendor's expense upon execution of the contract and may be invoiced to **<Organization Name>** after contract initiation only if itemized in the Cost Information Submission and in the executed contract. The final decision as to the requirement for a Performance Bond or Irrevocable Bank Letter of Credit will be made upon contract award and is at the State's sole discretion.

6. WARRANTIES

The warranty period, during which the contractor is responsible for all fixes needed to ensure that the systems and architecture operate according to **<State Agency Name>** specifications, will begin at the time that the **<State Agency Name>** has accepted the **<System Name>**. During the warranty period, the contractor will correct, at its expense, any defects reported by the **<State Agency Name>** which do not meet the agreed-upon design specifications. No additional charges for computer resources needed to maintain or correct the system shall be authorized. Upon completion of the warranty period, the contractor will be responsible for the maintenance and support of the **<System Name>** throughout the remaining contract operations and maintenance period. Any enhancements undertaken may need to include a warranty period as well. A State agency's draft of a service level



agreement (SLA) should be part of the RFP to set a baseline for negotiations. The final SLA will be part of the final contract and will address the technical support expectations for the contractor.

7. AUDITS

Audits may be performed by a number of State and Federal agencies or authorized agents. The contractor must fully cooperate with the audit process. An audit may include, but is not limited to, the following capabilities and applies to the applications and architecture:

- Storing, retrieving, and executing programs, whether such programs are part of the contractor's production system, or generated by contractor staff.
- Sampling and reconciling subsystem files to ensure accurate and timely maintenance.
- Demonstrating that services and/or benefits were provided for eligible clients.
- Reviewing the contractor's organization, policies, procedures, practices, effectiveness of control, operating efficiency, facility and software security, and back-up procedures.
- Reviewing the contractor's compliance with contract terms, system specifications, State or Federal regulations, administrative directives, and program documentation.
- Reviewing any phase or aspect of the project for any purpose related to the system.
- Responding to requests for data or information.
- Having access to files, documentation, and contractor personnel.
- Assisting Department staff in responding to federal inquiries. This level of support must also be provided to all other State audit agencies or their designees.

8. PERSONNEL REQUIREMENTS

Key Personnel are those positions that are considered to be critical and essential to the effective management, performance, and success of the project. It is essential that key positions are filled with qualified, experienced staff committed to the success of the **<System Name>** Project. It is essential that there is stability of the staff chosen to fill the key positions. The Key Personnel proposed by the Offeror will be taken into consideration during the proposal evaluation. Substitutions of personnel subsequent to contract award must be with staff of equal or greater knowledge, skills, abilities, and experience.

The Contractor must provide a sufficient mix of project staff with qualifications and experience to fulfill the requirements of this RFP. While the State has given the Offeror latitude on the structuring of resources for these interrelated efforts, the work plan submitted as required by this RFP may not show an over-allocation for resources that are assigned to multiple roles. Key Personnel must be physically located at **<Location Name>** *(if appropriate)*; other personnel may be located off-site.



A10.2.2 Part II—Contract Clauses

A10.2.2.1 Section I – Contract clauses

Section I includes standard clauses. Most of the clauses are incorporated by reference. Clause selection varies by the nature of the requirement (supplies, services) and the type of contract (Fixed Priced types or Cost Reimbursement types). Most are required by public law and have mandatory requirements to be performed by the contractor. Non-compliance can have serious legal ramifications on the contractor and the State.

Example Content:

9. COPYRIGHTS AND LICENSING

The State and FNS reserve royalty-free, nonexclusive and irrevocable license to reproduce, publish, or otherwise use and authorize others to use for Federal government purposes the copyright in any software and associated documentation developed under the resulting contract (2 CFR 200.315 Intangible property) which includes the following:

- (a) The copyright in any work developed under a grant, subgrant, or contract under a grant or subgrant; and
- (b) Any rights of copyright to which a grantee, sub-grantee or a contractor purchases ownership with grant support

The Provider certifies that all services, equipment, software, supplies, and any other products provided under this Agreement do not and will not infringe upon or violate any patent, copyright, trade secret or any other proprietary right of any third party. In the event of any claim by a third party against the State, the State shall promptly notify the Provider and the Provider, at its expense shall defend, indemnify and hold harmless the State against any loss, cost, expense, or liability arising out of such claim, including reasonable attorney fees.

The Provider may not publish or copyright any data without the prior approval of the department. The State and Federal government, if applicable shall have the right to publish, duplicate, use and disclose all such data in any manner, and for any purpose whatsoever, and may authorize others to do so.

The Department shall own all custom software. Such custom software shall include, but not be limited to, all source, object and executable code, operating system instructions for execution, data files, user and operational/administrative documentation, and all associated administrative, maintenance, and test software that are relevant to this Agreement.

A fundamental obligation of the Provider is the delivery to the Department of all ownership rights to the complete system, free of any claim or retention of rights thereto by the Provider. The Provider



acknowledges that this system shall henceforth remain the sole and exclusive property of the Department, and the Provider shall not use or describe such software and materials without the written permission of the Department. This obligation to transfer all ownership rights to the Department on the part of the Provider is not subject to any limitation in any respect.

*See appendix A16 Ownership Rights **for other examples of copyright and licensing clauses.***

1. FNS Required Federal Provisions (See 7 CFR 277.14 – Procurement Standards Excerpts)
2. Required Federal Procurement Clauses

*See appendix A11 **for related** Federal Procurement Clauses.*

Equal Employment Opportunity Act:

Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of federally assisted construction contract in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, “Equal Employment Opportunity” (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and implementing regulations at 41 CFR part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.” (2 CFR 200, Subpart F, Appendix II)

The EEO clause must be included or the State must have its own EEO similar clause.

Clean Air and Federal Water Pollution Control Act:

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended. Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). (2 CFR 200, Subpart F, Appendix II)

The Copeland “Anti-Kickback” Act, 40 USC §276c and 18 USC §874:

The “Anti-Kickback” section of the Act precludes a contractor or subcontractor from inducing an employee to give up any part of the compensation to which he or she is entitled under his or her contract of employment. The Act also requires the contractor and subcontractor to submit a weekly statement of the wages paid to each employee performing on covered work during the preceding payroll period.



Anti-Lobbying Act:

This Act prohibits the recipients of federal contracts, grants, and loans from using appropriated funds for lobbying the Executive or Legislative branches of the Federal government in connection with a specific contract, grant, or loan. As required by Section 1352, Title 31 of the U.S. Code and implemented at 2 CFR 200, Subpart F, Appendix II, for persons entering into a grant or cooperative agreement over \$100,000, as defined at 31 U.S.C. 1352, the applicant certifies that:

- a. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the making of any federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement;
- b. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form – LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions;
- c. The undersigned shall require that the language of this certification be include in the award documents for all sub-awards at all tiers (including sub-grants, contracts under grants and cooperative agreements, and subcontracts) and that all sub-recipients shall certify and disclose accordingly.

Americans with Disabilities Act:

This Act (28 CFR Part 35, Title II, Subtitle A) prohibits discrimination on the basis of disability in all services, programs, and activities provided to the public and State and local governments, except public transportation services.

Debarment, suspension, and other responsibility matters:

Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., pg. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. (2 CFR 200, Subpart F, Appendix II)



Drug Free Workplace Statement:

The Federal government implemented 41 U.S. Code § 8103, drug-free workplace requirements for federal grant recipients, in an attempt to address the problems of drug abuse on the job. It is a fact that employees who use drugs have less productivity, a lower quality of work, and a higher absenteeism and are more likely to misappropriate funds or services. From this perspective, the drug abuser may endanger other employees, the public at large, or themselves. Damage to property, whether owned by this entity or not, could result from drug abuse on the job. All these actions might undermine public confidence in the services this entity provides. Therefore, in order to remain a responsible source for government contracts, the following guidelines have been adopted:

- a. The unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in the work place.
- b. Violators may be terminated or requested to seek counseling from an approved rehabilitation service.
- c. Employees must notify their employer of any conviction of a criminal drug statute no later than five days after such conviction.
- d. Contractors of federal agencies are required to certify that they will provide drug-free workplaces for their employees.

Transactions subject to the suspension/debarment rules (covered transactions) include grants, subgrants, cooperative agreements, and prime contracts under such awards. Subcontracts are not included.

States to include in the RFP and Contract a statement of certification by the vendor, such as "By signing this contract, the vendor certifies it is not suspended or debarred as specified by these rules."

Royalty-Free Rights to Use Software or Documentation Developed

2 CFR 200.315 Intangible property.

(a) Title to intangible property (see §200.59 Intangible property) acquired under a federal award vests upon acquisition in the non-Federal entity. The non-Federal entity must use that property for the originally-authorized purpose and must not encumber the property without approval of the Federal awarding agency. When no longer needed for the originally authorized purpose, disposition of the intangible property must occur in accordance with the provisions in §200.313 Equipment paragraph (e).

(b) The non-Federal entity may copyright any work that is subject to copyright and was developed, or for which ownership was acquired, under a federal award. The Federal awarding agency reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for federal purposes and to authorize others to do so.



(c) The non-Federal entity is subject to applicable regulations governing patents and inventions, including government wide regulations issued by the Department of Commerce at 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Awards, Contracts and Cooperative Agreements.”

(d) The Federal government has the right to:

- (1) Obtain, reproduce, publish, or otherwise use the data produced under a federal award; and
- (2) Authorize others to receive, reproduce, publish, or otherwise use such data for federal purposes.

A10.2.3 Part III—List of Documents, Exhibits, and Other Attachments

A10.2.3.1 Section J – List of attachments

Section J lists all the documents that are included in the RFP but are attached as “stand-alone” documents. The contracting officer lists the title, date, and number of pages for each attached document, exhibit, and other attachment. Cross references to material in the other contractual sections may be inserted as appropriate. Examples include the System Specification, exhibits, technical or engineering data, SOW or PWS, training systems requirements document, system interface diagrams, Quality Assurance Surveillance Plan (QASP), and applicable regulations and policies.

Example Content:

Attachment One – Cost Estimate Worksheets

Attachment Two – Proposed Staffing Matrix Worksheet

Attachment Three – **<System Name>** Technical Specifications

Attachment Four – **<System Name>** Functional Requirements

Attachment Five – **<System Name>** On-Line Availability Time

Attachment Six – **<System Name>** Transaction Response Time

Additional Attachments as applicable and appropriate



A10.2.4 Part IV—Representations and Instructions

A10.2.4.1 Section K – Representations, certifications, and other statements of offerors or respondents

Section K provides representations, certifications and other statements that must be completed by the offeror (e.g., small business size, equal employment opportunity compliance, OSHA compliance). These documents are completed and submitted with the offeror's proposal.

Example Content:

CONTRACTOR CERTIFICATIONS

By submitting a proposal in response to this RFP, the offeror certifies to the best of its knowledge and belief that it, its principals, and proposed subcontractors are not presently debarred, suspended, proposed for disbarment, declared ineligible, or voluntarily excluded from covered transactions.

Have not within a **<# time period>** preceding the submission of the proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.

Are not presently under investigation for, indicted for, or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in **Paragraph <#.#.#>** above.

The Offeror must provide a statement that assures the State that the Offeror is not suspended or debarred from entering into contracts that are federally funded.

A10.2.4.2 Section L – Instructions, conditions, and notices to offerors or respondents

Section L provides guidance to the offerors or respondents in preparing proposals or responses to requests for information. This section includes submission guidance for preparing proposals and responses. This includes the specific proposal format, organization and arrangement of proposals, and general instructions (e.g., number of copies, number of pages, document formatting such as font size and spacing, etc.). The contractor should not be required to provide data that will not be evaluated, nor should the State have source selection evaluation criteria they have not asked the contractor to address in the proposal.



Example Content:

1. PROPOSAL SUBMISSION INSTRUCTIONS

- A. Bidders must submit Proposals in strict accordance with the requirements set forth in this section. Bidders must submit an original and **<Quantity (#)>** copies of all materials required for acceptance. Proposals **MUST** be received in the prescribed formats and must be date and time stamped by the designated area on or before **<#:## P.M. (Time Zone)>** on **<MM/DD/YYYY>**.
- B. Proposals that are received after the due date and time will be rejected.
- C. Any proposals that bear a date/time receipt later than the posted due date and time will be subsequently rejected by the Procurement Manager as part of the process by which all proposals are reviewed for preliminary acceptance. Proposals will be rejected due to lateness of submission as determined by the date and time recorded by the State at the point of receipt/acceptance. Should this occur, the Proposer will be notified of the rejection within three working days of the proposal due date. Under this situation, all Proposals will be returned to the vendor unopened.
- D. Faxed or emailed proposals **<will/will not>** be accepted. Proposals submitted in this manner will be rejected regardless of the date/time received. To ensure confidentiality of the document, all materials must be packaged and sealed and show the following information on the outside of the package:
 - Vendor's name and address
 - <System Name>** Contractor Support Proposal
 - RFP Number
 - Solicitation due date
- E. Proposals may be submitted using any of the methods that follow:
 - 1) Submitting via United States Postal Service (USPS): If the vendor selects this method, all materials are delivered by the USPS and are date- and time-stamped upon receipt. This serves as the official receipt date and time used to determine acceptance or rejection of the materials. Vendor to use this address for submission via USPS:
 - <State Agency Name>**
 - Attn: **<FirstName LastName>**, Procurement Manager
 - <Street Address>**
 - <City Name, State Postal Code>**
 - 2) Submitting via common carrier (e.g., UPS, FedEx, etc.): If the vendor selects this method, all materials are delivered by the common carrier to either the **<State Agency Name>** mail room or to the **<State Agency Name>** main reception desk at **<Address>**. All materials are date- and time-stamped upon receipt, which serves as the official receipt date and time used to determine acceptance or rejection of the materials. Vendor is to use this address for submission via common carrier:



<State Agency Name>

Attn: <FirstName LastName>, Procurement Manager

<Street Address>

<City Name, State Postal Code>

- 3) Submitting via in-person delivery: All materials delivered in person or by courier must be delivered to the **DHHS main reception desk located <Room #> of the ### Street in CityName, State.**, during the office hours of <#am to #pm>. Upon receipt, materials are date-and time-stamped, which serves as the official receipt date and time used to determine acceptance or rejection of materials. Vendor is to use this address for submission via in-person delivery:

<State Agency Name>

Main Reception Desk, First FloorAttn: <FirstName LastName>, Procurement Manager

<Street Address>

<City Name, State Postal Code>

2. TRANSMITTAL LETTER

- A. A Transmittal Letter must accompany the technical RFP package. It must be on official business letterhead of the prime bidder submitting the proposal and must be signed by an individual authorized to legally bind the bidder.
- B. The Transmittal Letter must stipulate the following information:
- That the bidder is the prime Contractor and is a corporation or other legal entity;
 - A statement identifying any and all subcontractors that will be responsible for fulfilling the requirements of this RFP is included in the proposal as appropriate;
 - That the Proposer certifies they have not directly or indirectly entered into any agreement or participated in any collusion or otherwise taken any action in restraint of free competition; that this proposal has been independently arrived at without collusion with any other Proposer, competitor or potential competitor; that this proposal has not been knowingly disclosed prior to the opening of proposals to any other Proposer or competitor;
 - That the Technical and Cost Proposal are valid for a minimum of <#> months from the proposal due date;
 - That the person signing this proposal is authorized to make decisions on behalf of the bidder's organization as to the prices quoted and that the person has not participated and will not participate, in any action contrary to this statement;
 - Assurance that the bidder will agree to execute and fulfill a contract according to the conditions and terms specified in this RFP;
 - That the proposal is predicated upon the requirements, terms, and conditions of this RFP, the posted Questions and Answers, all its attachments, and any supplements or revisions thereof;



- That an individual authorized to legally bind the bidder is signing this Transmittal Letter
- That the Proposer certifies that he or she has disclosed any potential real or perceived conflict of interest with the provider community that may interfere with fair competition or be in the best interest of the State.

3. PROPOSAL ORGANIZATION AND FORMAT

A. Technical Proposals must be typed and submitted on 8.5 by 11 inch paper bound securely; presented in 12-point Times New Roman font; and sections must appear in the order and by the number assigned in the RFP. Proposals must be organized with the headings and subheadings listed below. Each heading and subheading must be separated by tabs or otherwise clearly marked. Page limits for each section where appropriate are indicated in parentheses. An outline prescribing the RFP Sections which must be submitted or responded to in the Technical Proposal is illustrated below:

1) Cover Page (1 Page) Transmittal Letter

a. Technical Proposal

- i. Table of Contents
- ii. Executive Summary (<##> pages)
- iii. Mandatory Proposal Submission Requirement (<##> page)
- iv. Corporate Qualifications and Experience (<##> pages)
- v. Organization and Management Plan (<##> pages)
- vi. Staffing Plan (Capabilities, Resumes, References) (<##>pages)
- vii. Technical Approach (<##>pages)
- viii. Transition Phase Approach (<##> pages)
- ix. Cost Proposal
- x. Required forms
- xi. Designation of Confidential and Proprietary Information
- xii. Vendor Information
- xiii. Vendor References

b. Certification Regarding Debarment and Suspension (Attachment <xx>)

c. U.S. Department of Agriculture Certification Regarding Drug-Free Workplace Requirements Form FNS-730 (Attachment <xx>)

d. U.S. Department of Agriculture Certification Regarding Lobbying – Contracts, Grants Loans and Cooperative Agreements Form FNS-732 (Attachment<xx>)

2) Table of Contents – The Technical Proposal shall contain a Table of Contents, which includes page numbers (beginning and ending) for each section. In addition, this section of the proposal shall include complete cross-references from each part, section, and subsection of



the bidder's Technical Proposal back to the appropriate section and subsection of the RFP and Addenda

- 3) Executive Summary – The Executive Summary must not exceed **<Quantity (#)>** pages. Charts, tables, or other explanatory graphics are included in the page count. The Executive Summary shall condense and highlight the contents of the Technical Proposal in such a way as to provide evaluators with a broad understanding of the entire proposal. It should contain a concise overview summarizing the Proposers understanding of the requirements of this RFP and the **<System Name>** Project, the proposed schedule for the **<#>** project phases (**<phase name>** and **<phase name>**), qualifications of key personnel, and operational structure for handling maintenance and operations responsibilities. The bidders should emphasize the most important features offered by the proposed approach and methodology. The Executive Summary should conclude with a discussion of the corporate commitment to the performance of this contract.
- 4) Mandatory Proposal Submission Requirement – The Mandatory Proposal Submission Requirement document must not exceed **<Quantity (#)>** page. Charts, tables, or other explanatory graphics are included in the page count. Respond to the Mandatory requirements as described in section **<#.#>** of RFP.
- 5) Corporate Qualifications and Experience – The Corporate Qualifications and Experience subsection must not exceed **<Quantity (#)>** pages. Charts, tables, or other explanatory graphics are included in the page count. Financial Statements may be attached as a separate addendum and are not included in the page count. See section **<#.#>** of RFP for Bidder Qualifications and Experience for contents to be provided by the bidder in this section.
- 6) Organization and Management Plan – The approach to the Organization and Management Plan must not exceed **<Quantity (#)>** pages. Charts, tables, or other explanatory graphics are included in the page count. Vendor references may be attached as a separate addendum and are not included in the page count. See section **<#.#>** of RFP for Organization and Management Plans for contents to be provided by the bidder in this section.
- 7) Staffing Plan (Capabilities, Resumes, References) – The approach to the Staffing Plan must not exceed **<Quantity (#)>** pages. Charts, tables, or other explanatory graphics are included in the page count. Resumes and references for key personnel may be attached as a separate addendum and are not included in the page count. See section **<#.#>** of RFP for Staff Capabilities, Resumes and References for contents to be provided by the bidder in this section.
- 8) Technical Approach – The Technical Approach must not exceed **<Quantity (#)>** pages. The technical approach should describe design, development, and implementation activities. It



should include configuration management approach and testing of the system. Testing must include unit testing, functional testing, integration testing, regression testing, security testing, data migration testing, conversion testing, UAT and live Pilot Testing. Charts, tables, or other explanatory graphics are included in the page count. Examples of systems documentation, reports, or plan may be attached as a separate addendum and are not included in the page count. See section <#.#> of RFP for the contents to be provided by the bidder in this section.

- 9) Transition Phase Approach – The approach to the Transition Phase must not exceed <Quantity (#)> pages. Charts, tables, or other explanatory graphics are included in the page count. Examples of systems documentation, reports, or plans may be attached as separate addenda and are not included in the page count. See section <#.#> of RFP for Transition Phase Requirements for the contents to be provided by the bidder in this section.
 - A. Cost Proposal – See section <#.#> of RFP for contents to be provided by the bidder in this section. Note that no mention of the cost of the proposal can be present in the Technical Proposal. Inclusion of cost in the Technical Proposal may constitute grounds for rejection of the entire Proposal.
 - B. Required Forms – See section <#.#> of RFP for contents to be provided by the bidder in this section.
 - C. Vendor Information – See section <#.#> of RFP for contents to be provided by the bidder in this section.
 - 1) Vendor References – See section <#.#> of RFP for contents to be provided by the bidder in this section.
 - 2) Designation of Confidential and Proprietary Information – See section <#.#> of RFP for contents to be provided by the bidder in this section.
 - 3) Certification Regarding Debarment and Suspension – See section <#.#> of RFP for contents to be provided by the bidder in this section.
 - D. U.S. Department of Agriculture Certification Regarding Drug-Free Workplace Requirements Form FNS-730 (Attachment III)
 - E. U.S. Department of Agriculture Certification Regarding Lobbying – Contracts, Grants Loans and Cooperative Agreements Form FNS-732 (Attachment <xx>)



4. MULTIPLE PROPOSALS

Multiple Proposals from a vendor **<are/are not>** permitted.

These proposals may include alternate solutions in whole or part as described in section 4.2.3.2 Source Selection regarding best value.

5. ORAL PRESENTATIONS AND SITE VISITS

Top scoring bidders (based on an evaluation of the Technical Proposals) may be required to present demonstrations, participate in interviews, and/or entertain site visits by state staff to support and clarify their Proposals if requested by the Department. The Department will make every reasonable attempt to schedule each presentation at a time and location that is agreeable to the bidder. Failure of a bidder to interview or permit a site visit on the date scheduled may result in rejection of the vendor's proposal.

6. WITHDRAWAL OF PROPOSALS

Proposals shall be irrevocable until contract award is announced unless the proposal is withdrawn. Bidders may withdraw a proposal in writing at any time up to the proposal closing date and time. To accomplish this, the written request must be signed by an authorized representative of the bidder and submitted to the RFP Procurement Manager. If a previously submitted proposal is withdrawn before the proposal due date and time, the bidder may submit another proposal at any time up to the proposal closing date and time.

A10.2.4.3 Section M – Evaluation factors for award

Section M identifies all significant factors and any significant sub-factors that will be considered in awarding the contract. Section M also lists the relative order of importance of those factors and sub-factors and how the non-cost factors relate to cost. It describes pre-proposal conferences, (i.e., bidders conferences) and post-ward conferences. This section identifies small business set-asides, product classifications, and any requirements for submitting financial information. It lists the type of contract expected to be awarded as a result of the RFP.

Example Content:

1. PROPOSAL SELECTION AND EVALUATION PROCESS

A. Preliminary Evaluation

The proposals will first be reviewed to determine if they contain the required forms and if submittal requirements are met. Failure to submit specified forms and follow submittal requirements may result in the proposal being rejected. Further, the



proposals will be reviewed initially to determine if the mandatory requirement is met. Failure to meet the mandatory requirement may result in rejection of the proposal. The mandatory proposal submission requirement can be found in section <#.#> of the RFP.

Only submissions that meet all mandatory specifications will be considered for review unless no vendor is able to comply with one or more specifications. Should that occur, the State reserves the right to delete such specifications and proceed with the review. In the event that none of the vendors meet all the mandatory requirements, the State also reserves the right to continue the evaluation of the proposals and select the proposal which most closely meets the requirements specified in this RFP. Unless the best interests of the State demand otherwise, as solely determined by the Department at its discretion, failure to meet the mandatory requirement will result in rejection of the Proposal. The Department does not anticipate the need to exercise this discretion, so a vendor that does not respond to the mandatory requirement does so at its own risk. In addition, **DHHS** may request reports on bidders' financial stability and, if such stability is not substantiated, may reject a bidder's proposal.

B. Proposal Scoring

Accepted Proposals will be reviewed by an evaluation committee and scored against the stated criteria. A bidder may not contact any member of an evaluation committee.

The committee may request interviews and perform financial stability and/or litigation analysis. The State reserves the right to check any information, regardless of the source, including but not limited to information identified in the proposal or resulting from communication with other entities involved with similar projects.

Information requested may include, but is not limited to, some or all of the following: project description and background, job performed, functional and technical abilities, communication skills and timeliness, cost and schedule estimates and accuracy, problems (e.g., poor quality deliverables, contract disputes, work stoppages), overall performance, and whether or not the firm or individual would be considered for future engagements.

The Cost Proposals will be scored using a standard quantitative calculation with the most points awarded to the proposal with the lowest cost. Subsequent scores will be calculated as illustrated in section <#.#> of the RFP.



State of **<State Name>** agencies may make awards to certified Minority Business Enterprise (MBE), or certified Disabled Veteran-Owned Business (DVB) firms submitting a qualified submission when that qualified response is not more than **<##.##>**% lower than the submission with the apparent highest point score. Authority for this program is found in **<State Name>** Statutes §citation and **<State Name>** Procurement Manual **<Identification Number>**.

C. Reference Review

<State Agency Name> will determine which, if any, references to contact and/or to visit to assess the quality of work performed, the personnel assigned to the project, and/or to see the product in use.

Bidders shall provide a list of up to **<Quantity (#)>** clients/buyers/organizations with whom the bidder has done business of similar scope and size required by this solicitation within the last **<Quantity (#)>** years. For each client/buyer/organization listed, the Proposer must include:

- 1) The name, title, address, email, and telephone number of a contact person that can serve as a reference for the bidder related to the work performed on the project/assignment.
- 2) A brief description of the project/assignment that was the basis for the business relationship, including the major goals and objectives of the project/assignment.
- 3) The bidders full-time equivalents (FTE) counts for the project/assignment.
- 4) The duration of the project/assignment.
- 5) A list of the development technologies used, the technology implemented and results of the engagements.
- 6) A description of the bidder's project management best practices.

The bidder will not be present during any reference check site visits. The results of any reference checks will be provided to the evaluation committee and used to clarify and substantiate information in the written proposal. **<State Agency Name>**, at its sole discretion, may also utilize other pertinent sources of information regarding the services provided by the bidder. Submission of completed form **<Form Identification Number>** will be considered responsive to this section. **<State Agency Name>** reserves the right to consider excluding a proposal from further consideration at any point in the evaluation process should **<State Agency Name>** or the evaluation committee members determine that one or more references are unsatisfactory, inadequate or inappropriate.



D. Disclosure Statements

Bidders must provide a statement that discloses any administrative action or lawsuit, threatened or pending, that regards (1) a financial matter that could significantly affect the organization's solvency or financial ability to successfully perform under this contract; (2) a matter that has been or would be brought against the organization as a party to a contract by another party to that contract; or (3) a licensing or regulatory matter that would affect the organization's credentials or ability to perform under this contract. Furthermore, the bidder must disclose any past contract actions brought against the organization for breach of contract or any contracts that were terminated because of the organization's breach or financial instability.

If the bidder is a subsidiary, this information must also be submitted for all parent companies. If the bidder will use subcontractors, associated companies, or others to complete the work of the project, the Proposer's responses must include pertinent subcontractor information.

E. Financial Statements

Bidders and each subcontractor (if any) must be able to substantiate their financial stability. Independently audited financial statements for the last <#> completed fiscal years, along with additional supporting documentation (Income Statement, Statement of Cash Flows, Balance Sheet, and Statement of Change in Financial Position along with all auditors' notes) must be submitted with the proposal. If the Proposer is a subsidiary, the parent company must be identified and the consolidated audited financial statements of the parent company must be submitted. The State may request reports on financial stability from independent financial rating services to substantiate the proposing vendor's stability. Bidder name is to be included on each page submitted.

If no audit was required, please explain why and submit <#> years of financial statements certified by two officers of the Board of Directors, and the chief financial officer/financial manager.

F. Evaluation Criteria

The proposals will be scored using the following criteria:

Description		Max Points
1.	Technical Approach (PWS #.#)	40
2.	Cost (PWS #.#)	35
3.	Transition Phase Approach (#.#)	10
4.	Organization & Management Plan (PWS #.#)	6



Description		Max Points
5.	Staffing Plan (PWS #.#)	5
6.	Proposer Qualifications and Experience (PWS #.#)	4
	TOTAL	100

A proposal that receives less than **<#/%>** of the combined points in the following Technical Sections may be ineligible for further consideration and may not have its cost proposal scored: section **<#.#>** of the RFP Corporate Qualifications & Experience, section **<#.#>** of the RFP Organization & Management Plan, section **<#.#>** of the RFP Staffing Plan, section **<#.#>** of the RFP Technical Approach, and section **<#.#>** of the RFP Transition Phase Approach. The Department reserves the right to waive this requirement at its sole discretion.

G. Right to Reject Proposals and Negotiate Contract Terms

The State reserves the right to reject any and all Proposals. The State may negotiate the terms of the contract, including the award amount, with the selected bidder(s) prior to entering into a contract. If contract negotiations cannot be concluded successfully with the highest scoring bidder(s), the agency may initiate negotiations for a contract with the next highest scoring bidder(s).

The intent of this RFP is to award a contract for **<System Name>** project.

2. AWARD AND FINAL OFFERS

Subject to meeting the threshold percentage of points noted in section **<#.#>** of the RFP, the State will compile the final scores (Technical and Cost) for each proposal. The award will be granted in one of two ways. The award may be granted to the highest scoring responsive and responsible bidder. Alternatively, the highest scoring bidder or bidders may be requested to submit best and final offers. If best and final offers are requested by the State and submitted by the vendor, they will be evaluated against the same criteria as described in Section **<#.#>** of the RFP, scored and ranked by the evaluation committee. The award then will be granted to the highest scoring bidder. However, a bidder should not presume that the State will request any best and final offers.

3. NOTIFICATION OF INTENT TO NEGOTIATE A CONTRACT

All bidders who respond to this RFP will be notified in writing of the Department's intent to negotiate a contract as a result of this RFP.

After notification of the intent to award a contract is issued and under the supervision of agency staff, copies of all proposals will be available for public inspection from 8:00 a.m.



to 4:00 p.m. at **<Address>**. Proposers should schedule appointments for reviews with **<FirstName LastName>**, Procurement Manager (See Section **<#. #>** of the RFP).

4. PROTEST PROCESS

A vendor who is aggrieved in connection with a solicitation may protest to the procuring agency. Protestors should make their protests as specific as possible and should identify statutes and **<State Name> <Administrative Code>** provisions that are alleged to have been violated. A notice of intent to protest will be submitted in writing to the head of the procuring agency or designee within 5 working days after issuance of the solicitation. The protest will be submitted in writing to the head of the procuring agency or designee within 10 working days after issuance of the solicitation.

Protests concerning the intent to award or negotiate a contract:

A vendor who is aggrieved by the intent to award a contract may protest to the procuring agency. Protestors should make their protests as specific as possible and should identify statutes and **<State Name> <Administrative Code>** provisions that are alleged to have been violated. A notice of intent to protest will be submitted in writing to the head of the procuring agency within **<#>** working days after issuance of the notice of intent to award a contract. The protest must be submitted in writing to the head of the procuring agency, or designee, within **<#>** working days after issuance of the notice of intent to award a contract.

Any written notice of intent to protest the intent to negotiate a contract must be filed with:

<State Agency Name>

Attn: **<FirstName LastName>**, Secretary

<Street Address>

<City Name, State Postal Code>

The decision of the Secretary of **<State Agency Name>** may be appealed to the Secretary of the **<Superior Department Name>** within **<Quantity (#)>** working days after the date of decision issuance, with a copy of such appeal filed with **<State Agency Name>**. Any and all appeals must allege a violation of a **<State Name>** statute or a section of the **<State Name> <Administrative Code>**.

A10.3 Alternative RFP and Contract Formats

FNS does not prescribe a specific RFP and contract arrangement or format. The previous examples are based on the Uniform Contract Format from the Federal Acquisition Regulations. This section provides two alternative organization of contents for RFPs and contracts. They illustrate a more detailed organization of information



and other topics State agencies might consider for inclusion in their own project RFPs and contracts. Much of the information in the examples above could be reorganized into either of these two format examples.

A10.3.1 RFP and Contract Format Alternative - Example One

- 1.0 GENERAL INFORMATION
 - 1.1 Introduction and Background
 - 1.2 System Description
 - 1.3 Retention of Rights
 - 1.4 Procuring and Contracting Agency
 - 1.5 Definitions
 - 1.6 Clarification and/or Revisions to the Specifications and Requirements
 - 1.7 Calendar of Events
 - 1.8 Contract Term and Funding
- 2.0 PREPARING AND SUBMITTING A PROPOSAL
 - 2.1 General Instructions
 - 2.2 Incurring Costs
 - 2.3 Submitting the Proposal
 - 2.4 Transmittal Letter
 - 2.5 Proposal Organization and Format
 - 2.6 Multiple Proposals
 - 2.7 Oral Presentations and Site Visits
 - 2.8 Withdrawal of Proposals
- 3.0 PROPOSAL SELECTION AND AWARD PROCESS
 - 3.1 Preliminary Evaluation
 - 3.2 Proposal Scoring
 - 3.3 Reference Review
 - 3.4 Disclosure Statements
 - 3.5 Financial Statements
 - 3.6 Evaluation Criteria
 - 3.7 Right to Reject Proposals and Negotiate Contract Terms
 - 3.8 Award and Final Offers
 - 3.9 Notification of Intent to Negotiate a Contract
 - 3.10 Appeals Process
- 4.0 Technical Proposal Submission Requirements
 - 4.1 Proposer Qualifications and Experience
 - 4.2 Organization and Management Plan
 - 4.3 Staffing Plan: Capabilities, Resumes and References
 - 4.4 Technical Approach Proposal Requirements
 - 4.5 Transition Phase Requirements
 - 4.6 Health Insurance Marketplace
- 5.0 TECHNICAL REQUIREMENTS



- 5.1 Required Business Systems
- 5.2 System Interfaces
- 6.0 TRANSITION PHASE
 - 6.1 Introduction
 - 6.2 Professional Staffing Requirements
 - 6.3 Transition Planning for the <System Name>
 - 6.4 Transition Phase
 - 6.5 Operational Readiness of the Contractor
 - 6.6 Completion of Successful Trial Application Release in Test Environment
 - 6.7 Transition to Operations and Maintenance
 - 6.8 Start of Operations
- 7.0 COST PROPOSAL
 - 7.1 General Instructions on Preparing the Cost Proposal
 - 7.2 Proposed Facilities (Government Furnished Facilities)
- 8.0 SPECIAL CONTRACT TERMS AND CONDITIONS
 - 8.1 Contract Administrator
 - 8.2 Cooperation During Transition
 - 8.3 Executed Contract to Constitute Entire Agreement
 - 8.4 Federal Inspections
 - 8.5 Fixed Price Deliverables
 - 8.6 Foreign Corporation
 - 8.7 Inspection Of Work Performed
 - 8.8 System Name Access
 - 8.9 Legal Relations
 - 8.10 Liquidated Damages
 - 8.11 Minority Business Subcontractors
 - 8.12 Personnel Changes
 - 8.13 Prime Contractor Responsibility
 - 8.14 Settlement of Disputes
 - 8.15 Responsibilities Upon Termination
 - 8.16 Right to Publish
 - 8.17 Severability
 - 8.18 Site Rules and Regulations
 - 8.19 Software Ownership
 - 8.20 System Changes
 - 8.21 Equal Employment Opportunity
 - 8.22 Civil Rights Compliance
- 9.0 STANDARD TERMS AND CONDITIONS
- 10.0 REQUIRED FORMS
- APPENDIX A: Cost Proposal
- APPENDIX B: Staff Allocation Matrix
- APPENDIX C: Cost Worksheets
 - C1.1 – Maintenance Cost Worksheets



- C1.2 – Actual Billing Rates by Position Worksheets
- APPENDIX D: Service Level Agreements (SLA)
 - D1.1 – <System Name> Systems Online Availability Uptime
 - D1.2 – <System Name> Systems Transaction Response Time
 - D2.1 – Benefit Issuance File Creation and Transmission
 - D2.2 – Production Batch Jobs Execution
 - D3.0 User Acceptance Test Project Quality
- ATTACHMENT I: Business Associate Agreement
- ATTACHMENT II: Certification Regarding Debarment and Suspension
- ATTACHMENT III: USDA Certification Regarding Drug-Free Workplace Requirements (Grants) Alternative I –
For Grantees Other Than Individuals
- ATTACHMENT IV: USDA Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion
– Lower Tier Covered Transaction
- ATTACHMENT V: USDA Certification Regarding Lobbying – Contracts, Grants Loans and Cooperative
Agreements
- ATTACHMENT VI: Clean Air Act
- ATTACHMENT VII: Clean Water Act

A10.3.2 RFP and Contract Format Alternative - Example Two

- 1.0 Introduction
 - 1.1 Background
 - 1.2 Procurement Authority
 - 1.3 Overview of the Solution
 - 1.4 High Level Technical Overview
 - 1.5 Interstate Collaboration
 - 1.6 Project Implementation
 - 1.7 Project Funding
 - 1.8 Procurement Approach
 - 1.9 Project High-Level Schedule
- 2.0 Procurement Rules
 - 2.1 Procurement Authority
 - 2.2 Procurement Schedule
 - 2.3 Procurement Contact Information
 - 2.4 Basic Qualification Criteria
 - 2.5 Information to be Included in Proposals
 - 2.6 Subcontracting
 - 2.7 Pre-Proposal Conference
 - 2.8 Letter of Intent to Submit a Proposal
 - 2.9 Submission of Written Questions
 - 2.10 Submission of Proposals
 - 2.11 Late Submissions, Modifications and Withdrawal of Proposals



- 2.12 Alternate Proposals
 - 2.13 Contacts with Bidders
 - 2.14 State of Rhode Island Use of Proposal Ideas
 - 2.15 Award of Contract
 - 2.16 Contract Award Notification
 - 2.17 Protest of Contract Award
 - 2.18 Cost of Preparing Proposals
 - 2.19 Disposition of Proposals
 - 2.20 Access to Public Records Act
 - 2.21 Background Checks
 - 2.22 Contract Provisions
 - 2.23 Minority Business Enterprise and Equal Employment Opportunity
 - 3.0 Proposal Submission Requirements
 - 3.1 General Instructions
 - 3.2 Technical Proposal Requirements
 - 3.3 Cost Proposal Requirements
 - 4.0 Scope of Work
 - 4.1 Project Management Approach
 - 4.2 Task Orders
 - 4.3 Milestones and Deliverables
 - 4.4 Payment
 - 5.0 Business and Functional Requirements
 - 5.1 Integrated Business Vision
 - 5.2 Functional Purpose
 - 5.3 Assumptions and Constraints
 - 5.4 Business and Functional Requirements
 - 6.0 Technical Requirements
 - 7.0 Evaluation and Selection
 - 7.1 Evaluation Approach
 - 7.2 Evaluation Process
 - 7.3 Criteria for Evaluation
 - 7.4 Contract
 - 8.0 Contract Terms and Conditions
 - 8.1 State's General Conditions of Purchase
 - 8.2 Supplemental Terms and Conditions
- APPENDICES
- A. State General Terms and Conditions
 - B. Drug-Free Workplace Policy and Contractor Certificate of Compliance
 - C. Subcontractor Compliance
 - D. Environmental Tobacco Smoke
 - E. Certification Regarding Debarment, Suspension, and Other Responsibility Matters
 - F. Statutory and Regulatory Documents



- G. Mandatory Submission Checklists
- H. Approach to Staffing
- I. Deliverables
- J. Detailed Business Requirements
- K. Detailed Technical Requirements
- L. Eligibility and Enrollment Individual Process Flows
- M. Plan Management Process Flows
- N. Financial Management Process Flows
- O. Service Level Agreements
- P. Draft Certification Application
- Q. EOHHS Program Descriptions
- R. Health Benefits Exchange Mission, Vision, and Goals
- S. Cost Response

Endnotes

¹³⁰ "Uniform Contract Format", Federal Acquisition Register (FAR) Part 15.204-1, U.S. Government, <https://acquisition.gov/content/15204-1-uniform-contract-format-table-15-1-uniform-contract-format>.



A11. Federal Procurement Clauses

A11.1 Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of federally assisted construction contract in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." (2 CFR 200, Subpart F, Appendix II)

The EEO clause must be included or the State must have its own EEO similar clause.



See the [Department of Labor Executive Order 11246 – Equal Employment Opportunity](#) for more information.

A11.2 Clean Air and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended. Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). (2 CFR 200, Subpart F, Appendix II)

A11.3 Anti-Lobbying Act

This Act prohibits the recipients of Federal contracts, grants, and loans from using appropriated funds for lobbying the Executive or Legislative branches of the Federal government in connection with a specific contract, grant, or loan. As required by Section 1352, Title 31 of the U.S. Code and implemented at 2 CFR 200, Subpart F, Appendix II, for persons entering into a grant or cooperative agreement over \$100,000, as defined at 31 U.S.C. 1352, the applicant certifies that:



- a. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the making of any federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement;
- b. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form – LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions;
- c. The undersigned shall require that the language of this certification be include in the award documents for all sub-awards at all tiers (including sub-grants, contracts under grants and cooperative agreements, and subcontracts) and that all sub-recipients shall certify and disclose accordingly.

A11.4 Americans with Disabilities Act



See the [Americans with Disabilities Act website](#) for more information.

This Act (28 CFR Part 35, Title II, Subtitle A) prohibits discrimination on the basis of disability in all services, programs, and activities provided to the public and State and local governments, except public transportation services.

A11.5 Drug-Free Workplace Statement

The Federal government implemented 41 U.S. Code § 8103, Drug-free workplace requirements for Federal grant recipients in an attempt to address the problems of drug abuse on the job. It is a fact that employees who use drugs have less productivity, a lower quality of work, and a higher absenteeism, and are more likely to misappropriate funds or services. From this perspective, the drug abuser may endanger other employees, the public at large, or themselves. Damage to property, whether owned by this entity or not, could result from drug abuse on the job. All these actions might undermine public confidence in the services this entity provides.



Therefore, in order to remain a responsible source for government contracts, the following guidelines have been adopted:

1. The unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in the work place.
2. Violators may be terminated or requested to seek counseling from an approved rehabilitation service.
3. Employees must notify their employer of any conviction of a criminal drug statute no later than five days after such conviction.
4. Contractors of federal agencies are required to certify that they will provide drug-free workplaces for their employees.

Transactions subject to the suspension/debarment rules (covered transactions) include grants, subgrants, cooperative agreements, and prime contracts under such awards. Subcontracts are not included.

A11.6 Royalty Free Rights to Use Software or Documentation Developed

2 CFR 200.315 Intangible property.

(a) Title to intangible property (see §200.59 Intangible property) acquired under a Federal award vests upon acquisition in the non-Federal entity. The non-Federal entity must use that property for the originally-authorized purpose, and must not encumber the property without approval of the Federal awarding agency. When no longer needed for the originally authorized purpose, disposition of the intangible property must occur in accordance with the provisions in §200.313 Equipment paragraph (e).

(b) The non-Federal entity may copyright any work that is subject to copyright and was developed, or for which ownership was acquired, under a Federal award. The Federal awarding agency reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so.

(c) The non-Federal entity is subject to applicable regulations governing patents and inventions, including government wide regulations issued by the Department of Commerce at 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Awards, Contracts and Cooperative Agreements."

(d) The Federal Government has the right to:

(1) Obtain, reproduce, publish, or otherwise use the data produced under a Federal award; and



(2) Authorize others to receive, reproduce, publish, or otherwise use such data for Federal purposes.

A11.7 Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. (2 CFR 200, Subpart F, Appendix II)

States to include in RFP and Contract a statement of certification by the vendor, such as “By signing this contract, the vendor certifies it is not suspended or debarred as specified by these rules.”



A12. RFP and Contract Review Checklist

A12.1 General Review Items

FNS will review the RFP and resulting contract using this checklist. The checklist is organized using the Federal Uniform Contract Format as an example. Individual State agency formats may vary from this example. The primary concern is that the RFP and contract contain the same information.

There are some review criteria that don't specifically fit the organization of the RFP and contract, but apply to the whole document.

State:					
Project Name:					
Date Submitted:					
Title Page		Cover Letter		Table of Contents	

GENERAL REVIEW CRITERIA

✓	RFP/CONTRACT INCLUDES
	Does the RFP follow proper State and Federal procurement law?
	Do the tasks and deliverables make sense when compared to the stated project purpose in the APD?
	Do requirements in the RFP adequately reflect those in the APD?

A12.2 Part 1 - The Schedule

A12.2.1 Section A - Solicitation/Contract Form

Section A is the first page of the RFP. It may be a standard form or cover letter that gives the RFP number, explains what type of solicitation it is (Sealed Bid or Negotiated Bid), who issued the solicitation, the address of the interested party receiving the solicitation, where proposals or bids are to be delivered, closing date and time,



the contractor's name and address, and a brief description of the items or services to be performed. This will be signed by the contractor and returned with their proposal.

SECTION A - SOLICITATION/CONTRACT FORM

✓	RFP/CONTRACT INCLUDES
	Issuing office and agency manager responsible for procurement
	Agency(s)/Program(s) that will use the system
	Description of the purpose of the RFP/contract
	Description of the Contract Type (Firm Fixed Price, Time & Materials, etc.)
	Terms of the RFP and contract (single or multiple vendors)
	Submission requirements, such as: • Time and date proposals due (including time zone) • Office to which proposals must be sent • How proposal components must be separated and sealed
	An Order of Precedence in correct hierarchical order, first to last, for dispute resolution purposes. For example: • The signed contract • Federal standards and clauses • Standard State Appendices • Body of the Agreement and Exhibits • Revisions to the RFP • Official Questions and Answers • The RFP • The Contractor's Proposal • Any correspondence related to the Contractor's proposal) • Other documents needed to clarify the project's outcomes



A12.2.2 Section B - Supplies or Services and Prices/Costs

Section B is a listing of the deliverable supplies or services. There is a brief description of the supplies or services, the quantities, and costs of the items. Deliverables can be hardware, software, data, labor, or a combination of any or all of these items. At the solicitation stage, Section B will have blanks for the cost; the contractor fills in their proposed costs and submits as a separate pricing volume from the technical volume when sending their offer to the Government. When a contract is awarded, this information is usually incorporated into the contract, not as a separate volume.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

✓	RFP/CONTRACT INCLUDES
	Description of what is being purchased or leased
	Preferred method of payment for equipment (rental, lease, purchase)
	Specify the period of availability for services required
	Itemized equipment required (and statement that any equipment prices offered must be equal to or lower than those currently available to the state from the same vendor under other contracts.)

A12.2.3 Section C - Description/Specifications/Work Statement

Section C outlines to the contractor the actual tasks or outcomes to be performed. Depending on the acquisition, this section may be a Statement of Objectives (SOO), Performance Work Statement (PWS), or Statement of Work (SOW). If the acquisition requires a SOW or a PWS, the document may contain a Work Breakdown Structure (WBS). The WBS provides a way to align requirements, desired schedule, and deliverables to price proposals, staffing, performance standards, and delivery standards. The WBS provides a framework for the offeror's technical and management approach.



For detailed descriptions of PWS or SOW see chapter **4.0 Procurement**.



References to requirements should be explicitly included in the PWS and not linked to external web pages or Internet sites. Access to requirements on external web pages or Internet sites is not likely to be available post-award.

SECTION C - DESCRIPTIONS/SPECIFICATIONS/SOW

✓	RFP/CONTRACT INCLUDES
	Definition and background information to orient the reader
	Relationship(s) of proposed system to agency function and to other systems and organizations
	Major objectives of the proposed system (e.g., improved service delivery, accountability, operational efficiency)
	Itemize improvements that the State agency expects to gain: • New capabilities • Upgraded existing capabilities • Elimination of deficiencies
	Existing methods, procedures, systems, applications that the proposed system will support, supplement, change or replace
	Existing hardware configurations and components
	Operating system(s), system utility routines, database management, applications development, and other software currently in use
	Portions of current system environment that are expected to remain in place and interface with the new system, and portions that will be replaced
	Expected useful life of the proposed system
	Provide an incremental growth forecast for various workload data over the expected life of the system
	Explanation of project phasing and how phases relate to deliverables



SECTION C - DESCRIPTIONS/SPECIFICATIONS/SOW

✓	RFP/CONTRACT INCLUDES
	Allow for incremental installation of equipment where appropriate
	Flexibility in design to provide: • Interfaces with other software and hardware • Allow for future growth, changes and improvements through modular design
	Commitment to Open Systems Interface (OSI) standards to minimize negative effects of proprietary systems
	Offered solutions should use tried and tested state-of-the-art technology (unless a unique, untested option is specifically sought)
	Products and services the State agency expects contractor to deliver
	Functional Requirements Document (FRD): • Define the proposed system and document system goals, objectives, and programmatic requirements • Describe what the new system and/or hardware should do • Definitions are broken down into functional components in a logical sequence with proposed inputs, outputs, and processes
	Functions required in qualitative and quantitative terms
	Technical requirements and specifications
	State's requirements for • Federally compliant testing and live pilot • Phased implementation • Caseload conversion • Uninterrupted service to users and/or clients
	Statistics for such workload types as: • Timesharing sessions or connections



SECTION C - DESCRIPTIONS/SPECIFICATIONS/SOW

✓	RFP/CONTRACT INCLUDES
	• Online transactions • Batch jobs • Demand jobs
	Indicate volumes in terms of: • Regular and peak loads • Daily, weekly and monthly processing schedules • Production vs. development environments, if applicable
	Requirements of the system for: • Throughput requirements • Storage capacity • Transaction, input/output volumes, frequency • Telecommunications transmission rates • Data or processing sequencing requirements • Timing or turnaround restrictions
	Performance requirements: • Data and accuracy standards (mathematical, logical, legal, transmission) • Data validation • Timing (response time and processing time)
	Requirements for interfaces with the operating environment (equipment, communications network, software)
	Proposed integration of new equipment with currently installed equipment state expects to retain
	Requirements for provision of • Operating software • Performance of operating software • Implementation of operating software modifications and revisions
	Illustrate proposed data flow and overall view of planned capabilities



SECTION C - DESCRIPTIONS/SPECIFICATIONS/SOW

✓	RFP/CONTRACT INCLUDES
	Requirements for data and application conversion or reprogramming
	Caseload conversion requirements
	Database management requirements
	Security and privacy requirements
	Documentation and operation standards expected
	Documentation requirements – user manuals, operating instructions, design descriptions; standards, numbers of copies, format and media (e.g., paper, electronic, etc.)
	Safeguards against fraud, waste, and abuse
	System implementation requirements
	Require a test plan including, but not limited to: unit testing, integration testing, performance testing, end-to-end testing, UAT, and regression testing, live pilot
	Specify operational use time in terms of equipment availability and minimum downtime
	Requirements for on-site maintenance, on-call, and availability of replacement hardware components, if applicable
	Require on-site field modification of equipment on the same basis as furnished to other customers
	Any need for operations or facilities management to be part of the contract



SECTION C - DESCRIPTIONS/SPECIFICATIONS/SOW

✓	RFP/CONTRACT INCLUDES
	Any need for additional hardware, software, maintenance or support
	Responsibility for site preparation
	User training requirements, to include: • Skills to be taught • Number of users • Location(s) • Documentation to be provided
	Clearly delineate between mandatory requirements and optional features sought
	Require a plan/schedule for orderly delivery, install and testing of equipment
	Organization and flow of desired schedule: the timetable and expected outcomes make sense
	Require a conversion plan from legacy system to new system including: issues, requirements, tasks, services, facilities, equipment, and personnel
	Other State agency performance requirements (to assure open competition)
	Contract and Administrative Deliverables • Type and frequency of expected project status reports • Project meetings and teleconferences (to include frequency, attendees, scheduling, venue)
	Transition and Knowledge transfer activities

A12.2.4 Section D - Packaging and Marking

If there are any packaging and marking requirements, they are outlined in Section D. This section describes delivery information, such as, where products will be sent, delivery destinations, how packaging will be



accomplished and what markings must be included for deliverables. It may also define who is responsible for shipping fees, if applicable. For State agencies, this would affect delivery of information technology equipment, other hardware and parts required to support implementing a new system, and other property acquired through the procurement. It may also apply to any physical deliverables such as user's manuals, media containing electronic files (e.g., compact discs (CDs), digital video discs (DVDs), or any other tangible deliverable specified in the RFP.

SECTION D - PACKAGING AND MARKING

✓	RFP/CONTRACT INCLUDES
	Delivery details: • Address • Point of Contact (i.e., person) • Telephone number(s) • E-Mail address (as appropriate)

A12.2.5 Section E - Review and Acceptance

Requirements for review of deliverables, acceptance, quality assurance and reliability are explained in Section E. This often includes a review schedule, where reviews will occur, and acceptance criteria for each contract line item number (CLIN). Testing is part of review and would be appropriate for this section. Review can be either at the origin or destination; this should be specified in the contract. For physical deliverables such as IT equipment, an inspection should be done upon delivery to ensure no damage has occurred during shipment.

SECTION E - INSPECTION AND ACCEPTANCE

✓	RFP/CONTRACT INCLUDES
	State the functional title of the State Project Manager to whom the contractor will report
	Plan for State agency review and approval of work performed
	System acceptance requirements
	Description of standards to ensure the product meets functional and technical requirements: • Quality Assurance Surveillance Plan (QASP) • State the review and approval period for each deliverable



SECTION E - INSPECTION AND ACCEPTANCE

✓	RFP/CONTRACT INCLUDES
	• Service level Agreements
	State review and approval times for deliverables (Caution: avoid blanket statements such as “all deliverables will be reviewed within 10 days of submission”—some deliverables are huge, and sometimes several are delivered simultaneously. Look for distinctions or an escape clause to the general statement.)

A12.2.6 Section F - Deliveries or Performance

Section F specifies the requirements for place and method of delivery or performance. Delivery schedules for hardware and services may be described in terms of calendar dates or in specified periods of time from contract award date. The place of performance may also be included here (e.g., contractor facilities, state office, state central computer facility, training locations, local agency offices, etc.).

SECTION F - DELIVERIES OR PERFORMANCE

• ✓	RFP/CONTRACT INCLUDES
	Any tasks that must be done on site vs. at contractor’s offices
	Stipulate contractor’s responsibility for deliverables
	Require a schedule of proposed work with defined milestones and dates or timeframes
	Location of the service or product to be delivered
	Site conditions and limitations

A12.2.7 Section G - Contract Administration Data

Section G relays accounting, appropriation data, and funding source data. It includes any required contract administration information or instructions other than those on the solicitation form. It also includes a statement



that the offeror should include the payment address in the proposal, if it is different from that shown for the offeror.

SECTION G - CONTRACT ADMINISTRATION DATA

• ✓	RFP/CONTRACT INCLUDES
	Organizational responsibilities
	Invoicing instructions for the contractor
	How are payments to be made to the contractor
	Schedule of payments
	Billing method contractor is to use to ensure identification of costs for each Federal and State program
	Description of formal change order process

A12.2.8 Section H - Special Contract Requirements

Section H conveys any unique or special contract requirements such as options, warranties, government furnished equipment and performance penalties. These special clauses must be clear and concise. Because these are not standard clauses, the information is written in full text and not incorporated into the RFP by reference. Other elements may include key personnel provisions, option terms, economic price adjustment provisions, multiyear provisions, limitations on government obligations, and payment of incentive fees.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

• ✓	RFP/CONTRACT INCLUDES
	Constraints and limitations in terms of program requirements, organization, and cost
	Describe resources the State agency will make available (i.e., government furnished equipment, government furnished facilities, government furnished property, etc.)



SECTION H - SPECIAL CONTRACT REQUIREMENTS

• ✓	RFP/CONTRACT INCLUDES
	Items the contractor is required to provide for their own support (e.g., facilities, equipment, computer resources, etc.)
	Specify minimum personnel and experience requirements for development, maintenance, facilities management, or other contractor staff
	Provide estimates of the level of effort anticipated in terms of person years or other reasonable indicators
	Key project personnel (contractor) clause: • State gets to decide who is “key” • State’s right to approve replacements • Requirement that bidder disclose all other project assignments and their timeframes of any staff proposed for this project • State can reserve the right to apply liquidated damages if key personnel remain with the contractor but are not assigned to this project after they are proposed • State cannot prevent termination of employees by the contractor, but can have stipulations on replacements • Replacements must meet or exceed qualifications of proposed staff
	Standards for Subcontractors; stipulation that sub-contractors are the responsibility of the prime
	Other system contractors or providers with whom bidder must agree to cooperate
	Contract termination provisions/procedures (both parties)
	Performance bond requirements
	Performance expectations, prescribed remedies and penalties that protect the State in the event of a failure in performance by the vendors
	State vs. Contractor responsibilities



SECTION H - SPECIAL CONTRACT REQUIREMENTS

• ✓	RFP/CONTRACT INCLUDES
	Contract must assure FNS access to the system during design, development, and operation and to pertinent cost records of contractors and sub-contractors as FNS considers necessary



A12.3 Part 2 - Contract Clauses

A12.3.1 Section I - Contract Clauses

Section I includes standard clauses. Most of the clauses are incorporated by reference. Clause selection varies by the nature of the requirement (supplies, services, construction) and the type of contract (Fixed Priced types or Cost Reimbursement types). This section also includes intellectual property clauses. Most are required by public law and have mandatory requirements to be performed by the contractor. Compliance is a must. Non-compliance can have serious legal ramifications for the contractor and the Government.

SECTION I - CONTRACT CLAUSES

✓	RFP/CONTRACT INCLUDES
	All mandatory Federal clauses
	Royalty-Free Rights to Use Software or Documentation Developed
	Equal Employment Opportunity Act
	Anti-Lobbying Act
	Clean Air and Federal Water Pollution Control Act
	Debarment, suspension, and other responsibility matters
	Drug Free Workplace Statement
	Americans with Disabilities Act
	The Copeland "Anti-Kickback" Act, 40 USC §276c and 18 USC §874



SECTION I - CONTRACT CLAUSES

✓	RFP/CONTRACT INCLUDES
	State's standard procurement clauses
	Any additional conditions applicable to the selected bidder
	Contract period (Base Period and Extension Options)
	Turnover provision or non-transferability
	Notice to Cure
	Incentives, penalty, and termination clauses
	Hold harmless
	Force Majeure
	Procedure to resolve disputes
	Governing law/jurisdiction
	Taxes
	Modification and renewal clause
	Whole RFP may be canceled



SECTION I - CONTRACT CLAUSES

✓	RFP/CONTRACT INCLUDES
	Subject to availability of Federal funds
	Right to waive technicalities
	Bidder may not publicize
	Insurance
	State may contact secondary references
	Conflict of Interest
	Confidentiality
	Contractor must disclose if they've ever been terminated (for "cause" or for "convenience")



A12.4 Part 3 - List of Documents, Exhibits, and Other Attachments

A12.4.1 Section J - List of Attachments

Section J lists all the documents that are included in the RFP but are attached as “stand-alone” documents. The contracting officer lists the title, date, and number of pages for each attached document, exhibit, and other attachment. Cross references to material in the other contractual sections may be inserted as appropriate. Examples include the System Specification, exhibits, technical or engineering data, SOW or PWS, training systems requirements document, system interface diagrams, QASP, and applicable regulations and policies.

SECTION J - LIST OF ATTACHMENTS

✓	RFP/CONTRACT INCLUDES
	Include a listing and description of all attachments, supplements, and other supporting documentation required

A12.5 Part 4 - Representations and Instructions

The following Sections (K, L, and M) will not appear in the contract. These three sections are only found in the RFP because they give directions to the offerors on how to respond to the Government’s solicitation. Once a contract is awarded, these directions are no longer relevant. However, the Government does retain these three sections in the source selection files.

A12.5.1 Section K - Representations

Section K provides representations, certifications and other statements that must be completed by the offeror (e.g., small business size, equal employment opportunity compliance, OSHA compliance). These documents are completed and submitted with the offeror’s proposal.

SECTION K – REPRESENTATIONS

✓	RFP INCLUDES
	Qualifications – how vendors are qualified to do business with the State agency



A12.5.2 Section L - Instructions, Conditions, and Notices to Offerors or Respondents

Section L provides guidance to the offerors or respondents in preparing proposals or responses to requests for information. Prospective offerors or respondents may be instructed to submit proposals or information in a specific format, including how to organize the proposal (e.g., Administrative, Management, Technical, Past Performance, and Cost or Pricing data). The contractor should not be required to provide data that will not be evaluated, nor should the Government have source selection evaluation criteria they have not asked the contractor to address in their proposal.

SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS

✓	RFP INCLUDES
	Procurement Schedule (not the anticipated project schedule) with realistic time frames for: • Pre-proposal conferences • Questions & Answers • Proposal deadline • Evaluation • Contract negotiations • Date of award, (estimated) • Initiation of work
	Number of copies of Proposal required
	Headings and Titles (do not construe content)
	Details on general proposal appearance and organization
	Details on additional events and processes, such as: • Presentations/demonstrations • Rejection of proposals • Late proposals • Period of validity for proposals



SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS OR RESPONDENTS

✓	RFP INCLUDES
	Provide copies of all specific forms, charts, and worksheets that the bidder is required to submit for both the technical and business proposals
	Bidders required to propose how to meet the proposed functional requirements as outlined in the FRD.
	Bidders required to provide a statement, including personnel background and experience information, of the contractor's proposed project staff
	Bidders required to provide a statement of corporate financial resources, a history of prior involvement in similar projects, and information regarding pending litigation, debarment or suspension
	Bidders required to provide a line-item cost statement, covering both development and operational costs, for the expected life of the system
	Bidders are required to submit pricing and costing information in a separate volume from the technical approach
	Bidder must provide system installation details regarding space, weight, size, and other physical requirements for the system, as applicable
	Bidders required to provide key personnel résumés
	Bidders prohibited from contacting state staff other than procurement office
	Bidders must disclose any proprietary tools needed to read, manage or modify system code
	Bidders must disclose cost history/trend of licensing fee changes for any products proposed which involve such fees, such as Oracle
	Location, contents and access instructions for electronic Bidders library
	Limitations/stipulations imposed on all bidders, such as: • Data disclosure and confidentiality • Cost of preparing proposals



A12.5.3 Section M - Evaluation Factors for Award

Section M identifies all significant factors and any significant sub-factors that will be considered in awarding the contract. Section M also lists the relative order of importance of those factors and sub-factors and how the non-cost factors relate to cost. This section may include submission guidance for preparing proposals and responses that will be considered as evaluation factors. This includes the specific proposal format, organization and arrangement of proposals, and general instructions (e.g., number of copies, number of pages, document formatting such as font size and spacing, etc.). It describes pre-proposal conferences, (i.e., bidders conferences) and post-award conferences. This section identifies small business set-asides, product classifications, and any requirements for submitting financial information.

It is important to remember that source selection planning begins prior to RFP development and must be coordinated with the development of the RFP to ensure an effective evaluation of well-organized proposals. The Source Selection Plan should be agreed upon before the release of the RFP. In order to ensure an effective and defensible evaluation of proposals, the Source Selection Plan must be followed to the letter by everyone involved with the source selection. The RFP Section L (providing instructions to the offerors) and Section M (addressing the evaluation factors and sub-factors and the manner in which they will be evaluated) must mirror the same areas of the Source Selection Plan that address the information to the offerors and list the evaluation factors and sub-factors. By ensuring that these areas contained in Source Selection Plan are replicated in the RFP, and that the members of the Source Selection team adhere to the Source Selection Plan, the Government and the contractors can be assured of fair, unbiased evaluations of the proposals.

SECTION M - EVALUATION FACTORS FOR AWARD

✓	RFP INCLUDES
	Describe the general contract negotiation and award process, which includes: • Issuing letters of intent • Negotiating contract language, if necessary, and • Signing the contract
	Description of method the State will use to evaluate proposals
	Specify evaluation criteria and evaluation factor weight distribution
	Indicate not only how points will be awarded for both technical approach and total cost, but also the weight that will be given to each of the two proposal components



SECTION M - EVALUATION FACTORS FOR AWARD

✓	RFP INCLUDES
	The evaluation criteria must not specify bidder's geographic location
	Integrity of technical information (Needs have been sufficiently articulated)
	Document demonstrates an understanding of FNS requirements
	Matching references within the document • Dates and dollar figures in text coincide with schedule or budget • Text references to figures and appendices coincide with their title
	Details on how system demonstrations will factor into the evaluation process
	Alternative proposals are allowed or not allowed
	State's right to negotiate "best and final"
	Procurement schedule allows adequate response time for Federal review and allows adequate response time for potential bidders to respond.



A13. Sample Status Report

A13.1 Status Report Checklist

This sample report in this appendix is a suggested guideline, and models the Status Report Checklist found below. The sample report begins on the next page, in **section A13.2**.

The following text styles are used throughout this sample report:

- **Guidance Text - Descriptions, guidance, information, and suggestions of what to include in a particular section of the status report.**
- Sample Text - An example or concept that applies to the section and could be used with minor updates.
- **“Fill-In” Data – Information or data the State agency needs to “fill-in” based on their requirements.**

STATUS REPORT CHECKLIST

✓	ITEM
	Executive Summary
	Work Accomplished
	Deliverables in Progress
	Planned Activities
	Project Deliverables Status
	Project Budget and Actual Expenditures
	Updated Project Schedule of Milestones and Deliverables (Gantt Chart)
	Contractor Performance Update



A13.2 Cover Page

State of <XXXXX>

<Project Name/Phase> (*Planning, Development, Implementation*)

STATUS REPORT

Date Ending: <MM/DD/YY>

Contents

A13.1	Status Report Checklist	608
A13.2	Cover Page	609
A13.3	Document Information	610
A13.4	Executive Summary.....	610
A13.5	Status Overview	611
A13.6	Work Accomplished	611
A13.7	Deliverables in Progress	612
A13.8	Planned Activities	612
A13.9	What is Going Well?.....	613
A13.10	Key Issues with Resolution Strategy.....	613
A13.11	Project Deliverable Status.....	613
A13.12	Open Risks	615
A13.13	Problem Areas/Risk Mitigation	616
A13.14	Project Budget and Actual Expenditures	617
A13.15	Contractor Performance Update.....	618
A13.16	Updated Project Schedule of Milestones and Deliverables.....	618



A13.3 Document Information

DOCUMENT INFORMATION

Document Title	<Project Name> <Monthly or Quarterly> Status Report
Revision Number	<#.#>
Issued by	
Issue date	<mm/dd/yyyy>
Status	Final

A13.4 Executive Summary

Provide a short summary of current project efforts and notable achievements or variances. For example:

This document covers work performed and tasks accomplished from (phase/stage) on (date) through (date). The State WIC Program is in the Implementation Phase of installation of a transferred, management information system (XXXX) to replace the state's 32-year old system. The system will be hosted within the State IT environment. WIC is also implementing a WIC Electronic Benefits Transfer (EBT) system, to be hosted externally from the State IT environment to allow WIC benefit delivery via retail grocery locations.

This project was envisioned as two phases. This status report is for Phase Two, the Implementation Phase, and builds on Phase One for which the United States Department of Agriculture Food and Nutrition Service (USDA FNS) has granted approval through acceptance of State WIC's MIS/EBT Implementation Advance Planning Document (IAPD), and has awarded implementation funding. Phase One was the Planning Phase, which will was fully described in the Planning Advance Planning Document (PAPD).



A13.5 Status Overview

STATUS OVERVIEW (EXAMPLE)

	Controlled	Caution	Critical	Reason for Deviation
SCOPE		✓		The State is awaiting further guidance on items such as Hearings and Appeals, Notices, Account Transfer, contingency planning, and other major project facets. Additionally, MAGI conversion approval and HIP waiver resolution may present late rework or scope risk.
COSTS	✓			
SCHEDULE		✓		Due to account transfer BSD delay and pending online application guidance, requirements and design are affected. Additionally, the State is awaiting aforementioned guidance.

A13.6 Work Accomplished

Provide a short Narrative

A13.6.1 Work Completed for Last Reporting Period

This section contains the worked completed from since last status report submitted on <date>.

WORK COMPLETED FOR LAST REPORTING PERIOD

ACTIVITY #	ACTIVITY NAME	PREVIOUS STATUS	CURRENT STATUS	NOTES



A13.7 Deliverables in Progress

This section provides an overview of the major milestones and or deliverables that are in progress at the time of this report.

DELIVERABLES IN PROGRESS

DELIVERABLE (MILESTONE)	WBS NUMBER	PLANNED DATE	FORECASTED DATE	STATUS
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-

A13.8 Planned Activities

This section should have a narrative of upcoming activities at the State level (meetings, reviews, JADs, testing, training, etc.) that pertain to the next reporting period.

A13.8.1 Work Planned for Next Reporting Period

This section provides an overview of the work being performed during the next reporting period.

WORK PLANNED FOR LAST REPORTING PERIOD

ACTIVITY #	ACTIVITY NAME	PREVIOUS STATUS	CURRENT STATUS	NOTES
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-



A13.9 What is Going Well?

- Stage /Gate preparations / State Gate discussions
- IEDSS IV&V support and efforts in all aspects of project activities
- SNAP/TANF paper application finalization
- Budget

A13.10 Key Issues with Resolution Strategy

May also be assessed under risks.

KEY ISSUES WITH RESOLUTION STRATEGY

Key Issue	Resolution Strategy
Vendor contracts/amendments (DDI/M&O) incomplete	The State and vendor have approved amendment 1 to the DDI contract and submitted it for approval. The State is working on negotiation of amendment 2 while focusing heavily on SOW updates. Once this amendment is finalized, then the M&O contract will be addressed.
A high number of defects persist at the end of pilot	The State is reviewing the rollout schedule to determine the impact an extension to the pilot will have on the overall project schedule. The State procurement office is reviewing the contract clause that allows for extension of the pilot period to determine the time needed to exercise the clause. The State is also evaluating the level of internal resources available for assignment if the pilot period is extended. The State has notified FNS of the potential delay and is currently comparing the vendor's application solution against the State and Federal online application guidance, and is reaching out to other states regarding guidance alignment to ensure that an appropriate resolution is in place prior to rollout.

A13.11 Project Deliverable Status

This section is a quick table, which shows the status of the project deliverables as milestones. Two different examples are provided.

**PROJECT DELIVERABLE STATUS, EXAMPLE 1**

Quarter 2 Top Milestones and In-Process Items		Baseline	New Est.	Var	State	Status	Risk ID
1	Joint Application Design sessions for IVR and Document Management are in-process.	04/30/12	N/A		Open	Green	
2	Benefit Center floor plans completed and approved for two of three planned locations. Plan approval for the final location is in-process.	04/30/12	N/A		Open	Green	
3	Procurement activities for the hardware and software required for the IVR solution are in-process.	April 2012	June 2012		Open	Yellow	88544 - Medium
4	Pre-Screening, My Account and IVR application builds (includes input screens, screen and field help, data collection, messaging speak back, and security settings) are in-process.	05/01/12	N/A		Open	Green	
5	System Testing Concludes (Deployment 1 Code)	05/01/12	N/A		Open	Green	
6	UAT Initiates (Deployment 1 Code)	05/02/12	N/A		Open	Green	
7	Deployment 1 Go Live	05/17/12	N/A		Open	Green	

PROJECT DELIVERABLE STATUS, EXAMPLE 2

Major Milestones	Original Target Date	Revised Target Date	Actual Date	Status
Planning Project				
Implementation Project				
QA RFP Approved by FNS & Posted		n/a	1/7/2013	Complete
T&I RFP Approved by FNS & Posted		n/a	2/28/2013	Complete
EBT RFP Approved by FNS & Posted		n/a	2/28/2013	Complete
QA RFP Questions due	1/23/2013	n/a	1/23/2013	Complete & answers posted

**PROJECT DELIVERABLE STATUS, EXAMPLE 2**

Major Milestones	Original Target Date	Revised Target Date	Actual Date	Status
QA Bidder's Conference	2/7/2013	n/a	2/7/2013	Complete
QA Proposals due	3/11/2013	n/a	3/12/13	Complete
T&I and EBT RFP Questions due	3/20/2013	n/a	3/20/13	Complete
T&I Bidder's Conference	4/4/2013	n/a	4/4/2013	Complete
EBT Bidder's Conference	4/11/2013	n/a	4/11/2013	Complete
QA selection	4/11/2013	n/a	4/8/2013	Complete
T&I and EBT Proposals due	5/1/2013	5/20/2013		In Progress
QA Independent Review	6/12/2013	n/a	4/8/2013	Cancelled by DII
Charter Complete & Final	1/1/2013	5/1/2013	4/29/13	Complete
QA Contracting	4/19/2013	6/3/2013		In Progress
QA Starts	8/12/2013	8/12/2013		
T&I and EBT Proposal Review	6/20/2013			
T&I and EBT selection	6/20/2013			
T&I and EBT IR	7/22/2013			
T&I and EBT Contracting	9/13/2013			
Planning Procurement ends	9/30/2013			
Kickoff	9/30/2012			

A13.12 Open Risks

This section contains a list of all open risks, risks that have occurred, or are on the verge of occurring.

OPEN RISKS

RISK #	RISK NAME	RISK DATE	STATUS



A13.13 Problem Areas/Risk Mitigation

RISK MITIGATION

RISK	MITIGATION
Key Issues	The issues presented in section A13.10 present Risks if they are not addressed timely.
Aggressive Schedule	Reallocated resources, continue to refine schedule as needed, and continue to closely monitor progress. Vendor is working at risk pending Amendment 1 finalization, and the legacy vendors (ICES and RCR – FACTS) are working along with the State to support PPACA compliance. IV&V staff on hand to help support efforts.
IAPDU Needed	Working with federal partners to ensure appropriate capture of final IEDSS-related contracts and detailed hardware/software listings/costs. Much of the IAPDU has been drafted and is pending State stakeholder review.
Lawsuit Requirements	The FACTS, ICES, and State teams are heavily engaged in activities related to lawsuit compliance. Continuing to integrate requirement sessions into compliance activities. Final items should be rolled out to production in July 2013.
Competing Priorities/Schedules for External Interface Trading Partners May Delay the Completion of Interface Design and Testing	• Define milestone dates for each trading partner interface and identify priority (according to execution frequency) of the interface. • State ESB team to proxy conversations with State-based trading partners. • Prepare contingency plans for stub testing in the event that trading partners are not ready within the testing timelines.



A13.14 Project Budget and Actual Expenditures

A short narrative should be provided for the applicable reporting period to support a table or chart. This report should include estimated budget and actual costs. Actual budget and expenditures will be submitted with the appropriate APDU. Two examples are provided:

- *Project is Over/Under Budget*
- *Cost Variance (CV): <\$###>*

COST VARIANCE

Capital Budget:	Original Forecast	Current Forecast	Expended to Date	Estimate to Completion	Variance
	\$34,429,920	\$34,429,920	\$3,155,973.61	\$31,273,946.39	0

MIS EBT IMPLEMENTATION GRANT COST AND FORECAST SUMMARY

Line Item	FY 2013				FY 2014		FY / Project Total
	Q1 Actual Cost	Q2 Actual Cost	Q3 Actual Cost	Q4 Actual Cost	Q1 Actual Cost	Q2 Actual Cost	
State Costs							
State Staff Time	2,500.23	10,215.00					
Project Contract Staff	17,171.63	40,831.00					
Hardware	16,192.00	9,451.00					
State Total	\$35,863.86	\$60,497.54					



A13.15 Contractor Performance Update

Provide a short narrative on current contractor performance – this optional information is used to assist other states when FNS is asked about contractor performance, abilities, adherence to schedule and timelines, communications, quality of deliverables, reporting and correcting errors etc.

A13.16 Updated Project Schedule of Milestones and Deliverables

This is an optional section of the report. When used in this report, include known slippages or adjustments. Actual updates to the project schedule of milestones and deliverables will be reported in the appropriate APDU.



A14. Security Plan Checklist

A14.1 Security Plan Checklist Overview

The purpose of a Security Plan Checklist is to assist the States with protecting agency information and to protect their information processing assets from theft, fraud, misuse or unauthorized modification. Information used by any business or government enterprise must be available when and where needed while being safeguarded against tampering, loss, unauthorized disclosure, denial of service, and destruction. Technical reviewers and developers of security plans in State agencies will use the Security Plan Checklist (SPC) based on guidance from the National Institute of Standards and Technology (NIST)¹³¹, Federal Information Processing Standards (FIPS)¹³², and USDA/FNS guidance.

Not all items on the SPC are mandatory, but each major section should be addressed. In accordance with the NIST Handbook, the major IT security Controls addressed are:

- Management Controls
- Operational Controls
- Technical Controls
- Privacy Controls
- Electronic Benefits Transfer (EBT) Specific Controls

Each control has related security subgroups in this checklist. Use of the checklist during the development or upgrade of an IS Security Program will provide the State with a basic understanding of what security controls should be put into place. The checklist will provide guidance on further development, and maintaining a secure computing environment.



A14.2 System Identification

SYSTEM IDENTIFICATION

✓	ITEM TO BE INCLUDED
	System Name and Title
	Responsible Organization- Organization responsible for system operation.
	System Owner- Name, title, agency, address, phone number, email address.
	Authorizing Official- Senior management official who has authority to accredit the system and accept residual risk associated with the system.
	Designated Points of Contact- Other key personnel who can address system information.
	Assignment of Security Officer- Individual responsible for the system security.
	System Category- Major application or general support system.
	Application Categories, describe how they are integrated with your system- • Information access - hypertext, multimedia, soft content and data • Collaboration – newsgroups, shared documents, videoconferencing • Transaction processing – internet commerce or business, links to legacy systems
	System Status- Under development, operational, or undergoing a major modification.
	General Description/Purpose- Describe briefly (one to three paragraphs) the function and purpose of the system.
	Functions you are using the internet to perform- Data transfer, forms-based data entry, browser-based interactive applications, etc. Describe briefly.



SYSTEM IDENTIFICATION

✓	ITEM TO BE INCLUDED
	System Environment- Describe briefly the technical system including any environmental or technical factors that raise special security concerns, such as PDA's, wireless technology, etc.
	System Interconnection/Information Sharing- List each system interface or interconnection: • Name of system • Organization • Type of interconnection (internet, dial-up, etc.) • Authorizations for interconnection (MOU/MOA, etc.) • Date of agreement • Name and title of authorizing official(s)

A14.3 Sensitivity of Information Handled

SENSITIVITY OF INFORMATION HANDLED

✓	ITEM TO BE INCLUDED
	The degree of sensitivity of information/data generated or accessed by the system is described, considering the requirements for: • Confidentiality – Preserving authorization restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. • Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. • Availability – Ensuring timely and reliable access to and use of information.
	Minimum safeguards for protecting Personal Identifiable Information (PII) as required by the Office of Management and Budget guidance for protecting PII in memoranda M-06-15 and M-06-16 , "Protection of Sensitive Agency Information" are described.
	Identify and describe the following information sensitivity elements: • Applicable laws and regulations that require protection of sensitive information • A description of the data sensitivity • Data protection requirements for integrity, confidentiality, and availability



SENSITIVITY OF INFORMATION HANDLED

✓	ITEM TO BE INCLUDED
	System Security Measures – The system security measures in-place or planned that is intended to meet the protection requirements of the system. Security control measures should also be explained in general terms regarding the system are described.

A14.4 Management Controls

Focus on the management of the information system and the management of risk for a system. They are techniques and concerns normally addressed by management driven by policy and process.

Identify and document the processes and procedures for the following.

MANAGEMENT CONTROLS

✓	ITEM TO BE INCLUDED
	Establish configuration controls for reviewing and approving security changes made to the system hardware, software, and application(s).
	Create procedures for reporting security incidents or irregularities (e.g., virus, hackers, software bugs).
	Designate a security manager responsible for overseeing the security program.
	Assign responsibility for computer security at each office or site.
	Ensure security activities are incorporated into the security program, including: • Incorporate security specifications in the system design documents • Conduct risk assessments and system security reviews ○ Ensure the risk analysis measures vulnerability related to fraud or theft or loss of data and harm to agency activities ○ Ensure risk analyses are conducted whenever there is a significant change to the physical facility, hardware, or operating system and application software • Develop appropriate security documentation such as contingency plans, risk assessment report, security plan and updates as required



MANAGEMENT CONTROLS

✓	ITEM TO BE INCLUDED
	• Ensure corrective actions are effectively implemented
	Develop and use change control procedures as programs progress through testing to final approval.
	Determine the owner of sensitive or confidential data. Periodically verify with the owner of the data who has access to this data.
	Develop and enforce privacy policies for employees.

A14.5 Operational Controls

Address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and rely upon management activities as well as technical controls.

OPERATIONAL CONTROLS

PERSONNEL SECURITY	
✓	ITEM TO BE INCLUDED
	Duties are separated to ensure individual accountability.
	Distinct systems support functions are performed by different individuals.
	A process is developed and enforced for requesting, establishing, issuing, and closing user accounts: • Security is notified within a reasonable period of time of the termination and hiring of employees • User accounts for terminated employees are closed with access rights deleted within a specific (short) period of time • User accounts for new hires are opened and access granted according to supervisory designated rights within a specific (short) period of time



OPERATIONAL CONTROLS

PERSONNEL SECURITY	
✓	ITEM TO BE INCLUDED
	• When an employee is terminated, access is denied to the system and any data, program listings, procedure manuals, and other employees are informed of the termination • Manager periodically reviews authorized users and their access authorities, making necessary changes
	The delegation and maintenance of user access and passwords is limited to a select number of people.

OPERATIONAL CONTROLS

PHYSICAL AND ENVIRONMENTAL PROTECTION	
✓	ITEM TO BE INCLUDED
	Access to facilities is controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics.
	Visitor access to facilities is controlled and monitored.
	Management regularly reviews the list of persons with physical access to sensitive facilities.
	Deposits and withdrawals of storage media authorized and logged.
	Appropriate fire suppression and prevention devices are installed and working.
	Emergency procedures are documented and employees are familiar with the procedures.
	Computer monitors are located to eliminate viewing by unauthorized persons.
	Physical access to data transmission lines is controlled.



OPERATIONAL CONTROLS

PHYSICAL AND ENVIRONMENTAL PROTECTION	
✓	ITEM TO BE INCLUDED
	Sensitive data files are encrypted on all portable systems.
	Portable systems are stored securely.
	Equipment located in areas accessible to clients and/or the public are properly secured to prevent tampering or accidental interruption of service.
	Telecommunications closets and/or server areas are secured at all times.
	The system automatically logs off a user after a specified period of inactivity.
	Users logoff or turn off their computers/workstations when they will be away from an extended period of time.
	Computers/workstations, servers and telecomm closets are kept clean and free of dirt, dust, and food.
	Components are protected by surge protectors or line conditioners.
	A Uninterruptable Power Supply (UPS) is available and tested periodically.
	Users receive periodic training on emergency procedures and good housekeeping practices.

OPERATIONAL CONTROLS

CONFIGURATION MANAGEMENT	
✓	ITEM TO BE INCLUDED
	Organization develops, documents, and maintains under configuration control a current baseline configuration of the information system.



OPERATIONAL CONTROLS

CONFIGURATION MANAGEMENT	
✓	ITEM TO BE INCLUDED
	Organization determines the types of changes to the information system that are configuration controlled; approves changes to the system with explicit consideration for security impact analysis; documents approved changes, retains and reviews records of changes, audits activities associated with changes, and coordinates and provides oversight for configuration change control activities through committee or board that convenes on a regularly defined basis.
	Organization conducts security impact analysis of changes to the system to determine potential security impacts prior to change implementation.
	Organization establishes and documents mandatory configuration settings for information technology products employed within the information system using defined security configuration checklists.
	Organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of a defined set of prohibited or restricted functions, ports, and/or services.
	Organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures.

OPERATIONAL CONTROLS

INPUT/OUTPUT CONTROLS	
✓	ITEM TO BE INCLUDED
	There is a help desk or group that offers advice and assistance.
	Processes exist for the handling, distributing, and storing of output containing sensitive information.
	Processes exist to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.



OPERATIONAL CONTROLS

CONTINGENCY PLANNING	
✓	ITEM TO BE INCLUDED
	Critical data files and operations are identified and the frequency of file backup documented.
	Processing priorities been established and approved by management.
	A comprehensive contingency plan been developed and documented.
	There are detailed instructions for restoring operations.
	There is an alternate processing site. (Identify location)
	The location of stored backups is identified.
	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged.
	System and application documentation is maintained at the off-site location.
	The backup storage site and alternate site are geographically removed from the primary site. They are physically protected.
	Tested contingency/disaster recovery plans are in place.
	The plan is periodically tested and readjusted as appropriate.
	An incident response policy and procedure is defined, documented, and implemented.
	Organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training on a defined frequency.



OPERATIONAL CONTROLS

CONTINGENCY PLANNING	
✓	ITEM TO BE INCLUDED
	Organization implements an incident handling capability for security incidents.
	Organization tracks and documents information system security incidents.

OPERATIONAL CONTROLS

HARDWARE AND SYSTEM SOFTWARE MAINTENANCE	
✓	ITEM TO BE INCLUDED
	A formal, documented information system maintenance policy exists and is implemented.
	Access is limited to system software and hardware.
	Organization schedules, performs, documents, and reviews records of maintenance (controlled maintenance) and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; controls all maintenance activities (on-site or remote).
	Organization approves controls, monitors the use of and maintains information system maintenance tools.
	Organization obtains maintenance support and/or spare parts for a defined list of security-critical information system components and/or key information technology components within a defined time period of failure.
	All new and revised hardware and software is authorized, tested, and approved before implementation.
	Software change request forms are used to document requests and related approvals.
	Controls are adequate to restrict access to the database and database utilities.



OPERATIONAL CONTROLS

HARDWARE AND SYSTEM SOFTWARE MAINTENANCE	
✓	ITEM TO BE INCLUDED
	The type of test data to be used is specified, i.e., live or made up.
	Software distribution implementation orders including effective date provided to all locations exist.
	Version control is implemented.
	Contingency plans and other associated documentation are updated to reflect system changes.
	Systems are periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe calls).

OPERATIONAL CONTROLS

DATA INTEGRITY	
✓	ITEM TO BE INCLUDED
	Virus detection and elimination software is installed and activated.
	Firewalls and/or proxy servers used and their software are described.
	The level of data encryption used, if any, and whether it is hardware or software-based is described.
	The application languages being used (HTML, XML, JavaScript, etc.) and whether they are static, semi-dynamic, or dynamic is described.
	Database connectivity and any APIs being used is described.
	Hardware and software, if using separate web servers, is described.



OPERATIONAL CONTROLS

DATA INTEGRITY	
✓	ITEM TO BE INCLUDED
	The controls in place for shared resources including any of the following are described: • Password protection • User groups • Smartcards • Biometrics • Virus Scanners • Vulnerability scanners • Intelligent agents
	Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.
	Inappropriate or unusual activity is reported, investigated, and appropriate actions taken.
	Procedures are in place to determine compliance with password policies.
	Intrusion detection tools are installed on the system.
	Penetration testing is performed on the system.
	Message authentication is used.
	All system and data accesses are logged.



OPERATIONAL CONTROLS

DOCUMENTATION	
✓	ITEM TO BE INCLUDED
	There is sufficient documentation that explains how software/hardware is to be used.
	There is application documentation for in-house applications.
	There are network diagrams and documentation on setups of routers and switches.
	Software and/or documentation is properly logged, checked out, and locatable at all times.
	There are software and hardware testing procedures and results.
	There are user manuals.
	There are backup procedures.

OPERATIONAL CONTROLS

SECURITY AWARENESS, TRAINING, AND EDUCATION	
✓	ITEM TO BE INCLUDED
	Employees receive adequate training to fulfill their security requirements.
	There is mandatory annual refresher training.



OPERATIONAL CONTROLS

INCIDENT RESPONSE CAPABILITY	
✓	ITEM TO BE INCLUDED
	The capability exists to provide help to users when a security incident occurs in the system.
	Incidents are monitored and tracked until resolved.
	Personnel are trained to recognize and handle incidents.
	Incident information and common vulnerabilities or threats is shared with owners of interconnected systems.

A14.6 Technical Controls

Focus on controls the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. These controls should be consistent with the defined security management of the State or agency.

TECHNICAL CONTROLS

IDENTIFICATION AND AUTHENTICATION	
✓	ITEM TO BE INCLUDED
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance; and formal procedures to facilitate the implementation of the policy and associated controls.
	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of users).
	The organization manages information system identifiers for users and devices by receiving authorization from a designated organizational official to assign a user or device identifier, selecting an identifier that uniquely identifies an individual or device, assigning the user identifier to the



TECHNICAL CONTROLS

IDENTIFICATION AND AUTHENTICATION	
✓	ITEM TO BE INCLUDED
	intended party or device; preventing reuse of user or device identifiers and disabling user identifiers after a defined period of inactivity.
	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
	Users are individually authenticated via passwords, tokens, or other devices.
	Emergency and temporary access may be authorized.
	Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain system access.
	Passwords are changed at least every 90 days. (state # of days).
	Passwords are unique and difficult to guess (alpha/numeric, special characters). Provide password schema.
	Inactive user IDs are disabled after a specified period of time.
	Passwords are distributed securely and users informed not to reveal their passwords to anyone (social engineering).
	Vendor-supplied passwords are replaced immediately.
	There is a limit to the number of invalid access attempts that may occur for a given user. (state limit).
	Access controls enforce segregation of duties.



TECHNICAL CONTROLS

IDENTIFICATION AND AUTHENTICATION	
✓	ITEM TO BE INCLUDED
	Data owners periodically review access authorizations to determine whether they remain appropriate.
	Are user logons/passwords challenged frequently and under a multi-level protection scheme?
	Do you allow synchronization of passwords for single sign-on?
	Describe the number of staff that have administrative rights to the application, telecomm, and web servers and how access rights are separated.
	User profiles/roles and permissions protocol to be used are described.
	The system uniquely identifies and authenticates a defined list of specific and/or types of devices before establishing a connection.

TECHNICAL CONTROLS

LOGICAL ACCESS CONTROLS	
✓	ITEM TO BE INCLUDED
	Communication protocols being used (FTP, HTTP, Telnet, etc.) are described.
	Access controls are described: • Identification and authorization • Sensitive and privacy • No repudiation • Data integrity
	How the organization develops, disseminates, reviews/updates a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance is described.



TECHNICAL CONTROLS

LOGICAL ACCESS CONTROLS	
✓	ITEM TO BE INCLUDED
	How the organization manages information system accounts is described, including: identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
	How logical access controls restrict users to authorized transactions and functions is described.
	Separation of Duties of individuals as necessary to prevent malevolent activity without collusion; document separation of duties, and implements separation of duties through assigned system access authorizations.
	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
	The information system enforces a limit of consecutive invalid access attempts by a user during a defined period.
	The information system displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws.
	Access to security software is restricted to security administrators.
	The information system limits the number of concurrent sessions for each system account to a defined number.
	How workstations disconnect or screen savers lock system after a specific period of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication is described.
	Any encryption used and what type is used.
	Access is restricted to files at the logical view or field.
	Logical controls over network access are described.



TECHNICAL CONTROLS

LOGICAL ACCESS CONTROLS	
✓	ITEM TO BE INCLUDED
	Controls that restrict remote access to the system are described.
	If the network connection automatically disconnects at the end of a session is described.
	Firewalls or secured gateways installed are described.
	If the public accesses the system, controls implemented to protect the integrity of the application and the confidence of the public are described.
	A privacy policy posted on the web site.
	The organization documents allowed methods of remote access to the information system; establishes usage restrictions and implementation guidance for each allowed method; monitors for unauthorized remote access; authorizes remote access prior to connection; and enforces requirements for remote connections.
	The organization establishes usage restrictions and implementation guidance for wireless devices and for organization-controlled mobile devices; authorizes connection; monitors for unauthorized access; and enforces organizational policies and procedures.
	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store and/or transmit organization-controlled information using external information systems.

TECHNICAL CONTROLS

AUDIT TRAILS AND ACCOUNTABILITY	
✓	ITEM TO BE INCLUDED
	Activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated.



TECHNICAL CONTROLS

AUDIT TRAILS AND ACCOUNTABILITY	
✓	ITEM TO BE INCLUDED
	Off-line storage of audit logs is retained for a period of time. How access to these logs is strictly controlled is described.
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, and management commitment, coordination among organizational entities, and compliance; and formal documented procedures to facilitate the implementation of audit and accountability policy and associated audit controls.
	Organization determines, based on a risk assessment and mission/business needs, the system must be capable of auditing a defined list of auditable events; coordinates the security audit function with other organizational entities; and based on current threat information and ongoing risk assessment that the events are to be audited within the information system.
	Produces audit records that contain sufficient information, at a minimum, to establish what type of event occurred, when (date and time) the event occurred, where, the source of the event, and the outcome (success or failure), and the identity of any user/subject associated with the event.
	The information system provides an audit reduction and report generation capability.
	The information system uses internal system clocks to generate time stamps for audit records.
	The information system protects against an individual falsely denying having performed a particular action (non-repudiation).
	Audit records are retained for a defined period of time consistent with records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
	The organization monitors open source information for evidence of unauthorized ex-filtration or disclosure of organizational information on a defined frequency.
	The information system provides the capability to capture/record and log all content related to a user session; and remote hear/view all content related to an established user session in real time.



TECHNICAL CONTROLS

SYSTEM AND COMMUNICATIONS PROTECTION	
✓	ITEM TO BE INCLUDED
	Organization develops, disseminates, and reviews/updates on a defined frequency a formal system and communications protection policy that addresses purpose, scope, roles, responsibilities, coordination among organizational entities, and compliance.
	Information system separates user functionality (including user interface services) from information system management functionality.
	Information system isolates security functions from non-security functions.
	Information system prevents unauthorized and unintended information transfer via shared system resources.
	Information system prevents against or limits the effects of a defined list of denial of service attacks.
	Information system limits the use of resources by priority.
	Information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and connects to external networks or information systems only through managed interfaces consistent of boundary protection devices arranged in accordance with organizational security architecture.
	Information system protects the integrity of transmitted information.
	Information system terminates the network connection associated with a communications session at the end of the session or after a defined period of activity.
	Information system protects the confidentiality of transmitted information.
	Information system establishes a trusted communications path between the user and the defined security functions of the system to include at a minimum, information system authentication and re-authentication.
	Information system protects the integrity and availability of publicly available information and applications.



TECHNICAL CONTROLS

SYSTEM AND COMMUNICATIONS PROTECTION	
✓	ITEM TO BE INCLUDED
	Information system prohibits remote activation of collaborative computing devices with a list of defined exceptions where remote activation is to be allowed; and provides an explicit indication of use to users physically present at the devices.
	Information system associates security attributes with information exchanged between information systems.
	Organization defines acceptable and unacceptable mobile code and technologies, establishes restrictions and implementation guidance for acceptable code and technologies, and authorizes, monitors, and controls the use of mobile code within the information system.
	Organization establishes usage restrictions and implementation guidance by Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and authorizes, monitors, and controls the use of VoIP within the information system.
	Information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
	Information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems (recursive or caching resolver).
	Information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
	Information system fails to a defined known-state for defined types of failures preserving defined system state information in failure.
	Organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.
	Information system loads and executes the operating environment from hardware-enforced, read-only media; and loads and executes defined applications from hardware-enforced, read-only media (non-modifiable executable programs).



A14.7 Privacy Controls

Policy and procedural controls that govern the collection, use, storage, sharing, and disposal of personally identifiable information by staff and contractors. These controls should demonstrate compliance with applicable law, policies, and regulations. Additionally, they should provide transparency to the public in how the information is being protected and used.

PRIVACY CONTROLS

AUTHORITY AND PURPOSE	
✓	ITEM TO BE INCLUDED
	Determine and document the legal authority that permits collection, use, maintenance, and sharing of personally identifiable information (PII).
	Describe the purpose(s) for which PII is collected, used, and maintained. Share this in privacy notices.

PRIVACY CONTROLS

ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT	
✓	ITEM TO BE INCLUDED
	Appoint an officer accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations for the collection, use, maintenance, sharing, and disposal of PII.
	Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures.
	Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls.
	Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.
	Conduct Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any organizational procedures.
	Establish privacy roles, responsibilities, and access requirements for contractors, and service providers.



PRIVACY CONTROLS

ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT	
✓	ITEM TO BE INCLUDED
	Include privacy requirements in contracts and other acquisition-related documents.
	Establish monitoring and audits of privacy controls and internal privacy policy to ensure effective implementation.
	Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures.
	Have personnel certify acceptance of responsibilities for privacy requirements.
	Establish an accurate accounting of disclosures of information including: • Date, nature, and purpose of each disclosure • Name and address of the person or agency to which the disclosure was made
	Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer.
	Make the accounting of disclosures available to the person named in the record upon request.
	Design information systems to support privacy by automating privacy controls.
	Regularly update privacy plans, policies, and procedures.



PRIVACY CONTROLS

DATA MINIMIZATION AND RETENTION	
✓	ITEM TO BE INCLUDED
	Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of the collection.
	Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.
	Conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
	Retain each collection of PII for only the defined period to fulfill the purpose identified in the notice or as required by law.
	Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with the approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.
	Develop policies and procedures that minimize and protects the use of PII for testing, training, and research.

PRIVACY CONTROLS

INDIVIDUAL PARTICIPATION AND REDRESS	
✓	ITEM TO BE INCLUDED
	Provide a means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection.
	Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.
	Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.
	Ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.



PRIVACY CONTROLS

INDIVIDUAL PARTICIPATION AND REDRESS	
✓	ITEM TO BE INCLUDED
	Provide individuals the ability to have access to their PII.
	Publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records and access procedure in System of Records Notices.
	Adhere to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
	Provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended as appropriate.
	Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended.
	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

PRIVACY CONTROLS

TRANSPARENCY	
✓	ITEM TO BE INCLUDED
	Provide effective notice to the public and the individuals regarding: • Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII • Authority for collecting PII • The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices • The ability to access and have PII amended or corrected if necessary



PRIVACY CONTROLS

TRANSPARENCY	
✓	ITEM TO BE INCLUDED
	Describe: • The PII the organization collects and the purpose(s) for which it collects that information • How the organization uses PII internally • Whether the organization shares PII with external entities, the categories of those entities, and the purposes for sharing • Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent • How individual may obtain access to PII • How the PII will be protected
	Revise public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.
	Include Privacy Act Statements on forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.
	Ensure that the public has access to information about privacy activities and is able to communicate with the privacy officer.
	Ensure that privacy practices are publicly available through organizational websites or otherwise.

PRIVACY CONTROLS

USE LIMITATION	
✓	ITEM TO BE INCLUDED
	Ensure that the organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices
	Only share PII externally, for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes.

**PRIVACY CONTROLS**

USE LIMITATION	
✓	ITEM TO BE INCLUDED
	Where appropriate enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.
	Monitor, audit, and train staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.
	Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

A14.8 EBT Controls

State agencies are required to implement and maintain comprehensive security programs for all information systems involved in administering SNAP. In addition to the [7 CFR 277.18\(m\)](#)¹³³ requirements, there are additional requirements specific to EBT systems in [7 CFR 274.8\(b\)\(3\)](#).¹³⁴ This includes “A separate EBT security component shall be incorporated into the State agency Security Program for Automated Data Processing (ADP) systems where appropriate as prescribed under §277.18(m) of this chapter.”¹³⁵

Endnotes

¹³¹ US Department of Commerce, National Institute of Standards and Technology Information Technology Laboratory, Computer Security Resource Center (CSRC), (Washington, DC - 2015), <http://csrc.nist.gov/about/>.

¹³² US Department of Commerce, National Institute of Standards and Technology Federal Information processing Standards Publications (FIPS PUBS), (Washington, DC - 2015), <http://www.nist.gov/itl/fips.cfm>.

¹³³ “Information system security requirements and review process”, 7 CFR 277.18 (m), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=878cf8331a8f255a7cf31df85714ecf9&mc=true&node=se7.4.277_118&rgn=div8

¹³⁴ “Functional and technical EBT system requirements: System Security”, 7 CFR 274.8 (b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=a18b73a0c670d409f4080b898a333f48&mc=true&node=se7.4.274_18&rgn=div8

¹³⁵ “System Security”, 7 CFR 274.8(b)(3), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=a18b73a0c670d409f4080b898a333f48&mc=true&node=se7.4.274_18&rgn=div8

A15. Final Test Plan Template

A15.1 Introduction

The Food and Nutrition Service (FNS) Handbook 901 Chapter 6 describes the activities required for preparing an effective comprehensive test plan based on FNS testing requirements and industry best practices. It also includes information on the minimum requirements for the “Complete and Final Test Plan” FNS requires for submission prior to beginning the User Acceptance Test (UAT).



“Chapter 6 – Test Planning” and this appendix use the term “Complete and Final Test Plan” to distinguish it from the use of “test plan,” which is a general term or refers to the State agency’s comprehensive test plan.

The “Complete and Final Test Plan” has very specific content requirements that are based on the details found in the State agency’s comprehensive test plan.

FNS does not require a specific format for the “Complete and Final Test Plan.” The State agency may submit the test plan developed for its own use, as long as FNS can find all the required information. However, this appendix provides a suggested template to build the “Complete and Final Test Plan.”

Refer to chapter **6.0 Test Planning**, along with this appendix, to build a “Complete and Final Test Plan” that addresses FNS testing requirements. All data provided in this template is an example of the content that could be included in the “Complete and Final Test Plan”. However, it should not be used “as-is.” Information and data in any test plan should represent thorough test planning and should contain specifics unique to the State agency.



Chapter **6.0 Test Planning** should be used as a reference for additional guidance to produce this “Complete and Final Test Plan.”

A15.1.1 Summary of Final Test Plan Contents

The following list of minimum required components of the “Complete and Final Test Plan” includes cross-references to chapter **6.0 Test Planning** where additional information can be found.

- Timeline/Milestones (see section **6.4.4**)



- Testing Resources (see section **6.4.3**)
 - Staffing with Roles and Responsibilities (see section **6.4.3.2**)
 - Test Environment and Equipment – Itemized list (see section **6.4.3.2**)
- Test Approach (see section **6.4.1**)
- Items to Be Tested (see section **6.5.1**)
- Data Conversion (if required) (see sections **6.1.3** and **6.3.4**)
- System Security (see section **6.1.3**)
- Stress/Load Testing (see section **6.1.3**)
- Issue/Defect Tracking and Prioritization – At a minimum FNS expects to see these defect levels identified:
 - Defect Resolution process (see section **6.4.2**)
 - Regression Testing process (see section **6.1.3**)
 - Evaluation of Test Progression (see section **6.4.1**)
 - Go/No-Go Decisions (see section **6.4.7**)
- Roll Back Contingency Plan (see section **6.9.1**)
- Risk Management (see section **6.4.5**)

A15.1.2 How to Use This Template

Beginning with section **A15.2-Template for Test Plan Contents**, there will be three text styles used throughout the template. Each style communicates different elements of the template and are to be used in different ways.

1. **Guidance Text – Calibri font, Bold, Italic, Blue**
 - a. *This style represents descriptions, instructions, guidance, information, and suggestions made to State agencies of what to include in a particular section of the “Complete and Final Test Plan”.*
 - b. *This text is not to be included in a “Complete and Final Test Plan”.*
2. **Fill-In Data – Calibri font, Bold, Plum**
 - a. This style represents Information or data the State agency needs to “fill-in” based on its testing requirements.
 - b. The data presented in this style is generic. Numbers are presented as <#>, proper nouns are presented in descriptive terms (e.g. <City Name, State Name>), and dates are presented as <MM/DD/YYYY> or <Date>.
 - c. All individual fill-in data elements are separated by <brackets>.
3. **Sample Text – Times New Roman font, Black**
 - a. This style represents example language or concepts that apply to the section.

- b. While this is language that would normally be included in a test plan, it should be updated or changed to correct information representative of the State agency's testing planning and procedures.
- c. In some cases, the **<fill-in data style>** will be used concurrently within sample text.



This appendix provides a template only; it is not the "Complete and Final Test Plan." All data and examples are notional and should be replaced by data from decisions made after the appropriate test planning process for your project.

A15.2 Template for Test Plan Contents

A15.2.1 Scope and Purpose

This section of the "Complete and Final Test Plan" should briefly describe the system being tested and the scope of the testing (e.g., UAT, Pilot). For the system overview, describe the system under test in high-level component terms, including software and hardware.

The purpose of the test should briefly describe why the test is being conducted (e.g., complete system or testing of enhancements only). A brief statement should summarize or reference other sections in the Test Plan including items to be tested, resources needed, the configuration under test, limitations, and assumptions.

A15.2.2 Timeline/Milestones

FNS guidance for the minimum set of milestones in the "Complete and Final Test Plan" includes:

- Preliminary test plan submitted with the initial IAPD package
- Pre-testing validation of all functional requirements (System Integrity Review Tool)
- Individual development test milestones (e.g., Unit Testing, Integration Testing, End-To-End Testing, Performance Testing, Systems Testing)
- System accepted for UAT (meaning that the system meets the State agency's testing entrance criteria, including passing earlier testing phases conducted by the developer)
- Test environment definition (including facility, equipment, interfaces, security)
- Known and Potential test resource conflicts (equipment, facilities, people)
- Training on system and on test procedures



- User Acceptance Testing
- UAT Evaluation performed by the State agency (FNS concurrence required) (See section **6.4.7 Go/No-Go Decision Process**)
- Pilot to include data conversion/migration/preparation plan
- Pilot Evaluation performed by the State agency (See section **6.4.7 Go/No-Go Decision Process**)
- Statewide Rollout (FNS approval required)

The timeline will need to have multiple functional iterations if an agile development process is being used.

A15.2.3 Test Schedule

Estimate how long it will take to complete the testing phase by providing a detailed schedule of test activities. Some factors to consider include:

- *All test cases prepared need to be executed at least once*
- *If any defects are found, the defect must be documented and resolved*
- *Regression testing for defects and effect on overall schedule*

The test schedule should be focused on the current testing effort (unit, integration, regression) as defined in the scope. Assuming there is limited time dedicated to complete the desired testing effort, the test schedule may be defined as a constraint to testing. If test time is limited, it should be known ahead of time and documented either in this “Complete and Final Test Plan” or as a risk to test completion.

Table 58 defines the scheduled activities for UAT. Each task will include data for start/stop dates, estimated time duration, estimated numbers of test staff required, training status, and time duration the test system will be utilized. Roles and responsibilities of the testing participants are defined in **Section A15.2.4.1 Staffing with Roles and Responsibilities**.

Table 58: Example of Test Schedule

Test Activity	Start-Stop Dates	Total Duration	# of Test Participants	Training Status	Total System Time Utilized
Functional Test	<mm/dd/yyyy>	<Total weeks>	<#>	Completed	<Total hours>
Data Conversion Test (Data transfer)	<mm/dd/yyyy>	<Total weeks>	<#>	In progress	<Total hours>
Performance Test (Data speed transmission)	<mm/dd/yyyy>	<Total weeks>	<#>	Not started	<Total hours>



A15.2.4 Testing Resources

This section describes the resources needed to conduct the test. If these resources cannot be provided as planned, a risk to the project should be documented. Mitigations for each risk should be developed in accordance with the risk management plan. This may mean that either an alternative solution will be required, or that the testing requirements should be revisited.

A15.2.4.1 Staffing with Roles and Responsibilities

Provide an organization chart for the entire test team detailing names, organization, and test responsibilities. Also, provide a list or table for all staff members and training needs for the test event.

<Provide a test organization chart here>

Table 59 describes the primary roles and responsibilities for team members participating in testing and acceptance activities.

Table 59: Example of Test Staffing and Training Table

Role	Team Member	Responsibilities	Training Needed
Test Manager	State Agency Management (as appropriate)	Provide daily test status. Observe test events. Make intermediate decisions using Suspension Resumption criteria. Determine Daily Test Schedule.	Test Manager training if available. Detailed familiarity with the test environment and design of the software.
Application Test Analyst	Contractor/Developer Team	Test to validate the infrastructure / application for function testing. Perform proper defect tracking (identification, fixing, re-testing, and migration of defects). Follow the testing scenarios/scripts, standards, guidelines, and testing methodology as specified in the testing approach. Document outcome of each test. Review test results to validate that they meet the entry and exit criteria.	Training in industry standard testing techniques. Detailed familiarity with the environment, and design of the software.



Table 59: Example of Test Staffing and Training Table

Role	Team Member	Responsibilities	Training Needed
IT Specialist Subject Matter Expert Super User	State Agency	Test to validate the infrastructure / application for function testing. Perform proper defect tracking (identification, reporting, and re-testing). Follow the testing scenarios/scripts, standards, guidelines, and testing methodology as specified in the testing approach. Document outcome of each test. Review test results to validate that they meet the entry and exit criteria.	Training in industry standard testing techniques. Detailed knowledge of business functions system is supposed to support. Detailed familiarity with the environment and design of the software.
Test Leads	Contractor Team, State Agency staff	Authority and accountability for all work performed by the specific Test Teams (e.g., functional, integration, performance, UAT). Primary responsibility for the Test and Acceptance Plan, Test Cases, Test Scripts and Expected Results, Defect Tracking Report, User Acceptance Function Test (UAT), Stress Test, Acceptance Reports, and Pilot Acceptance Report deliverables. Contractor Team Test Lead Serves as the primary contact with the State on testing issues.	Training in industry standard testing techniques. Project Management. Configuration Management. Quality Control. Detailed familiarity with the environment and design of the software.
Tester	State Agency staff	Follow test scripts, as written, per their training, and document the results. Document outcome of each test. Review test results to validate that they meet the entry and exit criteria.	Training on how to perform test scripts and document outcomes. Training to recognize when a given script succeeds or fails.



A15.2.4.2 Test Environment

The test environment should replicate the production system as closely as possible. The definitions of the test environment and supporting equipment are as follows: Each item in the list should be described and have milestone dates for completion. Facility items should have milestone dates for definition, purchase, integration, check out, and scheduling for test.

- *Test Hardware (each component)*
- *Test interfaces to other systems*
- *Application software*
- *Test tools pre-test and post-test (developed and Off-the-Shelf)*
- *Facility*
 - *Space required*
 - *Power required*
 - *Air Conditioning required*
 - *Fire and Safety equipment required*
 - *Equipment (tables, desks, phones, computers, printers, chairs, internet connections)*

A15.2.4.3 Support Software

Identify any software required to support testing when it is not a part of the system being tested. The tool identification should include the name of the product, the version number planned on being used, and its function. Include tools that provide:

- *Systems support*
- *Communications*
- *Applications*
 - *DBMS*
 - *Office Productivity software (i.e., word processor, spreadsheet, presentation, e-mail, etc.)*
 - *Requirements tracking*
 - *Server formatting*
 - *Internet browser*
- *Recording and storage for data and media*
- *Scripts generation*
- *Defect reporting*



Table 60: Example of Support Software Description

Software	Function	Version Used for Test
• <word processor> • <spreadsheet processor>	• Produce test documentation • Produce test cases and procedures	<version>
<software name>	Software Requirements Tracking	<version>
Internet Explorer	Internet Data Input	<version>
<software name>	Policy Testing Component	<version>
<software name>	Defect Management	<version>

A15.2.5 Test Approach

The test approach is a descriptive statement about how the items will be tested for each item listed in A15.2.8 Items to be Tested.

The test approach for each of the items to be tested (see section **A15.2.8**) follows:

- Database generation test:
 - Will be conducted first as a standalone test without any interface to the application undergoing test or the internet. This will verify that the database can be generated and formatted as designed.
 - If this test is successful, then any change that corrupts the database after interface connection will be external to the database and not the generation capability.
- Security testing for passwords:
 - Will check for both valid and invalid passwords. A set of rules will be established for minimum and maximum length of passwords, the valid and invalid types of characters allowed for password definition, the maximum time for password validity, and rules for reuse of previous passwords.
 - Tests will be generated to check system response to both valid and invalid password recognition.
 - Password encryption will be enforced and file data retaining passwords will be checked for formatting.
- Testing of Notices:
 - Will be conducted during integration testing. Specific test cases will be generated containing known prerequisite data that cause a change in eligibility or benefits (e.g., changes in the ages of children, changes in income, changes in expenses, and time expiration of certification periods).
 - Each test will generate a Notice to the HH and match the results of the test against the data produced on the Notice.



A15.2.5.1 Entry / Exit Criteria

Entry criteria are the minimum set of conditions that should be complete in order to start the testing work. These are not the same as Go/No-Go criteria and are not the basis for getting FNS concurrence for UAT and approval for roll-out after the Pilot. (See section 6.4.1.1 for a description of why **Entry / Exit Criteria** are different than Go/No-Go criteria.) Entry criteria are documented and signed off during the test planning phase and are included in the relevant test cases depending on the items to be tested. These criteria should be agreed upon by the State agency as early as possible, knowing that they may be subject to controlled changes as the details of the project become clearer.

The entry criteria for UAT are listed below. If any of the conditions specified in the entry criteria cannot be met, an alternative plan of action will be recommended and approved prior to starting the test.

Examples of some typical entry criteria items for UAT:

- An approved test plan is available
- Approved test cases, test scripts, and test data are available
- All test hardware platforms have been successfully installed, configured, and are functioning properly
- No critical or major severity issues remain from previous testing
- Training has been completed
- Site readiness is completed
- A person is designated with authority to approve the alternative plan or waive the incomplete entry item

Exit criteria are the minimum set of conditions that must be met to successfully close a particular test phase. Exit criteria are documented and signed off during the test planning phase and are included in the relevant test cases. These criteria should be agreed upon by the State agency as early as possible, knowing that they may be subject to controlled changes as the details of the project become clearer.

The exit criteria for UAT are listed below. If any of the conditions specified in the exit criteria cannot be met, a recovery plan of action will be recommended.

Examples of some typical exit criteria items for UAT:

- Successful execution of Test Scripts is complete
- No open issues exist unless the issue is determined to be low impact, low risk. To be reviewed with Project Manager, Test Manager, and Development Team for acceptable resolution
- A certain level of requirements coverage has been achieved
- All high-risk areas have been fully tested, with only minor residual risks left outstanding
- Data conversion match rate target(s) have been met



A15.2.5.2 Pass / Fail Criteria

Once the testing entrance criteria are satisfied and testing commences, there must be criteria for when test cases and test scripts pass or fail. One of the main exit criteria is successful completion of testing, typically based on tests passing or failing.

- *A test passes if the system responds in a manner as documented in a test script's expected results column*
- *A test fails if the system does not deliver the expected result in a test step as required by the test script*
- *A test also fails in the event the system freezes, crashes, or stops executing while testing*
- *After failure of a test step within a test script, the test script as a whole is deemed to have failed*

*Any test repeats or restarts are at the discretion of the Test Conductor in coordination with the test committee, if one exists. Any failure is registered as a defect in the defect tracking tool, sent through the defect handling process, (see section **A15.2.9.1 - Defect Resolution Process**), and should be reflected in the test results report.*

A15.2.5.3 Test Suspension / Resumption Criteria

*A test suspension is not the same as a test failure. Section **A15.2.5.2 Pass / Fail Criteria** defines the failing criteria for a specific test case or test script. A test suspension condition defines the criteria for stopping, usually temporarily, all or portions of a test session. Resumption criteria are criteria that allow the test session to continue. Provide a listing of all test suspension criteria and all resumption criteria for the test phase under planning.*

The **<Test Manager>** has the authority to suspend a test. The criteria for System Test / UAT Suspension include:

- Unavailability of external dependent systems during testing
- When a test case or script fails that prohibits further testing

The **<Test Manager>** and the **<onsite State agency Test Lead>** have the authority to resume the test. The criteria for System Test / UAT Resumption include:

- Any dependent unavailable system becomes available
- The test team is notified a fix is successfully implemented and a patch is ready for installation

A15.2.5.4 Test Criteria

*For a review of test tolerance, test samples, and system breaks, see the section **6.4.1.2 Pass / Fail Criteria**. Provide a list of test tolerances for the article under test. For tests that will specify test criteria, provide the*



details of acceptable tolerance ranges. For tests that will run test samples, provide the details of the changes in the test conditions for each sample. A summary table or a bulleted list is acceptable.

Table 61 lists the acceptable sample and tolerance ranges for the UAT.

Table 61: Example of Systems Test /UAT Sample and Tolerance Data

Test	Tolerance Range	Sample Number	System Breaks
Response Time – 25 counties, 6 work stations /county	Feedback received (0.05 – 0.5) sec	3 times for 60 minutes each	Stop Test
Memory Buffer Usage	Never more 75% capacity	2 times for 60 minutes each	Stop Test
Data Flow to interfaces-errors received	Zero	3 transmission attempts	Stop Test

A15.2.6 Test Cases

A Test Case is a collection of test scenarios and test scripts designed to verify the system under test performs as expected. Each test case is related to an Item To Be Tested (see section A15.2.7). Test cases are comprised of test scenarios, test scripts, test data, expected results, related error handling routines, and specific test procedures for progressing through each test case. Testing any IS involves having a suite of test cases to verify and validate the system against requirements.

Test cases differ from test scripts in that the case is a manual, step-by-step input. The detailed test cases to be used during the test may be included in the appendices to this “Complete and Final Test Plan.” However, the State is required to provide a list of the cases to be used, and briefly state the objective of the cases. FNS may request a sample of the test cases.

Table 62 is a listing of all test cases planned for testing with a description of the test case objective.

Table 62: Example of Test Cases and Objectives

Test Case	Test Case Objective
Workstation Data Entry 1	This test case will input and store personal data into the system
Internet Data Entry	This test case will input and store personal data into the system
Data Matching 1	The test case will search for a Social Security Number from the Federal SSA database



A15.2.7 Test Scenarios / Test Conditions

A test scenario is a one-line pointer that testers create as an initial, transitional step into the test design phase. This is a definition of “What” is going to be tested with respect to a certain feature. A test scenario might result in multiple tests. A test condition defines the aim or goal of a certain test. Provide a detailed list of test scenarios and test conditions to be used.

Table 63 provides a complete listing of scenarios and associated conditions for the UAT.

Table 63: Example of Test Scenarios and Test Conditions

Test Case	Test Scenario	Test Conditions
Verify Database	Verify database response to incorrectly formatted or out of range data	<i>Input name data as all blanks, and check for an error message and no input</i> <i>Input name data as all digits, and check for an error message and no input</i>
Verify Database	Verify database response to correctly formatted data	Input last name as Davis and first name as Alan; check for addition to database of Alan Davis Input SSN as ***-**-**** , check for addition to database of <name> correct SSN
Verify Database	Verify that data from database can be recalled on a workstation	Search for <name> on work station; check data appears correctly in the name field Search for <name> SSN; check data appears correctly in the SSN field
Include additional Test Scenario and Test Condition items related to “Items to be Tested” as needed.		

A15.2.8 Items to be Tested

The items to be tested should be relevant to the scope of testing based on test cases (see section 6.5 and all sub-sections). Provide a list or table of items to be tested. Describe the items/features/functions to be tested that are within the scope of this “Complete and Final Test Plan.” Include a description of how the items will be tested, when, by whom, and to what quality standards. Also include a description of those items agreed upon not to be tested.

As testing progresses along project milestones, the items to be tested from this section can be archived in a separate list or table. The archived list or historical table will provide a total composite list of items tested



during unit, integration, system, performance, and end-to-end tests to date. In preparation for UAT, the only items that might have to be added would reflect implemented changes from system testing.

Table 64 provides the items to be tested for UAT.

Table 64: Example of Items to be Tested for UAT

Item to Test	Test Description	Test Date	Responsibility
Functional Items	<i>Test for Eligibility, Issuances, Notices</i>	<mm/dd/yyyy>	<Person name>
System End to End and Performance	<i>Test timing, bandwidth, stress, interfaces</i>	<mm/dd/yyyy>	<Person name>
Data Conversion / Migration	<i>Test data formats, parity, file formats, data interface transfer, database generation</i>	<mm/dd/yyyy>	<Person name>
Security	<i>Test sign on, passwords, personal data</i>	<mm/dd/yyyy>	<Person name>
Regression	<i>Test ripple effects on defect corrections and new code</i>	<mm/dd/yyyy>	<Person name>
Include additional items and plan contents for other needs related to "Items to be Tested"			

A15.2.8.1 Data Conversion

Data conversion plays a major factor in a successful Systems Testing and UAT due to the importance of interfacing with other systems. Eligibility and Issuance determinations make it imperative that the data is both transmitted and received correctly and therefore, must be addressed during test planning. Describe the approach and the plan for data conversion, migration, and preparation, and include it in the "Complete and Final Test Plan." If a standalone Data Conversion Plan exists, include the reference in this section.

The approach should contain:

- The basics of how data conversion, migration, and preparation will be done
- A data conversion/migration milestone entry on the project and test schedule
- The responsible organization for completing and testing the conversion and migration
- A milestone entry for generating a test database on System/UAT environment
- The responsible organization for generating and verifying the database

Table 65 contains the major elements for data conversion planning.

**Table 65: Example of Data Conversion Elements**

Item	Plan Contents
Plan – Conversion/Migration/Preparation	<Approach>
Plan – Conversion Milestones	<Start Date – Stop Date>
Plan – Migration Milestones	<Start Date – Stop Date>
Plan - Responsibilities	<Organization – Subject Expert>
Database Generation	<Approach>
DB – Generation Milestones	<Start Date – Stop Date>
DB - Generation Responsibilities	<Organization – Subject Expert>
Type verification tests	Database generation, data flow across interfaces
<i>Include additional items and plan contents for other needs related to testing data conversion and migration</i>	

A15.2.8.2 System Security

The six basic security concepts that need to be covered by security testing are confidentiality, integrity, authentication, availability, authorization, and non-repudiation. For each security concept applicable, describe the approach for security testing to include:

- *Operator sign on and password security*
- *Security of data within the system under test*
- *Security of data over multisystem interfaces*
- *Security of personal case data such as Social Security numbers*
- *System security from intrusion attempts*
- *Intersystem encryption use*

Provide a bulleted list or a table, and define the security concepts as they apply to testing for the items provided.

A15.2.8.3 Stress/Load Testing

Stress and Load testing are part of overall performance testing. The “Complete and Final Test Plan” describes how these tests are conducted and includes corresponding Test Cases, Test Scenarios, Test Scripts, Test Data,



and Test Criteria. See section 6.1.3 Required Testing Activities for additional information on Performance Testing.

- *Load testing checks the application's ability to perform under normal and peak load conditions to verify the application can handle the anticipated number of users.*
- *Stress testing evaluates an application under extreme workloads to see how it handles high traffic or data processing. The objective is to push the application beyond normal or peak load conditions to identify its breaking point.*

A15.2.9 Issue/Defect Tracking and Prioritization

A15.2.9.1 Defect Resolution Process

Describe the defect handling process to be used while testing. Include any test failures identified in Section A15.2.5.2 Pass / Fail Criteria in this process. If the project has a standalone process published for defect handling, the document must be included in this section or as an attachment to the "Complete and Final Test Plan."

The following four tables summarize the defect handling process for all pass/fail items. **Table 66** defines the process for defect identification and analysis.

Table 66: Example of Defect Identification and Analysis

Step	Description
1	Tester discovers a possible problem and may consult with the onsite test team before entering a possible defect
2	The tester enters a error using the supplied form and submits to the UAT analysis team
3	The defect is evaluated and amended, if needed, by the analysis team
4	The defect is classified for processing and routing

Table 67 describes the fields used on the defect tracking form and database.

Table 67: Example of Defect Tracking Form Field Definition

Field Name	Field Purpose/Description
Defect ID	Unique identifier for defect, usually tool generated
Defect Description	Describes defect in detail
Test Script Number	Identifies the Test Script executed when defect occurred

**Table 67: Example of Defect Tracking Form Field Description**

Field Name	Field Purpose/Description
Defect Type	Type of defect such as functional application, conversion, data, batch program, report, enhancement, screen name
Defect Severity	Criticality of defect

Table 68 defines each status of any defect as it progresses through the defect handling process.

Table 68: Example of Defect Status Description

Status	Description
New	Reflects the state of a defect initially identified. These defects have yet to be assigned for resolution.
Open	Reflects the status of a defect in review by testers or business analysts. Defects in 'Open' status are usually undergoing a review process prior to being assigned to a technical team for resolution.
Assigned	Reflects the state of a defect while being reviewed/analyzed/fixed by a technical resource.
Fixed	Represents the state of a defect once it is fixed/resolved by a technical resource. A defect in a 'Fixed' status is not currently available for re-test and could still be undergoing unit tests or awaiting a software application build.

Table 69 defines the defect severity and priority levels for defect processing.

Table 69: Example of Defect Severity and Priority Definitions

Severity Level – S Priority Level – P	Description
S – Critical	Causes the system to crash or freeze indefinitely and renders the whole system/business area within the system to be Non-Operational
S – High	The system fails to perform a critical function correctly, which results either in erroneous data being generated or displayed or a subsystem's component fails to function and thereby causes a subsystem or a portion of the system to be Non-Operational
S – Medium	Does not meet system requirements but does not affect accuracy of eligibility or benefit amount, and the performance impact is acceptable in the short term
S – Low	Not a critical issue and does not result in an erroneous action or data loss or inconvenience to complete a business function
P - 1	Defect needs to be fixed immediately in order to resume operations
P - 2	Defect has adverse impact on the work process, benefits, and payments
P - 3	Defect has minor impact on the work process, benefits, and payments



Table 69: Example of Defect Severity and Priority Definitions

Severity Level – S Priority Level – P	Description
P – 4	Defect has no impact on functionality, workflow, or data accuracy

A15.2.9.2 Regression Testing Process

As defects are discovered and fixed, there is a risk that any modification to the software might impact software already developed and tested. To minimize this risk, regression testing is performed for new builds that include fixed defects to verify and validate that previously tested functions and features are still performing correctly. Whenever regression testing is used as part of a test effort, the regression test scripts/cases should be documented and recorded in the State agency's comprehensive test plan.

Describe the regression testing process in general terms and the conditions when it is used.

<regression testing process description>

A15.2.9.3 Evaluation of Test Progression

This sub-section of the "Complete and Final Test Plan" describes the progression from one test to another. Eventually the entire cycle is completed. In some instances, the order of testing is independent of other tests. In other instances, it is necessary to conduct one test before or after another. Provide a list or table of the test progression planned for this test cycle, and document particular items in the progression that have order dependencies, such as linear or parallel execution.

Table 70 provides the listing for the test progression planned for this test event.

Table 69: Example of Test Progression

Order/ Progression	Software Test	Dependencies
1	Database Generation	• Test must be conducted before others begin • Test must complete successfully; database formatting, reading, and writing critical to remaining tests
2	Work Station Verification	• May not begin prior to Order 1 tests completed and successful • May be executed concurrently with Internet Verification (Order 3) • Must be conducted prior to Data Flow Between Input Devices (Order 4) • Test must complete successfully



Table 70: Example of Test Progression

Order/ Progression	Software Test	Dependencies
3	Internet Verification	• May not begin prior to Order 1 tests completed and successful • May be executed concurrently with Work Station Verification • Must be conducted prior to Data Flow Between Input Devices, (Order 4) • Test must complete successfully
4	Data Flow Between Input Devices	• May not begin until Order 2 and 3 testing completed

A15.2.10 Risk Management

See section 6.4.5 Test Risks/Issues for a discussion on risks and sources of risk. Provide a summary list of known risks to the test effort and the severity level, and briefly describe the method for managing the risks.

A15.3 Additional Final Test Plan Contents

A15.3.1 UAT Test Deliverables

Provide a list of documents that will be delivered to FNS as a result of the UAT.

The following documents are deliverable to FNS as a result of the UAT.

- UAT Test Plan (if modified since last shared with FNS)
- UAT Test Results and Report
- UAT Test Procedures
- UAT Test Cases and Scripts (upon request)
- UAT Report on Open Risks
- UAT Report on failures with severity levels

A15.3.2 Go/No-Go Determination Process

The Go/No-Go process is a formal system assessment conducted by the State agency to decide if the system has performed adequately enough to proceed to the next test phase. The process is performed a minimum of twice during the system lifecycle, once after completing UAT and again after completing the Pilot. FNS concurrence



with UAT results allows for the project to proceed from UAT to Pilot and the continuation of funding. FNS approval of Pilot results allows for the project to proceed from Pilot to Rollout and the continuation of funding. The Go/No-Go decision is not a test; however, the basis of this determination is derived from the UAT test results and the Pilot test results. Go/No-Go criteria are not the same as Entry/Exit Criteria (A15.2.5.1).

The process begins by the State agency conducting an assessment of the UAT results and comparing them to test expected results, analyzing test metrics, and measuring them against the pre-established Go/No-Go criteria. Following the assessment, the State agency will make a recommendation to the FNS for concurrence for continued funding to advance to pilot testing. The assessment results, test results, and recommendation are put into a formal document and sent to FNS requesting concurrence. This is repeated at the completion of the pilot, to get FNS approval and funding to advance to rollout.

Items required to be included in a formal No-Go document and a description of the Go/No-Go Decision Process are both included in section 6.4.7 Go/No-Go Decision Process.

A15.3.3 Roll Back Contingency Plan

The “Complete and Final Test Plan” must provide a roll back contingency plan from the State agency. The roll back contingency plan should include the specific targets or metrics that must be met during conversion or rollout before the state can proceed – incremental go/no-go points. Failure to meet these targets will trigger the need to stop the pilot and roll back to UAT, or to stop the conversion or rollout and return to pilot. A decision may have to be made to stop testing based on the number and severity of the defects/problems identified during UAT, Pilot, or Rollout. Two other considerations are the amount of time needed to fix defects and if test resources are not available for an unacceptable period of time. The plan should address rescheduling testing and options for either restarting or ending the project.

A16. Ownership Rights

A16.1 Policy Requirements

There are several policy requirements that State or local governments must include in all contracts for any software or software modifications and associated documentation that is designed, developed, or installed with Federal financial participation funding. These include ownership rights and a broad Federal License, among others, as provided in [7 CFR 277.18\(l\)](#).¹³⁶



“FNS reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use and to authorize others to use for Federal government purposes, such software, modifications and documentation [designed, developed or installed with Federal funds].” - 7 CFR 277.18(l)(ii)

Proprietary vendor software packages and operating systems (OS) that are provided at established catalog or market prices and sold or leased to the public are not subject to these ownership provisions. Federal funding is not available for proprietary applications software developed specifically for SNAP or WIC.

The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal government purposes such as system analysis and/or transfer.

A16.2 Understanding the Policy

A16.2.1 Purpose

The primary purpose of these policy requirements is financial stewardship of FFP to ensure that federal funds are not used to pay repeatedly for the same functionality. Another purpose is to facilitate transfers of useful systems among States in support of the financial stewardship purpose. There are two major considerations affecting transferability: the right to transfer (i.e., ownership and licensing) and the ability to transfer (i.e., technological compatibility, interoperability, and portability).

A16.2.2 Supporting the Policy in Acquisitions

State agencies' ability to fulfill these policy requirements depends largely on well-written solicitations and requests for proposals (RFPs). State agencies must explicitly include sufficient information for offerors to understand what the State Agency is buying, what information they must provide, and how their proposals will be evaluated.

In State contracts, the responsibility and discretion to negotiate the State's minimum needs is significant. Many States may have default clauses for intellectual property (IP) rights and rights in technical data. In the absence of State-specific procurement clauses for such contracts, the parties must negotiate all that is addressed in the standard IP contract clauses. If these clauses do not exist (the potential rights and issues are so involved), it is a best practice to use as a guide some model that has been rigorously tested. One such model is the FAR. States are not required or obligated to use FAR references in their RFPs and contracts. Nonetheless, the FAR clauses would be a valuable reference to use as a model for State RFP and contract IP clauses, especially given the federal awarding agencies' involvement and the use of FFP.

A16.2.3 Software Ownership

Under the Federal License, FNS and the State agencies who grant the license may use this license to share the software and associated system documentation with other State agencies who may be interested in transferring the software. The Federal License is a product of intellectual property rights (i.e., copyright) rather than funding source (i.e., State public funding and/or Federal financial participation). State ownership of software designed, developed, or installed with FFP means the State agency should secure copyright ownership from the vendor or developer through specific contract clauses. These are included in the appropriate sections of the solicitation, RFP, and resulting contract.



The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal government purposes such as system analysis and/or transfer.

A16.2.4 Licensing Principles

Software is a product or work of intellectual activities and is covered by copyright law. Copyright law establishes ownership for the creator of the work who, as the owner, retains all copyright protections, unless they transfer



those through a recognized written legal instrument. For software, this is typically accomplished through user licenses, which are further reinforced by contract law.

Generally speaking, there are two types of licenses: exclusive and non-exclusive. Under copyright law, the copyright owner has exclusive rights to “reproduction, adaptation, publication, performance, and display.” The phrase “exclusive right” means that only the copyright holder, or licensees that have been granted those exclusive rights, are free to exercise those rights. Others are prohibited from using the work without the copyright holder’s or exclusive licensee’s permission. This is an exclusive license. The exclusive rights may be sub-divided into limitations, restrictions, qualifications, and exemptions, which are then provided in specific sections of the U.S. copyright law. For these to be legitimate, they must be in writing and signed by the grantor. As the exclusive rights are limited, qualified, and restricted, they become non-exclusive, and the written result is a non-exclusive license. Non-exclusive licenses mean that the copyright owner has some rights and the license holder has some rights. However, unless the license transfers all exclusive rights to the licensee, the licensor (i.e., the copyright holder) still has exclusive rights, and has only granted permissions to the licensee. Without a valid, thorough, written and signed agreement, the legal status of the many rights that are the subject of a copyright may be difficult to unravel. The issue becomes who has the right to do what with the respective copyrights. The terms of licenses can be negotiated and executed through contracts, serving as a mechanism establishing the respective rights in writing.

A16.2.5 “Rights in Data” and “Works-Made-for-Hire”

Government entities often express ownership of software produced as a contract deliverable as “rights in data.” The content of these rights in data clauses varies with each contract, although they are outlined in the FAR. While the FAR has extensive provisions for “rights in data,” the FAR is not directly applicable to State agencies when acquiring software using FFP. This is because, even though States are using FFP, they are executing State contracts (i.e., non-FAR contracts), not federal contracts (i.e., FAR contracts). However, the FAR is indirectly applicable through the various Codes of Federal Regulations (CFR) governing use of FFP and administration of public assistance programs. Although not required, many States often use language similar to the FAR for rights in data in their contracts for procuring software using FFP.

“Data” means recorded information, regardless of form or the media on which it may be recorded. The term is widely understood to include technical data and computer software delivered in the performance of a government contract. The rights to that data may be unlimited, limited, or restricted. Unlimited data rights are the default rights in data. This means that the contractor who delivered the data is generally not allowed to assert intellectual property rights unless the contracting officer grants permission. It also means the government may use the data in any manner it sees fit without restraint or restrictions. State agencies and contractors may negotiate rights in data when writing contract clauses for acquisitions using FFP, but must protect State interests for ownership and transferability to maintain eligibility for FFP.



States may also invoke “works-made-for-hire” clauses in their contracts, which have special meaning within U.S. copyright law. “Works-made-for-hire” clauses mean that an employee of an organization is not entitled to intellectual property rights for works created in the performance of their duties for the employer. Any intellectual property rights attendant to works created by employees are reserved for the employer. State contracts, unlike federal contracts, may apply the “works-made-for-hire” clauses to contractors. In other words, the RFP and the resulting contract specify that the relationship between the State agency and the contractor is an “employer to employee” relationship, for purposes of intellectual property. The contractor is not an “independent contractor” where no “employer to employee” relationship exists. The result is that ownership and intellectual property rights belong to the State agency, not the contractor. Without the specific “works-made-for-hire” clauses, it is an “independent contractor” relationship and intellectual property rights belong to the contractor. When the intellectual property rights belong to the contractor, the contractor grants licenses.

Unlike the Federal government, U.S. copyright allows States to own copyrights under U.S. copyright law for works produced by their employees. This provides a stronger basis for establishing State ownership for deliverables based on copyright law rather than FFP eligibility policies, but is not sufficient by itself.

Assignment of rights or transfer of rights clauses must also be included in the RFP and contract to ensure proper State ownership in copyrights for software and technical documentation is achieved. Assignment and/or transfer of rights clauses operate under both U.S. copyright law and contract law, providing the most effective means to secure ownership for software and technical documentation as contract deliverables. States should take steps to verify that the contractor assigning copyright has full right and title to the copyright being transferred. In other words, that prime contractors have established proper employer/employee relationships with their own employees and any sub-contractors they may use for the delivery of contract deliverables.

A16.2.6 Assistance Provided by State Employee

Whether FNS may use privately developed software when a State employee may have assisted the private developer depends on the degree of assistance. If the employee’s assistance is significant enough to make him or her a joint author of the software, then [Chapter 2, Section 201\(b\) of the Copyright Law of the United States](#)¹³⁷ would confer ownership of the employee’s share upon the State because of the “work-for-hire” relationship between the State and the employee. It could be argued strongly that [7 CFR 277.18 \(I\)\(1\)](#) would give FNS a license, at least with regard to the employee’s contribution, because of the relationship between the State agency and the Federal agency providing federal funding. The government is not in a strong position to claim licensing rights in software developed at private expense with assistance from a State employee, unless the employee’s contribution is equal to co-authorship. Such rights are best addressed in a formal agreement at the time a State employee is requested by a private organization to participate in software development.

A16.2.7 Public Domain Status

The term “public domain” has often been misunderstood or misapplied to software developed by State agencies using federal funding. Those software products are not public domain. Public domain software is, technically speaking, the complete absence of copyright ownership or intellectual property rights for the software. Statutes and case law do not recognize public domain intellectual property as public property; public property is still owned. They recognize public domain intellectual property as those intangible works which no one owns and are available for use by members of the public without infringing on anyone’s intellectual property rights.

“Public domain” may be used incorrectly to refer to any software distributed under a free software license. Although the software distributed under a free software license was released under a license that grants rights to others (such as the freedom to modify and redistribute the software), the copyright (or other rights) to the software may still be held by the author. Therefore, such software would not be in the public domain. The term “public domain” may also be used to mean free, as in having no cost (i.e. gratis). However most gratis software is not in the public domain, but simply released under a free software or Open Source Software license that permits distribution of the software so long as no charge is levied. Examples of this include Adobe Acrobat Reader and Mozilla’s Firefox internet browser. The term “public domain” has also been used incorrectly to characterize the ownership of software developed using FFP.

When a State agency obtains ownership through the application of copyright laws in contracts, the software or software modifications and associated documentation designed, developed, or installed with FFP are not public domain. The use of FFP does not revoke the State’s copyright ownership, nor does the Federal License.

A16.2.8 Transferring Software

Facilitating transfer of systems involves more than ensuring the RFP contains appropriate provisions for intellectual property rights. It also means including requirements that result in a system that is oriented towards transferability in its design; that it will be interoperable, portable, and that commercial elements can be easily identified and segregated from elements owned by the State agency.



See chapter **5.0 System Planning** for more information about design considerations.

Listed below are several key transferability characteristics States need to consider when going through the APD process. The intellectual property clauses and the Modular Open Systems Architecture (MOSA) examples in section **A16.4.1 - Modular Open Systems Approach (MOSA)** and **A16.3 - Applying the Policy - Contractual**



Provisions are examples of how many of these can be addressed in RFPs and contracts. **Intellectual Property transferability considerations should include the following:**

- State Ownership – Is transferability possible because the donor State has full ownership of the system?
- Federal License – Does the donor system have a Federal License associated with it in accordance with applicable policies?
- Rights for Derivative Works – Does the donor system include appropriate licensing for the recipient State to be able to use derivative components of the donor system?
- Licensing for Third Party Software – Are all licenses for third party software that are components of the donor system available to the recipient State to use and keep the system operating?
- Ownership of Preexisting Products – Are proprietary components and vendor-owned components of the donor system clearly identified and licensed for the recipient State to use and keep the system operating?

Transferability considerations should be addressed in procurement documentation. The RFP and contract must make it clear that the source code, documentation, database schema, and other supporting components must be made available by the State and/or Vendor to other State agencies for Federal government purposes such as system analysis and/or transfer. Such documentation may be part of the service deliverables from the system provider as part of the RFP and the resulting contract for the selected offeror. See examples of how to incorporate appropriate clauses addressing these considerations in section **A16.3 - Applying the Policy - Contractual Provisions** below. State agencies may also plan to collaborate, to the extent that it is practical to do so, on further development of the software. This may be facilitated by including a provision in the RFP/contract that recognizes the State agency may be sharing software code on an ongoing basis to promote the efficient use of resources for system enhancements.

A16.3 Applying the Policy - Contractual Provisions

A16.3.1 Ownership and Licensing

In fulfilling compliance requirements for FFP eligibility, the State agency should secure intellectual property ownership for any software or software modifications and associated documentation through the application of U.S. copyright law principles. By securing copyright ownership, the State agency will have exclusive ownership in the intangible property delivered under the State contracts for SNAP and WIC systems, which allows them to grant licenses. This is the foundation upon which the Federal License and system transfers are possible.

A16.3.2 Example Contract Clauses

Under a State contract, in any case of application of “work-made-for-hire” clauses, assignment of rights, or transfer of rights, the State Agency should obtain copyright ownership in any deliverables (see section **A16.2.5**); this would be an exclusive license. It is important to use appropriate contract clauses to secure copyright ownership. Likewise, it is important not to negotiate these rights through subsequent licensing of rights back to the vendor once secured. The clauses for copyright ownership and licensing for software delivered in performance of the contracts for the systems can be grouped into five major categories:

- State Ownership
- Federal License
- Rights for Derivative Works
- Licensing for Third Party Software
- Ownership of Preexisting Products

Included in the appendix are examples of contract language that has been used by various State agencies to achieve FFP eligibility requirements and proper ownership of software or software modifications and associated documentation designed, developed, or installed with FFP. A “Jurisdiction” might be a county, State, Consortium of States or Counties, Territory, or Indian Tribal Organization. The following examples could be used for RFPs as long as the Federal License requirement is included.



See appendix **A10 Request for Proposal Template** for additional details and examples of ownership clauses.

State Ownership

All Deliverables and modifications, in whole and in part, shall be deemed works made for hire of **<the jurisdiction>** for all purposes of copyright law, and copyright shall belong solely to **<the jurisdiction>**. To the extent any work or Deliverable is deemed not to be, for any reason whatsoever, work made for hire, the Contractor agrees to assign and hereby assigns all rights, title and interest, including but not limited to copyright patent, trademark and trade secret, to such work and Deliverables, and all extensions and renewals thereof, to **<the jurisdiction>**. **<The jurisdiction>** shall own all right, title, and interest to the software and associated documentation, including all copyright, patent, trade secret, trademark and other intellectual property rights created by the contractor in connection with such work (in whatever form), that comprise **<the jurisdiction>**’s System as designed, developed or installed in accordance with the terms of this Agreement. The contractor shall take all actions necessary and transfer ownership of the Deliverables to **<the jurisdiction>**, including, without limitation, the Custom Software and associated Documentation, including all copyright, patent, trade secret, trademark and other intellectual property rights, on Acceptance of each Deliverable and following final payment for each Deliverable.



Federal License

All appropriate State and Federal agencies (including without limitation the Federal government agencies providing Federal financial participation) shall have a royalty free, nonexclusive, and irrevocable license to reproduce, publish, translate or otherwise use and to authorize others to use for Federal government purposes all materials, the software and modifications thereof, and associated documentation designed, developed, or installed with Federal financial participation under this Agreement.

Rights for Derivative Works

The Contractor shall grant to **<the jurisdiction>** and the Contractor shall require each Contractor Custom Software Sub-Licensee to grant to **<the jurisdiction>** a worldwide, non-exclusive, perpetual, irrevocable, fully paid up right and license to use, copy, modify and prepare derivative works based on custom deliverables, such modifications thereof, and derivative works.

Licensing for Third Party Software

The Contractor will represent and warrant to **<the jurisdiction>** that it has obtained all rights, grants, assignments, conveyances, licenses, permissions and authorizations necessary or incidental to any materials owned by third parties supplied or specified by it for incorporation in the deliverables to be developed.

Ownership of Preexisting Products

The Vendor will retain all right, title and interest in and to all Property developed by it, 1) for clients other than **<the jurisdiction>**, and 2) for internal purposes and not yet delivered to any client, including all copyright, patent, trade secret, trademark and other intellectual property rights created by the Vendor in connection with such work prior to the date of the contract.

A16.4 Example Clauses for Supporting Transferability

To support transferability of systems procured with FFP, consideration needs to be given to including appropriate requirements, instructions to offerors, and evaluation for award criteria in the applicable solicitation and RFP sections. Below are several simplified examples adapted from actual clauses included in federal and DoD contracts, including the RFP section where they should be included. Not all examples would necessarily be required in a RFP. More extensive and detailed examples of relevant contract clauses can be found in "Incorporating Software Requirements into the System RFP - Survey of RFP Language for Software by Topic, v. 2.0" from the Software Engineering Institute (SEI) at Carnegie Mellon University.¹³⁸



Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation – RFP Evaluation Criteria

In evaluating the Data Rights, **<the jurisdiction>** will use information in the proposal to assess the extent to which the rights in technical data, computer software, and computer software documentation, offered to the **<the jurisdiction>** ensure unimpeded, innovative, and cost effective production, operation, maintenance, and upgrade of the **<System Name>** throughout its lifecycle; allow for open and competitive procurement of **<System Name>** enhancements; and permit the transfer of the **<System Name>** non-proprietary object code and source code for [jurisdictional] purposes in accordance with applicable intellectual property rights established by the contract.

Treatment of Proprietary or Vendor-Unique Elements – RFP Instructions to Offerors

The Offeror shall justify any use of proprietary, vendor-unique, or closed components, including but not limited to Commercial off-the-shelf software (COTS), and interfaces in current or future designs. This justification shall include documentation of the decision leading to the selection of specific COTS products (e.g. with test results, architectural suitability, best value assessments, etc.). The Offeror shall define its process for identifying and justifying proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software to be used. The Offeror shall describe how the integration of closed or proprietary, vendor-unique equipment, interfaces, data systems or functions due to a unique or specific system requirement will not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system. The Offeror shall identify and take steps to prevent the open elements of the system from intertwining with proprietary or vendor-unique elements in a manner that restricts or limits the ability to replace or upgrade the open elements using an open competitive selection process. The Offeror shall describe and demonstrate that the modularity of the system design promotes identification of multiple sources of supply and/or repair, and supports flexible business strategies that enhance subcontractor competition.

A16.4.1 Modular Open Systems Approach (MOSA)

Modular Open Systems Approach is a design and system architectural approach that supports transferability of technology. The example clauses below provide guidance on how to include clauses in the RFP and contract to acquire this type of solution. Each example goes into different parts of the RFP as indicated by the sub-title in the sample below.



See chapter **5.0 System Planning** for more information on Open Systems Architecture.



PWS Requirements

The Offeror shall use a modular open system approach (MOSA) to evaluate the appropriateness of implementing a modular design strategy for building systems. A primary consideration to meet the design functionality shall be the impact to the overall modular open systems architecture. A modular open systems approach and analysis of long term supportability, interoperability, and growth for future modifications shall be major factors in the Offeror's final selection of an integration approach. All the systems components shall facilitate future upgrades and permit incremental technology insertion to allow for incorporation of additional or higher performance elements with minimal impact on the existing systems.

The architectural approach shall provide a viable technology insertion methodology and refresh strategy that supports application of a modular open systems approach and is responsive to changes driven by mission requirements and new technologies. The Offeror shall develop a detailed modular design and integration that includes but is not limited to the following aspects: interoperability, intra-operability, upgradeability, re-configurability, transportability, software standards, interface standards, long-term supportability, sources of supply and/or repair, business strategies, and other entities that affect application of a modular open systems approach.

For those portions of hardware, firmware, or software that are driven to proprietary and/or closed system architectures by mission specific requirements, a hardware/firmware/software partitioning or other design features to mitigate the system level impacts shall be provided. The Offeror shall provide an orderly, planned approach to address migration of proprietary or closed system equipment or interfaces to a modular design when technological advances are available.

The Offeror's modular design and integration shall preclude long term dependence on closed or proprietary interface standards, technologies, products, or architectures. Secure or classified data systems shall also conform to the modular design approach as much as practical. The design shall provide sufficient growth and open interface standards to allow future reconfiguration and addition of new capabilities without large-scale redesign of the system.

RFP Evaluation Criteria:

1. Identification of specific acquisition objectives (e.g., affordability, ease of change, leveraging commercial investment in new technology, etc.) and operational capabilities (e.g., ease of integration, interoperability, etc.) directly or indirectly dictate the use of open systems in the program.
2. A system architecture characterized by modular design.
3. The degree to which the program risk management strategy and modular open systems approach (MOSA) complement each other.
4. Justification of modular open system design via business case analysis (e.g., cost/benefit analysis, market research findings, etc.).
5. Proactive management of system interfaces.



6. Identification of key system interfaces based on the module characteristics (e.g., criticality of function, ease of integration, change frequency, interoperability, commonality, etc.).
7. Appropriate designation of open standards for key system interfaces.
8. Open Standards Indicators - Feasibility studies to assess the use of open standards for key interfaces.
 - a. Application of a standards selection process that gives preference to open standards.
 - b. Standards selection for key interfaces is based on application of specific criteria (e.g., industry consensus, market support, prime contractor recommendation, etc.). Additionally, does the Offeror's proposal provide the User with the ability to:
 - i. Quickly interconnect, reconfigure, and assemble existing forces, systems, subsystems, and components?
 - ii. Interchange and use information, services and/or physical items among components within a system?
 - iii. Interchange and use information, services and/or physical items among systems within an integrated architecture, platform, or domain?
 - iv. Support reuse of software and the common use of components across various product lines?
 - v. Transfer a system, component, or data, from one hardware or software environment to another?
 - vi. Adapt hardware or software to accommodate changing workloads?

RFP Instructions to Offerors:

Open Systems Approach and Goals. The Offeror shall describe its open systems approach for using modular design, standards-based interfaces, and widely supported consensus-based standards to achieve the following goals. At a minimum, the Offeror shall provide the following as part of its proposal:

1. Address Open Architecture Requirements – A detailed description of the Offeror's approach for addressing a system architecture that incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability.
2. Design Disclosure – Within the constraints of contractual data rights, a detailed description of the Offeror's approach to facilitate the sharing of system or component (e.g., software, hardware, middleware) design information in support of peer reviews and the development process. The Offeror shall describe how its design will be documented and modeled using industry standard formats (e.g., Unified Modeling Language), and how it will use tools that are capable of exporting model information in a standard format (e.g., Extensible Markup Language Metadata Interchange (XMI) and ISO 10303). The Offeror shall identify the proposed standards and formats to be used.
3. Technology Insertion and Refresh – A detailed description of how the Offeror's proposed system will allow for rapid and affordable technology insertion and refresh. For example, the Offeror should describe how the proposed system will allow incremental systems improvement through upgrades of individual hardware or software modules with newer modular components. At a minimum, the description shall address how



the Offeror's architectural approach will support this requirement including how components from third party providers and reuse sources shall be included.

4. Asset Reuse – A detailed description of the steps taken to reduce acquisition of duplicative system components where possible. At a minimum, the Offeror shall describe artifacts from the **<specific assets>** or common components. ***State agencies should insert descriptions of relevant, specific asset reuse repositories/libraries that the Contractors will review for components to be reused.***
5. Modular Open Systems Approach (MOSA) – A detailed description of the Offeror's modular open systems approach. At a minimum, the Offeror shall address:
 - a. Plans for integrating the systems both internally and with external systems;
 - b. The means for ensuring conformance to open standards and profiles, as discussed in Statement of Work (SOW) or Performance Work Statement (PWS), throughout the development process;
 - c. A description of how the technical approach ensures having access to mature as well as the latest technologies by establishing a robust, modular, and evolving architecture based on open standards.
 - d. A description of the strategy for maintaining the currency of technology (e.g., through Commercial off-the-shelf software (COTS) or reusable Non-Developmental Item (NDI) insertion, technology refresh strategies, and other appropriate means); and
 - e. Identification of processes for:
 - i. Isolating functionality through the use of modular design;
 - ii. Evaluating modular open system baseline standards, defining and updating profiles, and evaluating and justifying new or vendor-unique profiles;
 - iii. Validating implementation conformance to selected profiles;
 - iv. Managing application conformance to selected profiles; and
 - v. Training in use of profiles.
 - f. A detailed description of how the Offeror intends to use a modular open systems approach as an enabler to achieve the following objectives:
 - i. Adapt to evolving requirements as identified by **<the jurisdiction>**;
 - ii. Enhance interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions thereof;
 - iii. Facilitate systems reconfiguration and integration;
 - iv. Reduce the development cycle time and total life-cycle cost; and
 - v. Mitigate the risks associated with reliance on a single source of supply over the life of the system, to include, but be not limited to, technology obsolescence and dependence on proprietary or vendor-unique technology.
 - g. Life-cycle Supportability – A detailed description of how the Offeror intends to enhance life-cycle supportability by implementing performance-based logistics arrangements to sustain the components through their lifecycle.
 - h. Employ a Layered Modular Architecture – A detailed description on how the proposed system architecture is layered, modular, and uses of COTS that do not hinder or conflict with open standards architectures.



- i. Traceability of System Requirements – A detailed description of the Offeror’s approach for ensuring that all system requirements (including those contained in the Statement of Work (SOW) or Performance Work Statement (PWS) of this Solicitation) are accounted for through a demonstrated ability to trace each requirement to one or more modules. Modules consist of components (one of the parts that make up a system and may be hardware and/or software) which are self-contained elements with well-defined, standards-based and published interfaces.
- j. Minimize Inter-component Dependencies – A detailed description of the Offeror’s approach for designing a system that, to the maximum extent practicable, minimizes inter-component dependencies and allows components to be decoupled and re-used, where appropriate, through transfer to other State systems.
- k. Rationale for Modularization Choices – A detailed description of the Offeror’s rationale for the modularization choices made to generate the design. At a minimum, the rationale shall explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.
- l. Future System Upgrades – A detailed description of how a modular design strategy will be demonstrated in all aspects of future system upgrades.
 - i. In addressing the specified requirements, the proposal, at a minimum, must demonstrate how the modular design strategy applies, and the effect it will have on future system maintenance, operations, and upgrades.
 - ii. The proposal shall describe an orderly planned process to address migration of proprietary, vendor-unique, or closed system equipment or interfaces to a modular open systems design when technological advances are available or when operational capability is upgraded. The proprietary, vendor-unique or closed systems implementation shall also be reflected in the Offeror’s system level lifecycle cost estimates.
 - iii. The modular design approach shall either mitigate or partition — at the lowest subsystem or component level — proprietary, vendor unique or closed system implementation to avoid out-year supportability issues, diminished maintenance and upgrades, interoperability, and portability.

Inter-Component Dependencies – PWS Requirements

The Contractor’s design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or available to the <jurisdiction> with at least a nonexclusive, irrevocable, paid-up royalty-free worldwide license to use, modify, reproduce, release, perform, display or disclose the work by or on behalf of the <jurisdiction> and the FFP Federal



awarding agency. The system architecture shall minimize inter-component dependencies to allow components to be decoupled and re-used, where appropriate, to support maintenance, upgrades, interoperability, and portability.

A16.5 Inappropriate Intellectual Property Clauses

Having used properly structured clauses to obtain ownership of deliverable software, and to put in place applicable licensing, the State agency must guard against negating or nullifying these by including other clauses. Below are discussions of clauses that could effectively negate or nullify the State agency's ownership rights and the Federal License.

A16.5.1 Limiting State Ownership

Any contract language that undermines the objective of obtaining absolute State ownership of the copyrighted works should not be included in contracts. States should avoid any language that implies that the deliverable provides for anything other than the State's complete and exclusive ownership. For instance, language that implies that the software is being licensed to the State by the vendor should be avoided. A request to sign an end user license agreement (EULA) or to pay ongoing license fees indicates that the State is not receiving absolute ownership. The contract should be reviewed and amended to secure full ownership for the State.

A16.5.2 Use of the Software or resulting work

Any language that states or implies that the State is limited in what it may do with the deliverable is objectionable. Ownership of the copyright, as required by rules governing FFP eligibility, implies freedom to transfer or dispose of the intellectual property in whatever way the State sees fit. The State is free to grant, sell, or license the software however it wants. Any language that implies the State must seek permission from the vendor for the deliverable, excluding third party components identified elsewhere in the contract, is suspect and indicates that the vendor is retaining rights that should be delivered to the State.

A16.6 Best Practices

A16.6.1 Maintaining authority to hold copyright

Nothing in U.S. copyright law implies that software developed with FFP automatically becomes public domain. Although the U.S. Copyright Act precludes the Federal government from asserting copyright in government works under federal contracts, States are authorized to hold copyright in such works. However, not all States choose to do so. States do have the discretion to avoid holding copyrighted works, or to dispose of the copyright and put



the software in the public domain. Some States do not hold copyrights as a rule, and some State agencies are required to receive permission from higher State authorities in order to hold copyrights. FFP eligibility requires that the State obtain ownership of the copyright in order to transfer the required non-exclusive license to the Federal awarding agency. In order to remain in compliance with the FFP eligibility rules, States may need to ensure that proper authorization from higher State authorities exists for them to accept ownership of copyright. Failure to do so may jeopardize compliance with FFP eligibility requirements. It may also mean that no mechanism exists for the State to grant the required non-exclusive license to the Federal government in accordance with FFP requirements. A State cannot transfer a license to a copyrighted work for which it does not hold exclusive rights.

A16.6.2 States Capitalizing on Intellectual Property

States have discretion to determine whether it is in their best interest to capitalize on their intellectual property. Some States may not consider intellectual property as an asset that can be used for revenue generation, whereas others may be required to do so in some circumstances. Licensing State-owned copyrights back to the vendors is a better practice than simply granting rights to the vendor to profit from State-funded works. This allows the State to generate revenue from their IP, and secure rights in derivative commercial works.

A16.6.3 Vendor Profiting from Deliverables

States have discretion to decide whether to allow vendors to profit from deliverables under a State contract by licensing products developed at the public expense to third parties, or by creating derivative works from such products. However, States should be aware of vendors' intentions to profit from works developed at public expense, and at least secure irrevocable non-exclusive rights in the derivative works. Because the State is required to own the copyright, the vendor would be required to receive a license from the State before it could market the copyrighted work, or risk infringing the State's copyright. If a State agency decides to provide a license to the contractor, a best practice might be for the State to license the work to the vendor to include securing a licensing fee from any sale or license of the work, or derivative works to third parties.

A16.7 Use of Privately Developed Software

Privately developed software is considered to be proprietary, typically based on the principle that the developer used private funding exclusively to develop the software independently of any contract. Such development inherently means copyright attaches to the software, making it proprietary as a matter of intellectual property rights. Provisions in [2 CFR 200.448](#)¹³⁹ and [7 CFR 277.18\(l\)](#)¹⁴⁰ require State agencies acquire a Federal License to privately developed software where grant or sub-grant money was used to purchase copyright ownership, or grant or sub-grant funds were used in the development of software. This is relevant with regard to FNS' right to use privately developed software.



This regulation means that State use of FNS funds to purchase ownership of copyright in software would give FNS royalty-free use of the software, including the right to authorize other States to use the software in FNS programs. State use of FNS funds simply to lease contractor-developed software would not give FNS such royalty-free use.

FNS requires State agencies to incorporate the Federal License in any federally-funded sub-grant or contract to develop software. FNS is entitled to the Federal License in software only if FNS funds are used to develop the software, or if a State uses FNS funds to purchase copyright ownership of privately developed software.

A16.8 Acceptance of Free Software

Offers of free, or practically free, software should be rejected if acceptance thereof would give the offeror an unfair competitive advantage as to subsequent hardware procurement or follow-on software. This would be equal to receiving a gift from an interested party, or would be an unauthorized barter arrangement rather than a gift.

A16.9 Protecting State Agency Ownership

Any time (prior to contract award or during contract performance) that a contractor offers or proposes to pay for part of the development costs, a red flag should be waving. Do not allow the contractor to formally or informally shift costs so that the contractor exclusively is funding some piece of the requirement. Do not allow statement of work changes that might lead to the same result. These concerns also apply where the contractor attempts to partially fund something that previously was funded exclusively by the State, as software not paid for by the State may not be covered by transfer, assignment, copyright, or ownership provisions in the contract.



Endnotes

- ¹³⁶ "Ownership Rights, Software", 7 CFR 277.18 (l)(1)(ii), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=6a761d62f7ce6055cfad4e5088ec004a&mc=true&node=se7.4.277_118&rgn=div8
- ¹³⁷ "Ownership of Copyright", Copyright Law of the United States, Chapter 2, Section 201, Copyright Ownership and Transfer, Ownership of copyright, section 201(b), U.S. Government, <http://www.copyright.gov/title17>
- ¹³⁸ "Incorporating Software Requirements into the System RFP: Survey of RFP Language for Software by Topic", v. 2.0, Carnegie Mellon University Software Engineering Institute, Charlene Gross (2009) https://resources.sei.cmu.edu/asset_files/SpecialReport/2009_003_001_15017.pdf
- ¹³⁹ "Intellectual Property", 2 CFR 200.448, U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=dcd66228019bf16cbe86dcb76393381a&mc=true&node=pt2.1.200&rgn=div5#se2.1.200_1448
- ¹⁴⁰ "Ownership Rights", 7 CFR 277.18 (l), U.S. Government, http://www.ecfr.gov/cgi-bin/text-idx?SID=59f48aaf609e6da054a5218fa242d9a9&mc=true&node=se7.4.277_118&rgn=div8



In accordance with Federal civil rights law and U.S. Department of Agriculture (USDA) civil rights regulations and policies, the USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Persons with disabilities who require alternative means of communication for program information (e.g., Braille, large print, audiotope, American Sign Language, etc.) should contact the State or local Agency that administers the program or contact USDA through the Telecommunications Relay Service at 711 (voice and TTY). Additionally, program information may be made available in languages other than English.

To file a program discrimination complaint, complete the USDA Program Discrimination Complaint Form, AD-3027, found online at [How to File a Program Discrimination Complaint](#) and at any USDA office or write a letter addressed to USDA and provide in the letter all of the information requested in the form. To request a copy of the complaint form, call (866) 632-9992. Submit your completed form or letter to USDA by: (1) mail: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, SW, Mail Stop 9410, Washington, D.C. 20250-9410; (2) fax: (202) 690-7442; or (3) email: program.intake@usda.gov.

USDA is an equal opportunity provider, employer, and lender.