How States Safeguard Supplemental Nutrition Assistance Program Participants' Personally Identifiable Information

April 2023

Nondiscrimination Statement:
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, gender identity (including gender expression), sexual orientation, 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, audiotape, American Sign Language, etc.) should contact the responsible Agency or USDA's TARGET Center at (202) 720-2600 (voice and TTY) or contact USDA through the Federal Relay Service at (800) 877-8339. 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, 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.

How States Safeguard Supplemental Nutrition Assistance Program Participants' Personally Identifiable Information

Final Report

April 2023

Hiren Nisar, Dennis Okyere, Arpita Chakravorty, Lan Hu, and Raphael Dzanie

Submitted to:

Food and Nutrition Service (FNS)
United States Department of Agriculture (USDA)
1320 Braddock Place
Alexandria, VA 22314
Project Officer: Andrew Burns
Contracting Number: 12319818F0081

Submitted by:

2M Research
1521 N. Cooper St., Suite 600
Arlington, TX 76011

Disclaimer:
This study was conducted by 2M Research, under Contract No. 12319818F0081. The findings and conclusions in this report are those of the author(s) and should not be construed to represent any official USDA or U.S. Government determination or policy.

TABLE OF CONTENTS

LIST OF ACRONYMS

Abbreviation	Definition
BENDEX	Beneficiary Data Exchange
CMS	Centers for Medicare & Medicaid Services
EBT	Electronic Benefits Transfer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FNS	Food and Nutrition Service
GAO	U.S. Government Accountability Office
HIPAA	Health Insurance Portability and Accountability Act
IEEE	Institute of Electrical and Electronics Engineers
IEVS	Income and Eligibility Verification System
ISO	International Standards Organization
IT	Information Technology
MARS-E	Minimum Acceptable Risk Standards for Exchanges
NDNH	National Directory of New Hires
NIST	National Institute of Standards and Technology. NIST is the U.S. Federal agency that is tasked with protecting sensitive government information that is stored or handled by third parties, partners, and contractors. To this end, the agency produces special publications to give Federal partners a standard by which to safeguard confidential information and cybersecurity
PARIS	Public Assistance Reporting Information Systems
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
ROs	Research Objectives
RQs	Research Questions
SA(s)	State Agency (Agencies)
SDX	State Data Exchange
SNAP	Supplemental Nutrition Assistance Program
SSN	Social Security Number
USDA	U.S. Department of Agriculture

LIST OF DEFINITIONS

Term	Definition
Denial of Service Attack (Cybersecurity and Infrastructure Security Agency)	"A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible."[1]
Encryption	"Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state."[2]
Hardware-based encryption	"Hardware-based encryption uses a device with a processor designed specifically to authenticate users and encrypt data. Examples of hardware encryption devices include encrypted USB and external hard drives, self-encrypting SSDs, and even mobile phones with built-in encryption capabilities."[3]
Masking	"The process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym." [4]
Malware/Malicious Code	"Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code."[5]
Macro-level System Failure	A macro-level system failure could occur when the database where information is stored is corrupted and cannot be rescued.
Non-Sensitive PII	"Non-Sensitive Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, would not result

[1] Understanding Denial-of-Service Attacks | CISA - US-CERT
[2] Encryption - Cybersecurity Glossary
[3] Software vs. Hardware Encryption: The Pros and Cons (dsolutionsgroup.com)
[4] masking - Glossary | CSRC
[5] malware - Glossary | CSRC

Term	Definition
	in any substantial harm, embarrassment, inconvenience, or unfairness to an individual."[6]
Noise	"Statistically, adding noise to a dataset suggests slight alterations to mask the dataset. The noise hides PII, ensuring that the privacy of personal information is protected, but it's small enough to not materially impact the accuracy of the output of an analysis of the dataset."[7]
Phishing	"A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person. Phishing is also a form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake website that requests information."[8]
Pharming	"Using technical means to redirect users into accessing a fake website masquerading as a legitimate one and divulging personal information. An attacker corrupts an infrastructure service such as DNS (Domain Name System) causing the subscriber to be misdirected to a forged verifier/relying party, which could cause the subscriber to reveal sensitive information, download harmful software, or contribute to a fraudulent act."[9]
Software-based encryption	"Software-based encryption refers to programs that use a computer's processing power to encrypt data. This type of encryption typically relies on passwords as encryption keys to authenticate users."[10]
Spyware	"Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code."[11]
Sensitive PII	"Sensitive Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised. Some categories of PII are sensitive as stand-alone data elements, including your Social

[6] Sensitive PII - The IT Law Wiki - Fandom
[7] How statistical noise is protecting your data privacy
[8] phishing - Glossary | CSRC (nist.gov)
[9] Pharming - Glossary | CSRC
[10] Software vs. Hardware Encryption: The Pros and Cons (dsolutionsgroup.com)
[11] spyware - Glossary | CSRC (nist.gov)

Term	Definition
	Security number (SSN) and driver's license or state identification number."[12]
Spoofing	Faking the sending address of a transmission to gain illegal entry into a secure system. "Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity."[13]
Virus	"A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk."[14]

[12] DHS Handbook for Safeguarding Sensitive PII
[13] Caller ID Spoofing | Federal Communications Commission (fcc.gov)
[14] virus - Glossary | CSRC (nist.gov)

EXECUTIVE SUMMARY

Approximately, 21 percent of American households submit personally identifiable information (PII) in order to receive public benefits, 13 percent of which do so to receive the Supplemental Nutrition Assistance Program (SNAP).[15] PII includes information that could be used to deduce an individual's identify. This could include immediately identifying details like names and Social Security numbers (SSNs), as well as geographical details like home addresses and phone numbers. While state agencies (SAs) implement policies and practices to safeguard PII collected during SNAP applications, little is systematically known about them.

This study examines how SAs are currently protecting PII of SNAP applicants and participants submitted during applications and maintained in SNAP case files. The study includes a survey administered to all 53 SNAP SAs, supplemented by interviews with industry experts and follow-up interviews with five selected, exemplary SNAP SAs. Using the information captured during these three primary data collection activities, this study compiled best practices by states to protect SNAP PII. This list of best practices identifies barriers to compliance, gaps in knowledge and implementation, and important supports for maintaining PII security.

The study team categorized safeguards into three domains of the procedures that SAs typically implement to safeguard PII: (1) *personnel policies and procedures*, (2) *security policies and procedures*, and (3) *safeguarding practices used during program operations*. In accordance with these conceptual domains, we present the study's key findings.

Personnel Policies and Procedures

This domain pertains to the approaches SAs employ to ensure only appropriate staff have access to SNAP PII, and that those working with PII data have met security requirements such as regular security training and education. Evidence from the SA survey suggests that a vast majority of SAs limit staff access to PII by requiring them to get approval to either modify (93 percent; 41 out of 44 SAs) or access SNAP recipient/applicant data (84 percent; 37 out of 44 SAs). Considering the sensitive nature of SNAP PII, the majority of SAs offer PII training to staff who handle SNAP applicant/recipient data at different levels within their organizations. The findings also reveal variations in the frequency and nature of trainings SAs provide to their staff. For example, based on the interviews with staff from exemplary states, some SAs offered quarterly training while others offered annual training to their staff. For all SAs, however, new staff members are required to complete security training within a specific timeframe, usually within the first three days. Generally, the majority of SAs provide PII training in the following: (1) reasoning behind the requirement of PII (98 percent; 43 out of 44 SAs); (2) procedures for reporting violations to management (98 percent; 43

[15] https://www.census.gov/newsroom/archives/2015-pr/cb15-97.html

out of 44 SAs); and (3) protecting accidental disclosure and penalties for not protecting PII when there is a data breach (98 percent; 43 out of 44 SAs).

Security Policies and Procedures

This domain consists of the policies and procedures the Food and Nutrition Service (FNS) requires to ensure SAs have developed a robust security plan and are securing PII across hardware, software, and networks. The policies also include engaging in assessing risk, vulnerabilities, and security testing. The policies are also meant to include response to security incidents and the measures established to prevent unauthorized access to SNAP PII. The findings from the SA survey indicate that a sizeable number of SAs allow remote access to systems containing PII, but a majority (28.3 percent; 13 out of 46 SAs) only permit remote access to PII data on equipment authorized by the SA. In addition, only 1 SA (2.2 percent) permits staff to remotely access systems containing PII using their personal devices. Due to elaborate policies to respond to and prevent data breaches, many SAs have not experienced such incidents (20.9 percent; 9 out of 43 SAs). Most of the SAs (91.1 percent; 41 out of 45 SAs) conduct regular onsite and offsite backups, especially to a cloud environment, to prevent unauthorized access to SNAP PII on personal computers. The SAs also have policies in place to secure disposal of data (84.4 percent; 38 out of 45 SAs) and have procedures to identify critical areas within their facilities for upgrading especially where SNAP PII is stored (84.4 percent; 38 out of 45 SAs).

> *"I believe we're the largest system running SNAP in a cloud environment. There are a couple other states that are also in the cloud, but I know that we're definitely the largest and that's also been helpful for us as far as being able to manage and maintain a secure system within our cloud environment."*

Staff from exemplary SAs provided additional insights into the security policies and procedure safeguards that their agencies have implemented, as follows—

- SAs implement a robust security plan to provide a consistent baseline for multiple users.
- SAs run SNAP in a cloud environment as an effective approach to securing PII.
- SAs require hard drives to be encrypted now, using BitLocker, for example.
- Some SAs have disabled the "print" button in their case tracking systems to prevent leaks.
- Some SAs do not display full Social Security numbers on our client server applications.
- Some SAs do not allow external memory devices to be plugged into their laptops, which prevents users from downloading any type of data files.
- SAs use role-based access control to restrict system access.

Safeguarding Practices Used During Program Operations

Program operations include the various processes and procedures associated with administering SNAP, such as masking or timeout features used when collecting data from program participants, use of secure data systems when processing PII data to administer program benefits, and matching PII to other data sources to enhance program integrity or verify eligibility. SAs use several national and state data sources for data matching, and the most often used data source is the National Directory of New Hires. The majority of data matching is done using Social Security numbers (SSNs) (88.9 percent; 40 out of 45 SAs), names (86.7 percent; 39 out of 45 SAs), and dates of birth (84.4 percent; 38 out of 45 SAs) of SNAP applicants/recipients. However, there are variations in the process utilized by SAs. Almost all SAs employ some form of encryption method for transmitting, maintaining, and storing PII data. Software- and hardware-based encryption are the most common encryption methods employed to safeguard PII, with 79.5 percent (35 out of 44 SAs) using it for transmitting PII data and 82.2 percent (37 out of 45 SAs) using it for storing PII data. Masking is another alternative, but only a few SAs mask SSNs during data entry (9.1 percent; 4 out of 44 SAs). One staff, from the interviews with exemplary SAs, explained they use masking for the purposes of testing and performing development so that they "don't expose production data to that set of staff within the organization" that do not need to see it. The majority of SAs (95.5 percent; 43 out of 45 SAs), however, have timeout features to protect the PII; although the time for timeout varies across the SAs.

Industry Best Practices for Safeguarding PII

The study team also interviewed experts to determine industry best practices for safeguarding PII that SAs should consider implementing during distinct phases of the data lifecycle, such as information collection, information processing, information transmission and dissemination, information storage, and information destruction. Experts shared their views on PII safeguarding best practices to ensure that staff working with PII have met the security requirements to access data at approved security levels and have received regular security training and education. Industry experts identified general best practices common to the different areas of the data lifecycle, some of which are presented in **Exhibit ES-1.**

Exhibit ES-1 | Industry Best Practices for Safeguarding SNAP PII

Domain	Safeguards
Personnel Security	Implementing least privilege access to ensure users who access PII records only have access to the minimum amount of PII needed to perform their roles.
	Testing controls that ensure SAs are continuously assessing users who need access to various levels of information, and that they are closing out access to individuals when they no longer use the information.

Domain	Safeguards
	Requirements for performing background checks based on access to varying levels of sensitive information.
	Providing initial and ongoing staff training and education related to security awareness and best practices.
	Implementing appropriate controls that ensure staff do not retain sensitive information once they leave their previous position or their position is terminated.
Information Collection	Limiting data collection to the least amount necessary for the SA to provide the service or establish eligibility for SNAP.
	Obtaining consent from applicants prior to the collection of their data, and to give applicants the opportunity to understand the data being collected.
	Providing guidance to SAs on where to conduct interviews with applicants when they may collect applicants' PII.
Information Processing	Implementing controls to ensure users only have access to records they need to perform their function.
	Purging of PII when no longer required, by SAs regularly reviewing its holdings of previously collected PII.
	Encryption of PII in transit and at rest.
	Performing effective access controls around any repository or system that processes PII, and logging and monitoring of activities related to processing of PII.
	Complying with the National Institute of Standards and Technology (NIST), particularly the full set of security and privacy controls related to information processing NIST SP 800-122 and 53 Rev.5.
Information Transmission and Dissemination	Securely restricting the endpoints involved in the transmission, and appropriately securing access to those endpoints.
	Cryptographic encryption with one-way hashes.
	Ensuring adherence to Federal Information Processing Standards Publication 140 (FIPS 140).
	Ensuring adherence to NIST SP 800-122 on effectively de-identifying PII.
	Implementing the concept of differential privacy, where SAs would devise means to not increase participants' risk of exposure.
Information Storage	Broadly encrypting PII at rest within a database.
	Using sound and secure cryptography to perform encryption.
	Implementing access controls when information is stored in the cloud.
Information Destruction	Complying with NIST SP 800-88, Guidelines for Media Sanitation Sanitization methods contained in this publication comprise clear, purge, and destroy.

SAs Capacity to Implement Best Practices

Based on the interviews with staff from exemplary SAs, the study team identified factors that can be considered necessary "ingredients" for ensuring SAs have the capacity to adapt and implement the best practices identified by the industry experts. Below we present these factors about the processes and the key steps that contributed to exemplary SAs achieving a high level of success in safeguarding PII.

- Culture of security, where SAs regard data security as a core value of their agencies.
- Cybersecurity education to create security awareness among staff.
- Effective partnerships with technology vendors and state and county agencies.
- Advancements in technology, such as cloud computing.
- Strong state leadership support.

1. INTRODUCTION

The Supplemental Nutrition Assistance Program (SNAP) is the largest domestic nutrition assistance program in the United States, having served approximately 41.5 million low-income Americans in 2021, with $108.7 billion in benefits provided during that time.[16] These millions of households submit personally identifiable information (PII) in order to receive SNAP benefits. This study examines how SAs are currently protecting PII of SNAP applicants and participants, which is submitted during the application process and maintained in SNAP case files. This study includes a survey of all 53 SNAP SAs, supplemented by interviews with industry experts and follow-up interviews with selected, exemplary SNAP SAs. The study compiled a list of "benchmark practices" by states to safeguard PII, and identified gaps in knowledge and implementation, barriers to compliance, industry best practices, and important supports for maintaining PII security.

SNAP Policy Background and Context

SNAP benefits are funded by the Government through the U.S. Department of Agriculture, Food and Nutrition Service (FNS), but administrative expenses are shared by FNS and SAs. SNAP administrative expenses include those related to information technology (IT) and caseworker wages. As part of their administrative responsibilities, SAs are required to ensure that PII provided by SNAP applicants and participants is properly safeguarded and secure.

The US Government Accountability Office (GAO), in a 2008 report,[17] identified three major areas of agency privacy protection that were most challenging: (1) applying privacy protections consistently to all Federal collection and use of personal information; (2) ensuring that collection and use of PII is limited to a stated purpose; and (3) establishing effective mechanisms for informing the public about privacy protections.

These challenges remain important in protecting SNAP participants' PII. To date, SAs have largely succeeded in keeping SNAP PII safe from compromise and loss as there are no known breaches of SNAP data. However, the following three issues suggest a need for more focus on this area: (1) the growing amount of data stored by SAs (and by government as a whole); (2) the degree to which PII is shared or matched with data from multiple state and federal agencies; and (3) the increasingly sophisticated methods for breaching data.

These trends (as well as limited resources in many SAs) have left many states behind in the race to fend off threats to data security. The contexts in which SAs operate also contribute to inadequate levels of PII security. Based on discussions with SNAP experts and FNS and

[16] Supplemental Nutrition Assistance Program Participation and Costs Data as of July 1, 2022. Accessed from https://fns-prod.azureedge.us/sites/default/files/resource-files/SNAPsummary-7.pdf
[17] GAO (2008). Privacy. Alternatives exist for enhancing protection of personally identifiable information. Retrieved from https://www.gao.gov/new.items/d08536.pdf

reviews of pertinent documents and reports,[18] these contextual factors include the following:

- Use of vendor company security services that are inadequate or outdated.
- Providing unnecessary access to staff that do not require PII to perform their assigned job duties.
- Inadequate alignment between the safeguards used by SAs and other state social service agencies.
- Insufficient resources for IT system security development, security staff expertise, and/or ability to fully implement security protocols.
- Focus on other work that has higher and more immediate priority.
- Specific features of the SNAP system that involve PII, such as benefit delivery through Electronic Benefits Transfer (EBT); systematic data sharing with other federal and state agencies as required to prevent fraud and abuse; and ensuring that children receiving SNAP benefits receive free school meals.

These factors may cumulatively lead to a situation in which SAs do not have the time, resources, or expertise to prevent security breaches and take appropriate corrective steps if compromise occurs. Some SAs also may be unfamiliar with multipronged efforts to safeguard PII that other states or entities in private industry have implemented.

Study Objectives and Research Questions

This study has five main objectives:

1. Describe legislation, regulations, and policies that address safeguarding SNAP participant PII.
2. Describe methods that can be used to safeguard PII.
3. Describe how states currently safeguard participant PII.
4. Examine the consistency of safeguarding practices across states.
5. Provide recommendations to states for improved safeguarding of PII.

For each objective, the study team identified methods of data collection and analysis associated with specific research questions (RQs). Each objective and corresponding RQs are shown in **Exhibit 1-1**.

[18] Deloitte, LLP, National Association of State Chief Information Officers. (2018). *2018 Deloitte-NASIO Cybersecurity Study – States at risk: Bold plays for change.* Washington, DC: Deloitte.
U.S. Department of Agriculture, Food and Nutrition Service. (2017). *FNS handbook 901: The advance planning document process: A state systems guide to America's food programs*. Washington, DC: U.S. Department of Agriculture.

Exhibit 1-1 | Research Questions by Research Objective and Associated Methods of Data Collection and Analysis

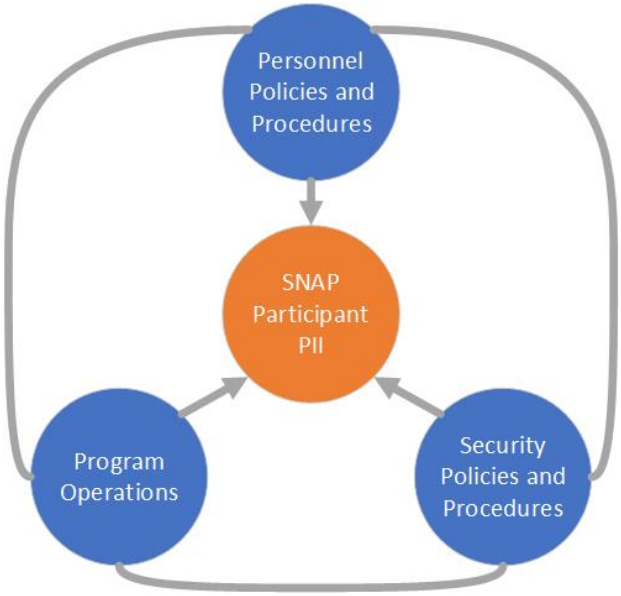
Research Objectives and Research Questions	Data Collection Methods				Methods of Analysis
	Document Review	Interviews with Industry Experts	Interviews with Staff from Exemplary SAs	Web Survey	
Objective 1: Describe legislation, regulations, and policy that address safeguarding SNAP Participant Data					
1.1 What federal legislation addresses SAs and Federal Government agencies' handling of PII? What legislation specifically addresses SNAP participants' PII?	X				Document Review
1.2 What federal regulations address SAs and Federal Government agencies' handling of PII? What regulations specifically address SNAP participants' PII?	X				Document Review
1.3 What additional guidance has FNS provided SAs in regard to handling PII?	X				Document Review
1.4 What state legislation and regulations govern SAs' handling of PII?	X				Document Review
1.5 Describe the National Institute of Standards and Technology (NIST) guidelines.	X				Document Review
Objective 2: Describe methods that can be used to safeguard PII					
2.1 What measures are established to prevent unauthorized users from accessing PII?		X	X		Qualitative Coding
2.2 Are appropriate role permissions established to limit PII access to authorized individuals only? If so, what are they?		X	X		Qualitative Coding
2.3 Does the state allow remote access to systems containing PII? If so, what is the process?		X	X	X	Qualitative Coding and Descriptive Tabulations
2.4 Is masking used in PII data entry, particularly for SSNs?		X	X	X	Qualitative Coding and Descriptive Tabulations
2.5 Is there a timeout function used on application screens that contain PII? If so, what is the time limit for the timeout? What policy or guidance covers timeout functions?		X	X	X	Qualitative Coding and Descriptive Tabulations

Research Objectives and Research Questions	Data Collection Methods				Methods of Analysis
	Document Review	Interviews with Industry Experts	Interviews with Staff from Exemplary SAs	Web Survey	
2.6 Are encryption methods used for transmitting and storing PII? If so, what are the methods in place?		X	X	X	Qualitative Coding and Descriptive Tabulations
Objective 3: Describe how states currently safeguard participant PII					
3.1 What vulnerabilities and threats to privacy have states encountered?		X	X	X	Qualitative Coding and Descriptive Tabulations
3.2 When states perform data matches of state SNAP administrative data with other administrative data, what data files do states perform matches with? What PII is used for linking the files? How do states protect confidentiality in files produced by data matching? How does PII and confidentiality protection vary among different data matches?			X		Qualitative Coding
3.3 How do states handle law enforcement requests for PII?			X		Qualitative Coding
3.4 Do states follow the Federal Information Security Management Act (FISMA) or NIST guidelines?				X	Descriptive Tabulations
3.5 What is the training process to ensure personnel understand their responsibilities in protecting PII?				X	Descriptive Tabulations
3.6 Which states have had data breaches? What has been the response?		X		X	Qualitative Coding and Descriptive Tabulations
3.7 How secure is the transmission of online application data? How is the confidentiality of paper applications secured?		X	X	X	Qualitative Coding and Descriptive Tabulations
3.8 How do safeguarding practices differ between states with county-administered SNAP versus those with statewide administration?			X	X	Qualitative Coding and Descriptive Tabulations
3.9 What other measures has the state implemented to ensure the protection of PII?			X	X	Qualitative Coding and Descriptive Tabulations

Research Objectives and Research Questions	Data Collection Methods				Methods of Analysis
	Document Review	Interviews with Industry Experts	Interviews with Staff from Exemplary SAs	Web Survey	
Objective 4: Examine the consistency of safeguarding practices across states					
4.1 What are the safeguarding practices that vary the most among states?			X	X	Qualitative Coding and Descriptive Tabulations
4.2 What are the safeguarding practices that are most often practiced within states?			X	X	Qualitative Coding and Descriptive Tabulations
4.3 In which areas are the safeguarding practices of states most in need of improvement?				X	Descriptive Tabulations; Possibly Contingency Tables or Cluster Analysis
Objective 5: Provide recommendations to states for improved safeguarding of PII					
5.1 What best practices should states implement to ensure the safeguarding of PII?		X	X	X	Qualitative Coding and Descriptive Tabulations

Conceptual Framework

Exhibit 1-2 | Conceptual Framework



SAs face common threats and vulnerabilities related to safeguarding applicant and participant PII. To mitigate these threats and vulnerabilities, SAs can adopt and implement an array of safeguards that fall into one of three domains:

- **Personnel policies and procedures** are how SAs ensure that staff working with PII data have met security requirements and receive regular security training and education.
- **Security policies and procedures** are what FNS requires to ensure SAs have developed a robust security plan; are subsequently securing PII across hardware, software, and networks; and are regularly engaged in assessing risk, vulnerabilities, and security testing.
- **Safeguarding practices used during program operation** are the processes and procedures for administering SNAP, such as masking or timeout features used when collecting data from program participants, use of secure data systems when processing PII data to administer program benefits, and matching PII to other data sources to enhance program integrity or verify eligibility.

These three domains and their associated safeguards provide a comprehensive approach to safeguarding the PII of SNAP participants. For each domain, the study team identified a collection of associated safeguards including the citation of the sources from which the safeguards were identified during the review of applicable rules, regulations, and pertinent documents while answering Study Objective 1 (See **Appendix A** for more details).

Organization of the Report

The report is organized into five sections. Following this introduction, Chapter 2 describes the study methodology, including methods the study team used to develop each sample as well as the processes followed to collect and analyze the data from each sample. Chapter 3 presents the findings on SAs current practices to safeguard PII, drawing largely from the web survey and, where appropriate, findings from industry-expert interviews. Chapter 4 covers the development of best practice recommendations for SAs, based largely on interviews with industry experts. Chapter 5 concludes the study.

2. METHODOLOGY AND DATA COLLECTION APPROACH

This section describes the methodology to identify and assess how states safeguard SNAP PII and provide details on the study design, sampling strategy, data collection and analysis, challenges encountered, and the limitations of the study.

Overview of the Study Design and Sampling Strategy

The study team employed a mixed method evaluation approach that draws from both qualitative and quantitative data sources. Because the RQs are multifaceted, the study team employed different sampling strategies to collect the data. The study invited all 53 SAs that administer the SNAP program to participate in the web survey. This included SAs for the 50 states, the District of Columbia, and two U.S. territories: Guam and the U.S. Virgin Islands. The study team employed a modified snowball sampling method to identify and conduct eight interviews with industry experts with extensive knowledge in IT, SNAP data collection and management, EBT, and privacy protection legislation based on the recommendation from FNS and the industry experts themselves.[19] Finally, the study team interviewed program and IT staff from five states that have exemplary practices regarding safeguarding PII, according to their responses in the web survey.

Approaches to Data Collection

Web Survey of State Agencies

The web-based survey was employed to collect data on SAs' approaches to prevent and mitigate threats to PII, familiarity with and implementation of laws governing PII protection, staff knowledge of their SA's policies and procedures, and compliance with benchmark practices. The data collection period for the web survey was September 10, 2021 through January 31, 2022. Out of the 53 SNAP SA directors that were invited to participate, 47 SAs completed more than 60 percent of the survey—an 88.7 percent response rate. A review of the survey items for the 47 SAs that were considered to have completed the web survey showed that 89.8 percent of the survey questions were answered by at least 80 percent of SAs. Of the 47 SAs, 39 were state administered and the remaining eight were county administered.

Interviews with Industry Experts

This phase of the study consisted of interviews with eight experts to discuss their broader views of PII protection from private industry and public sector perspectives, and to clarify both private industry and public sector benchmarks for information security, thereby

[19] The project's Subject Matter Experts (SMEs), Ms. Ann Collins and Mr. Larry Goolsby, contributed to the understanding of SNAP SA procedures for maintaining and safeguarding participants' PII throughout the project.

informing recommendations for SNAP SAs for improving their procedures and processes for safeguarding SNAP participants' PII. 2M used a modified snowball sampling approach to identify industry experts in the fields of IT, data privacy protection, SNAP outreach, and EBT and SNAP benefit redemption. A preliminary list of experts was developed from a list recommended by the USDA FNS, the study's subject matter experts, and industry experts identified by the 2M study team. Experts who agreed to participate in the interviews were asked to provide their availability for the interview; those who declined were encouraged to recommend other experts who might be willing to participate. During the interviews, the study team also inquired about additional experts from the interviewee's organization or network whom the study team may want to interview. FNS and the study team reviewed the names provided and interviewed experts deemed appropriate for the project.

Interviews with Exemplary State Agencies

For this component of the study, we interviewed staff from five SAs about their broader views on effective practices for safeguarding SNAP PII. Based on survey responses, industry expert interviews, and consultations with FNS and other SNAP experts, we reached out to staff from SAs deemed exemplary in safeguarding SNAP PII. We identified these exemplary SAs using a scoring method that helped rank the SAs by their performance across the three domains of the study. Please see **Appendix B** for more details on our approach to selecting and recruiting interview participants. 2M selected an initial list of 11 exemplary SAs. This list provided options for FNS to determine the group of exemplary SAs that most effectively met its priorities, as well as alternates if a selected SA declined to participate in this phase of the study. FNS selected the following five SAs for interview: Oklahoma, South Carolina, North Dakota, California, and New Jersey.[20] Next, the study team began recruiting and scheduling interviews with SA staff most knowledgeable about the procedures and processes for safeguarding PII of SNAP participants. 2M designed the semi-structured interviews with exemplary SAs to discover lessons learned, uncover information about staff experiences protecting PII, and glean on-the-ground insights that can be used to create strategies for improving PII-protection practices.

The study team also leveraged data from secondary sources, including the laws, regulations, and policies cited in the Objective 1 RQs (see **Exhibit 1-1** and **Appendix A**). The study team also extracted information on state legislation and regulations that govern SAs' handling of PII from FNS, state websites, and those of related agencies such as the National Association of State Chief Information Officers.

[20] Nebraska, Indiana, Missouri, and Kentucky were potential back-ups that the study team did not contact.

Approach to Data Analysis

Quantitative Survey Analysis

The study team tabulated survey responses and generated descriptive statistics for all survey items. This provided an overview of the prevalence of and variation in specific practices, and the degree to which SA staff are aware of legislation, regulations, and guidelines regarding safeguarding PII. The study team also examined regional variation in the implementation and understanding of best practices among SAs (See **Appendix B** for more details).

Qualitative Interview Data Analysis

A robust analysis of the information collected in the industry expert and exemplary SAs interviews was vital for answering the study's research questions and furthering FNS' knowledge of industry best practices associated with safeguarding SNAP PII. Accordingly, the research team implemented a rigorous qualitative analysis of the interview data to ensure subsequent findings gave FNS a greater insight into SAs effective practices for safeguarding SNAP PII. The interview summary reports were uploaded into NVivo software to facilitate qualitative analysis. The study team coded the interviews by using a multistep procedure for semi-structured interview transcripts (See **Appendix B** for more details).

Methodological Limitations

The study was designed to collect pertinent survey and interview data on best practices associated with SNAP PII and rigorously analyze the data to answer key research questions while mitigating methodological limitations. Despite the study team's efforts, we had difficulty recruiting industry experts with SNAP SA expertise for the second phase of the study (interviews with industry experts). Of the industry experts we interviewed, only two had direct experience working with SNAP SAs. One expert's experience related to SNAP outreach, which is driven by matching SNAP records to other public assistance programs that are then used to identify eligible individuals. The other expert's experience related to SNAP EBT and benefit redemption operations. Accordingly, the study team was unable to obtain as detailed information as we would have liked. The study team filled this gap by leveraging the multiple data sources of the study, especially through interviews with staff from exemplary SAs. As noted earlier, the interviews with exemplary SAs focused on staff experiences in protecting PII, lessons learned, and on-the-ground insights for improving PII practices.

3. STATES' CURRENT PRACTICES TO SAFEGUARD PII

This section presents the findings of the web survey and, where appropriate, supplements findings from industry-expert interviews. This chapter addresses Study Objectives 2, 3, and 4, and it is organized around the RQs associated with those objectives and the domains of the study. Study Objective 1 is addressed in **Appendix A**.

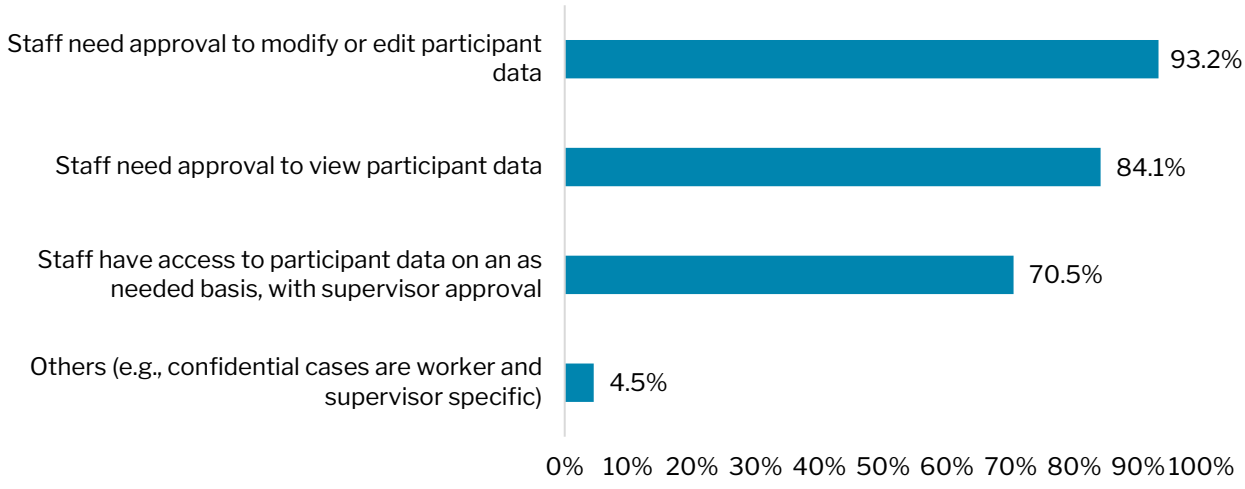
Personnel Policies and Procedures

This section pertains to how SAs ensure that only staff requiring access to SNAP PII data have it, and staff working with PII data have met requisite security requirements and receive regular security training and education.

Type of Role Permissions Established to Limit Access to PII data

Exhibit 3-1 depicts the role permissions established to limit access to SNAP PII data. Among the 44 SAs that responded, the most common permission employed by SAs to limit staff access to PII data is for them to get approval to either modify or edit participant data (93.2 percent). Another 84.1 percent of SAs (n=37 SAs) indicated that they require their staff to seek approval to view participant data, but do not have the permission to modify/edit contents. Approximately 70 percent of SAs (n=31 SAs) are provided access to participant data for a specific purpose authorized by their supervisors.

Exhibit 3-1 | Type of Role Permissions Established to Limit Access to PII Data

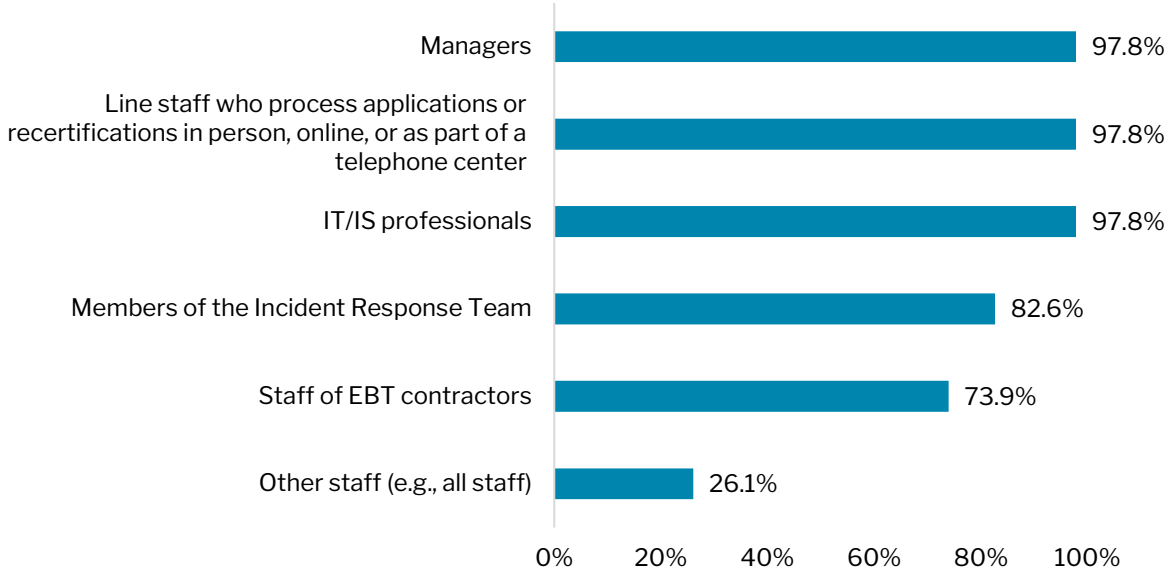


Notes: Findings about type of role permissions established to limit access to PII data are based on the responses from 44 SAs; total sample size = 47. Additional types of role permissions were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 3.2.

Training Process to Ensure Personnel Understand their Responsibilities in Protecting PII

Nearly all SAs (97.8 percent) indicated that they provide PII training to managers, staff who process applications/recertification, and IT/IS professionals (see Exhibit 3-2). More than 4 in 5 (82.6 percent) also provided training to members of the incident response team, whereas slightly less than 3 out of 4 SAs (73.9 percent) provided training to staff of EBT contractors. Overall, most SAs ensure that personnel receive sufficient training to understand their role and responsibility in protecting PII. These trainings are provided at regular intervals to maintain awareness among staff.

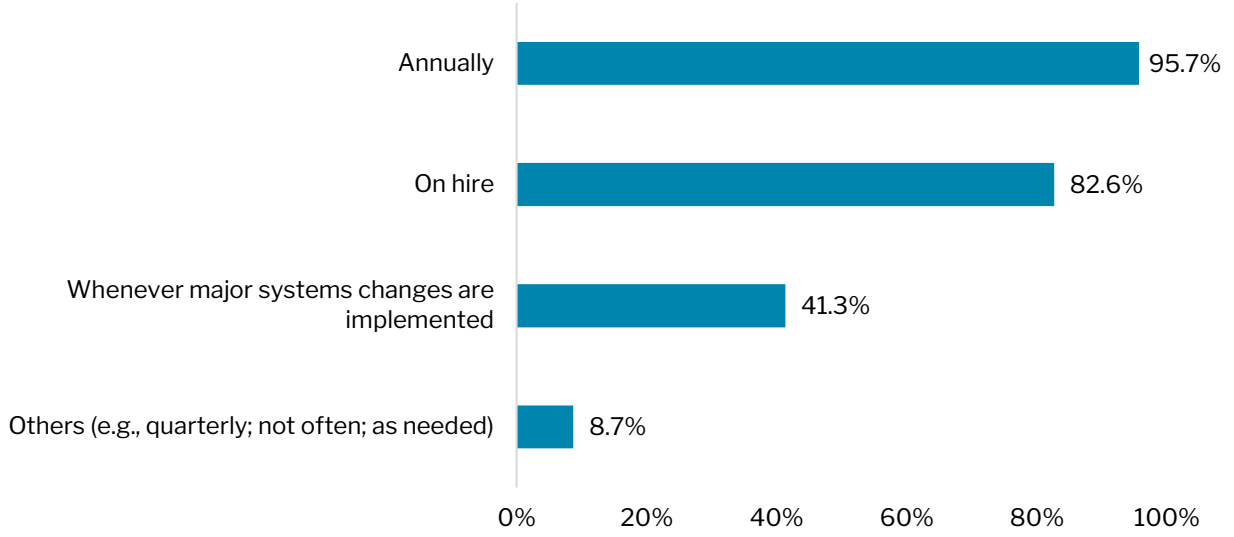
Exhibit 3-2 | Staff by Type that Receive Training on PII



Notes: Findings about the type of staff that receive training on PII are based on the responses from 46 SAs; total sample size = 47. Additional types of staff were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 3.3.

Regarding how often SAs conduct PII training, almost all SAs (95.7 percent) reported that they provide PII training annually, while 82.6 percent of SAs (n=38 SAs) provided training as part of the hiring process (see Exhibit 3-3). Less than half of the SAs (n=19 SAs; 41.3 percent) reported that they provide training during system upgrade. SAs utilize various training methods, but most use online training methods. Nearly 90 percent of SAs (n= 40 SAs) reported that they provide self-paced online training. To a lesser extent, SAs also indicated that they provide PII training online in a group setting (n=18 SAs; 40 percent), while 31.1 percent of SAs (n=14 SAs) indicated that they provide this training through a webinar.

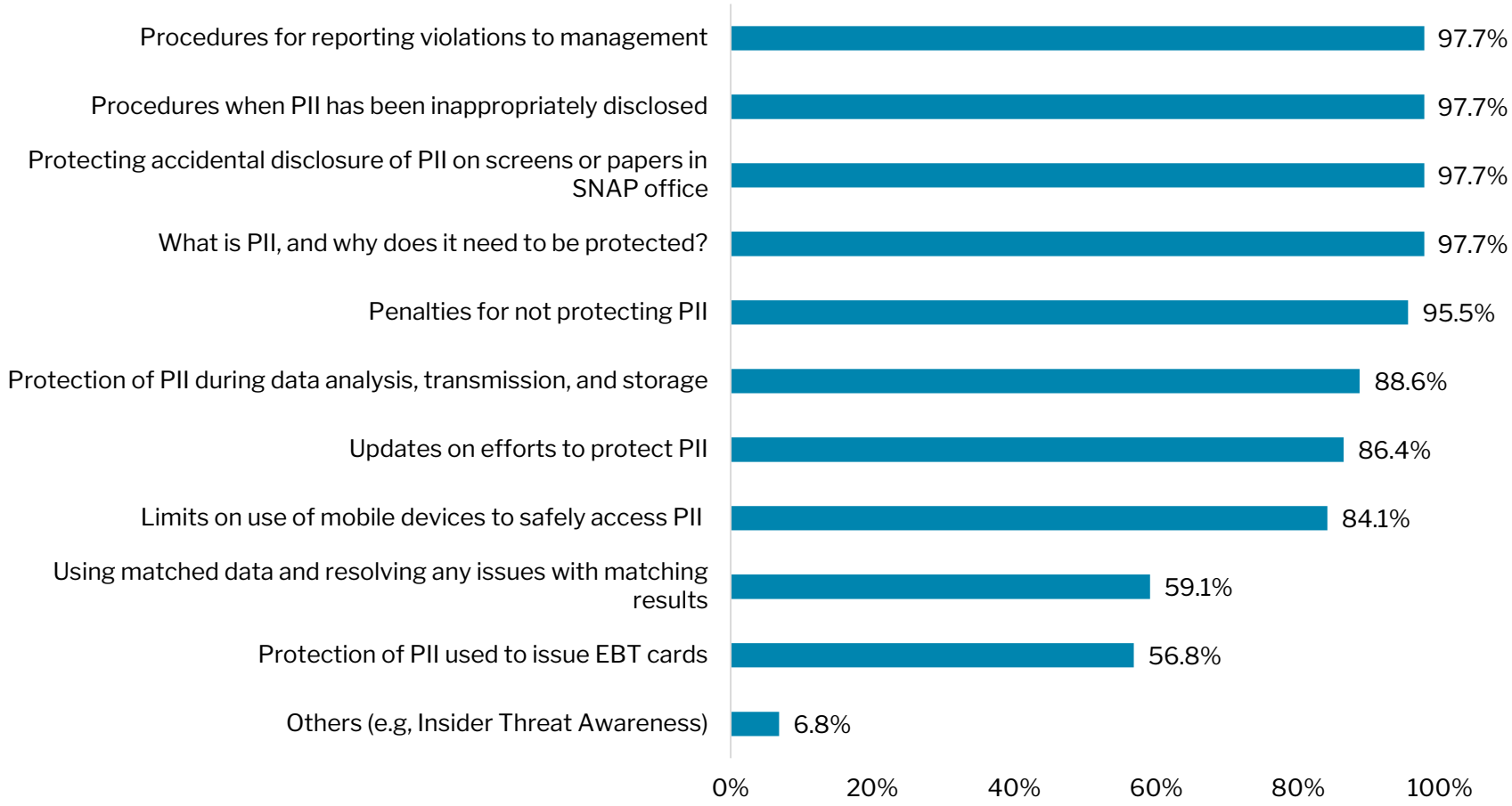
Exhibit 3-3 | Frequency of Training the Majority of Staff with Access to PII



Notes: Findings about the frequency of training the majority of staff with access to PII are based on the responses from 46 SAs; total sample size = 47. Additional frequencies were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 3.5.

Exhibit 3-4 shows the main components that are part of the PII training. These include asking what PII is and why it needs to be protected; procedures for reporting violations to management and for when PII has been inappropriately disclosed; protecting accidental disclosure; and penalties for not protecting PII. Since trainings have been identified as the primary method of raising awareness among staff, these components are quite consistent across SAs, irrespective of their training method or frequency.

Exhibit 3-4 | Major Components of the PII Training



Notes: Findings about major components of the PII training are based on the responses from 44 SAs; total sample size = 47. Additional components were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 3.8.

The findings on personnel policies and procedures from the web survey are largely consistent with the findings from the interviews with exemplary SAs.

"*We do quarterly training with staff. Another thing we also do is we sent phishing emails as well just to test their aptitude on how they click on suspicious emails or are they responding to or replying to those emails, or they click on attachments. We kind of get all those metrics and that really helps us shape the focus of our cyber security education efforts.*"

Staff from all five SAs overwhelmingly indicated training as a resource that helps program staff and vendors ensure the confidentiality of applicant and participant data. The frequency of training varied by SAs, with two SAs offering quarterly training, and the other three SAs offering annual training. But for all SAs, new staff members are required to complete security training within a specific timeframe, usually within the first 3 days. For some SAs, certain positions require special training. For example, staff members in special security roles require supplemental training. Generally, the SAs noted they follow federal requirements based on the NIST SP 800-53 framework and implemented through their system security plans to design their training programs.

While many exemplary SAs did not provide details about the mode of their training, staff from one SA noted they offer security training through an automated and interactive learning management system that notifies staff about mandatory training and compliance deadlines. Another staff also mentioned a type of mediated training assigned to users based on how well they perform on the universal training.

For example, the staff noted, "*If a user failed three or more phishing emails in a 12-month period, they get additional training. So, we kind of look at it as not admonishing them but knowing that they also kind of serve as a threat to the network and our data.*"

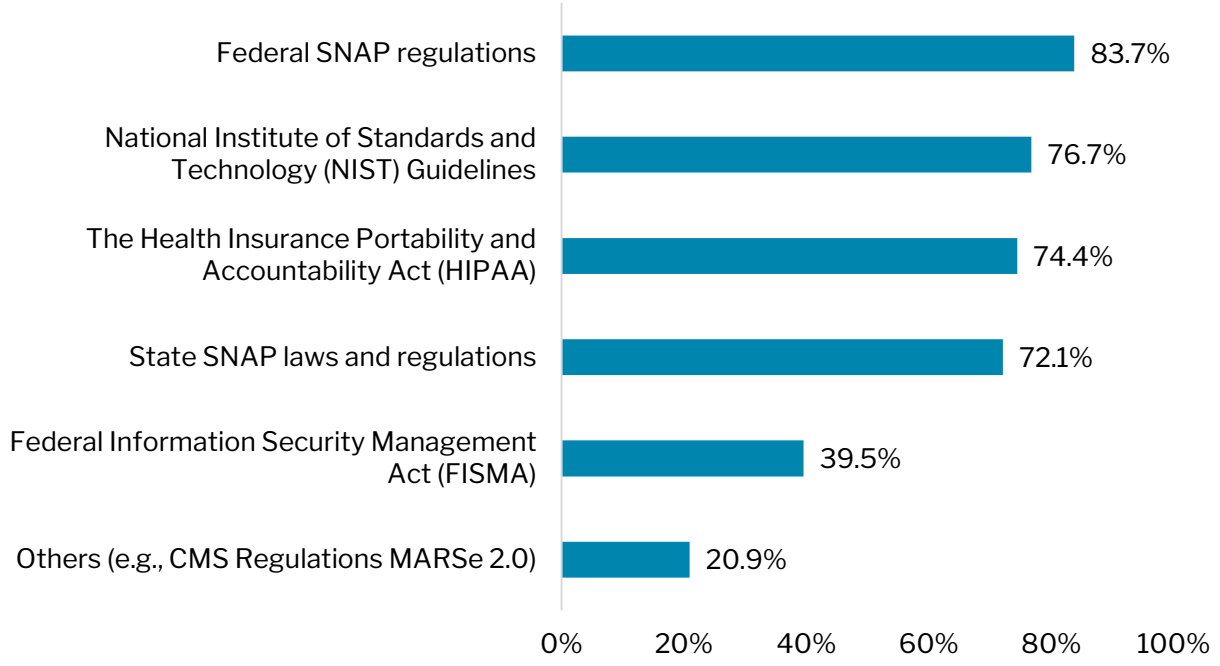
Security Policies and Procedures

This section consists of the policies and procedures FNS requires to ensure SAs have developed a robust security plan; are subsequently securing PII across hardware, software, and networks; and are regularly engaged in assessing risk, vulnerabilities, and security testing.

SA's Adherence to Various Federal and State Policy Guidelines

SAs' policies to safeguard SNAP PII are based on various federal and state policy guidelines. As depicted in Exhibit 3-5, 83.7 percent of SAs (n=36 SAs) indicated that their policies to safeguard PII data are based on federal SNAP regulations. Approximately three-fourths of SAs reported that their policies are based on the NIST guidelines (n=33 SAs; 76.7 percent), Health Insurance Portability and Accountability Act (HIPAA) guidelines (n = 32 SAs; 74.4 percent), and state SNAP laws and regulations (n = 31 SAs; 72.1 percent). Less than half of SAs (n=17 SAs; 39.5 percent) also indicated that their policies are based on the Federal Information Security Management Act (FISMA).

Exhibit 3-5 | SA's Policy was Based on Various Federal and State Policy Guidelines



Notes: Findings about which federal and states guidelines were used for SA's policy are based on the responses from 43 SAs; total sample size = 47. Additional guidelines were specified in an open-text response; the open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 2.2.

Vulnerabilities and Threats to Privacy Encountered by States

Interviews with industry experts helped isolate vulnerabilities and threats to privacy that SAs encounter. Throughout the interviews, experts identified general, internal, and external threats to safeguard PII in electronic databases and files that contain SNAP applications or case files. One respondent identified a lack of clear and consistent guidance concerning compliance with data security protocols as a general vulnerability. They described a large amount of variability across states in terms of how data security compliance is implemented and prioritized, implying that many programs may not give much thought to data security compliance because they are unaware of federal guidance or established best practices.

Another expert noted that most successful security attacks are often internal due to the way employees access information. They explained that often an employee receives a phishing e-mail and clicks on a link that gives the attacker that employee's information and, therefore, the ability to access PII data. This suggests that the greatest internal threat would be a lack of employee knowledge surrounding data privacy and IT attacks. Another respondent identified publicly available datasets as an external threat to data security. While a publicly available dataset would have any identifiers removed, it can be combined with

another dataset, such as voter registration records, to reveal PII information. So, states need to ensure their data systems are not vulnerable to both internal and external threats and need to have procedures in place to safeguard PII from these types of threats.

Consistent with the findings from the web survey, staff from exemplary SAs noted a lot of their legislation and regulations that govern their handling of PII are based on the federal standards that are more applicable to the programs they administer than their own state legislations. These federal regulations include NIST SP 800-53 Rev. 5, the Department of Homeland Security (DHS) HR Policy Manual, Internal Revenue Code (IRC) Section 6103, and the Social Security Administration (SSA) Privacy Act of 1974.

"*I haven't seen any state legislation with regard to protecting information since I've been in my position. All of our SNAP policy that we receive is through the federal regulations. So, anything we change with the federal regulations comes from rules or laws that have been passed by Congress, typically in the Farm Bill*."

NIST SP 800-53 provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets. These include PII processing and transparency and personnel security. Staff from one SA noted they have enterprise architecture standards built upon NIST SP 800-53 framework, which provide details on how to handle sensitive information such as "desktops having an encrypted hard drive." Based on this framework, the staff added they "just moved to a 15-character password for user access to strengthen the authentication standards." On the IRS and SSA guidelines, staff from one SA explained they are the data transmission agency for their state for Social Security information, thus, they have computer matching agreements with both IRS and SSA. In addition to these federal regulations, staff from two out of the five SAs were able to identify their applicable state legislations and regulations that govern PII security.

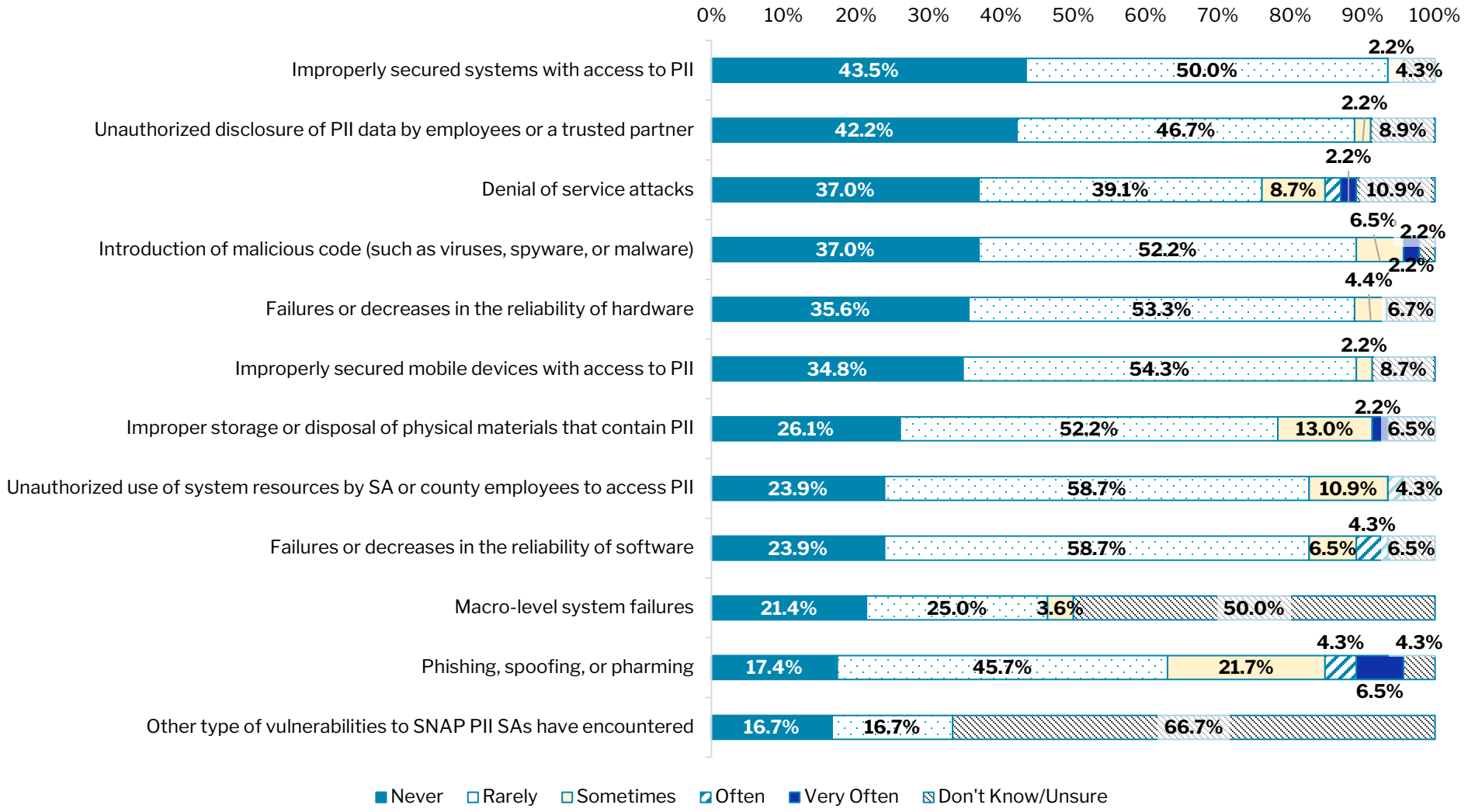
In the web survey, SA themselves rated the internal vulnerabilities and external threats they have encountered. The majority of SAs reported never or rarely encountering external attacks (see Exhibit 3-6). Only 10.9 percent of SAs (n=5 SAs) reported that they encounter phishing, spoofing, or pharming very often. Another 2.2 percent of SAs (n=1 SA) indicated that they encounter malicious code very often. Regarding internal vulnerabilities, the majority of SAs also reported that they have never/rarely encountered threats of that nature. Out of 46 SAs, only 1 SA (2.2 percent of SAs) indicated it improperly stores or disposes physical materials that contain PII very often. Another 4.3 percent of SAs (n=2 SAs) reported that their software is most often not reliable.

SA's Plans/Policies for Responding to Security Incidents

SAs were asked to indicate whether they have experienced data breaches and the policies in place to either prevent/respond to such incidents (see Exhibit 3-7). Almost 56 percent of SAs (n=24 SAs) indicated that they have not experienced any data breaches. Only 1 in 5 SAs (n=9 SAs; 20.9 percent) reported experiencing some form of data breaches in the past, while 23.3 percent of SAs (n=10 SAs) were unsure. A vast majority of SAs (97.8 percent)

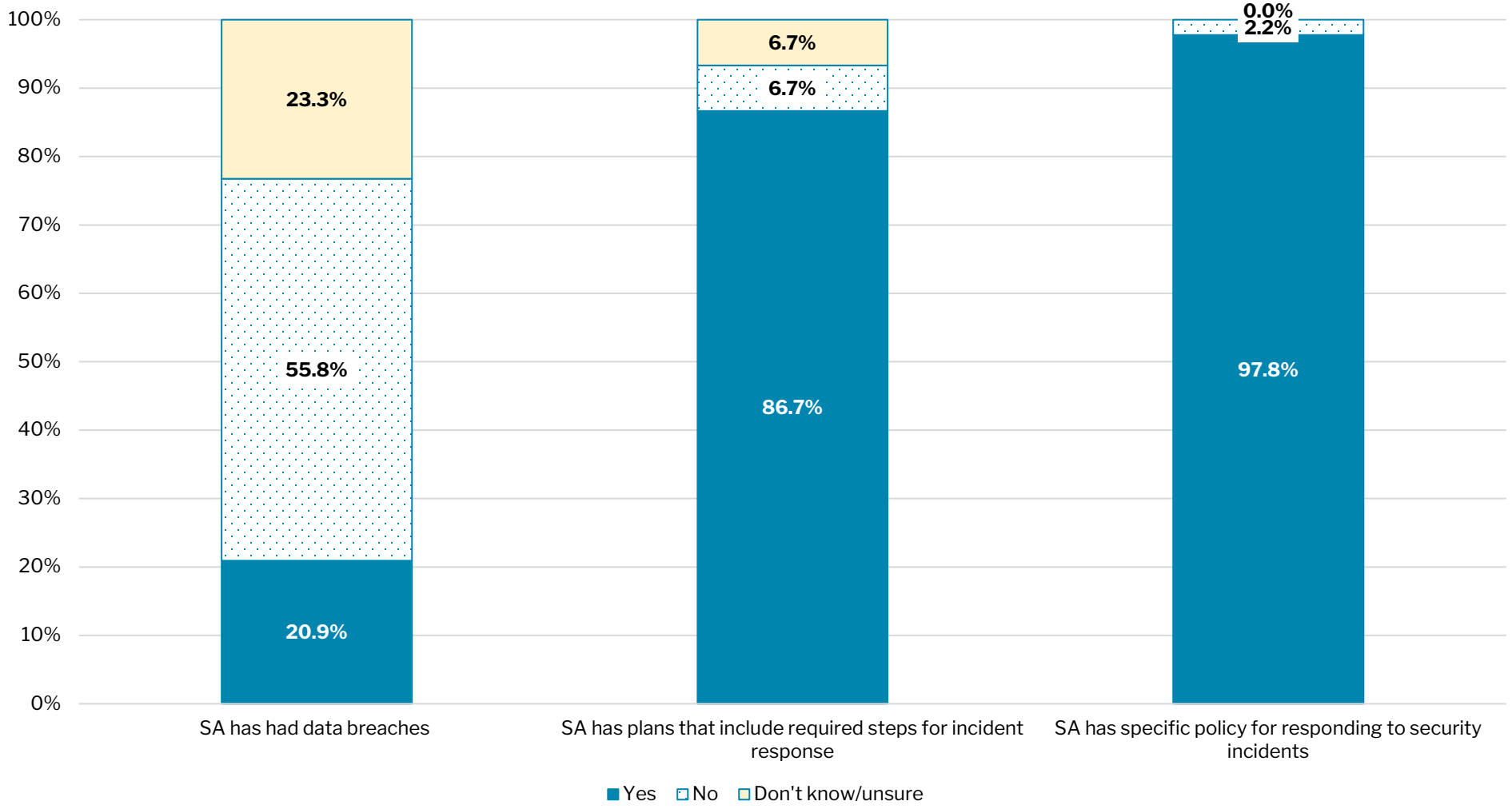
stated they have policies for responding to security incidents. Approximately 87 percent of SAs have well-defined steps in place to respond to a security breach as a part of the said policy.

Exhibit 3-6 | SA's Rating of Internal Vulnerabilities and External Threats They Have Encountered



Notes: Number of responses varies for each type of internal vulnerability and external threat; total sample size = 47.
Source: SNAP PII State Agency Survey, question 4.1.

Exhibit 3-7 | SA's Plans/Policies for Responding to Security Incidents

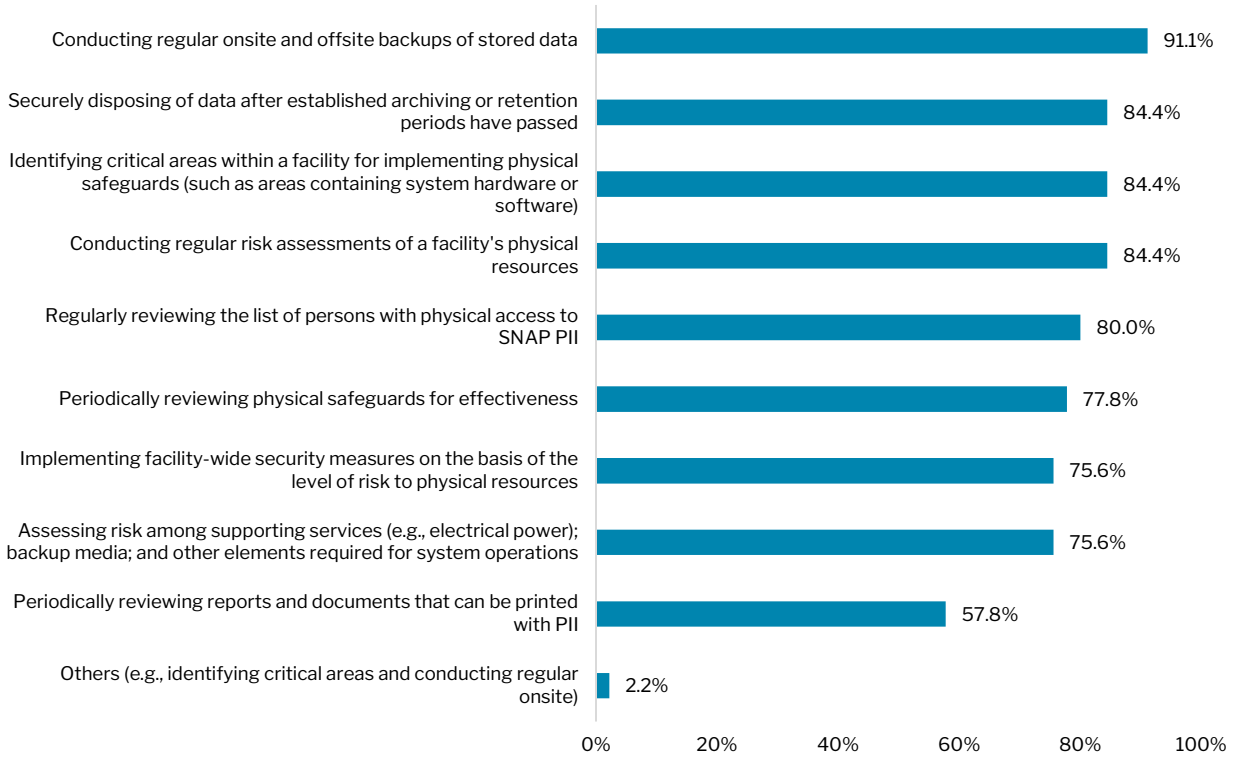


Notes: Number of responses varies for each survey item; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 5.13, 5.14, and 5.15.

Measures Established to Prevent Unauthorized Users from Accessing PII

Exhibit 3-8 summarizes the measures implemented by SAs to prevent unauthorized physical access to stored SNAP PII. Almost all SAs (n=41 SAs; 91.1 percent) reported that they conduct regular onsite and offsite backups of stored data to prevent data loss and limit unauthorized access to the data. Industry experts explained that regular backups protect stored data from unauthorized access by keeping copies in secured facilities offsite or in an encrypted cloud environment. Nearly 84 percent of SAs (n=38 SAs) indicated that they conduct regular risk assessments of their facilities' physical resources, securely dispose of data, and identify critical areas of facility for upgrading. Three in four SAs (n=34 SAs) indicated that they implement facility-wide security measures based on the level of risk to physical resources. About three in five SAs (n= 26 SAs) reported that they review reports and documents that can be printed with PII periodically.

Exhibit 3-8 | Measures Implemented by SAs to Prevent Unauthorized Physical Access to Stored SNAP PII

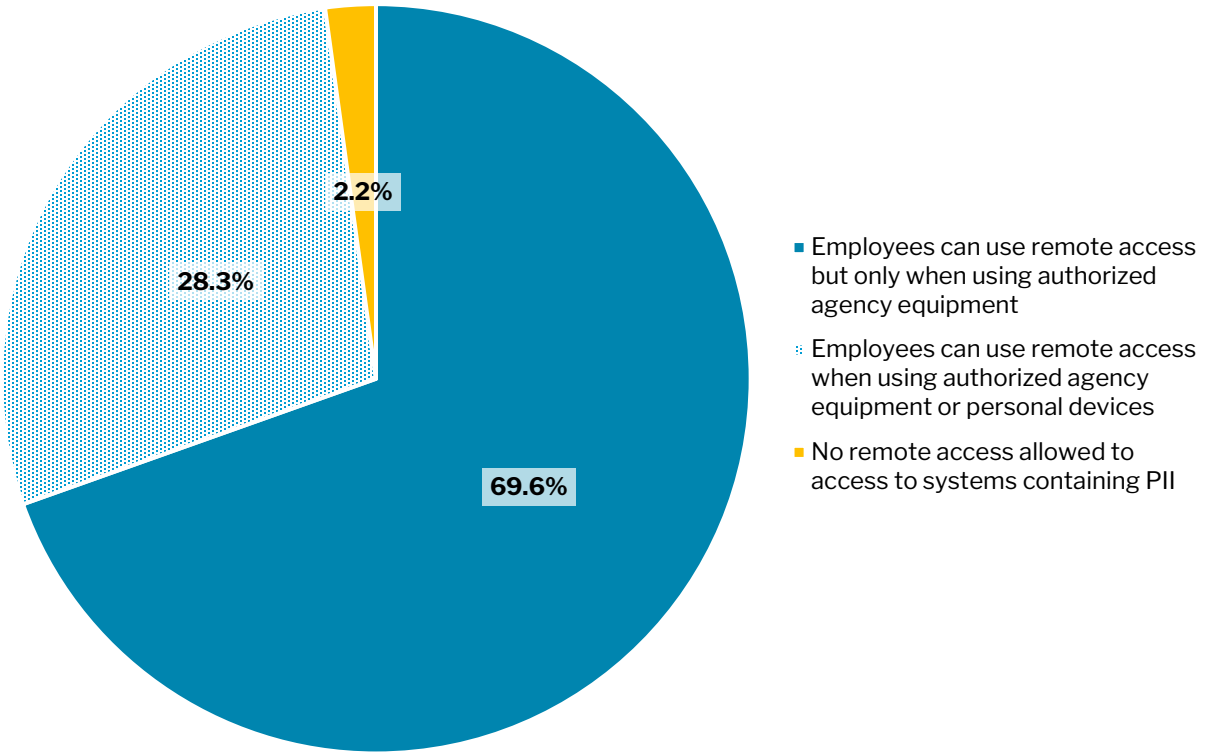


Notes: Findings about measures implemented by SAs to prevent unauthorized physical access to stored SNAP PII are based on the responses from 45 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 6.1.

SA's Policies Regarding Remote Access to Systems Containing PII

Nearly all SAs allowed remote access to systems containing PII, but their implementation of remote access varied. As detailed in Exhibit 3-9, almost all SAs allowed employees to use equipment authorized by the agency to remotely access systems containing PII; however, only 28.3 percent of SAs permitted employees to use their personal devices to remotely access systems containing PII. One SA does not allow remote access to systems containing PII.

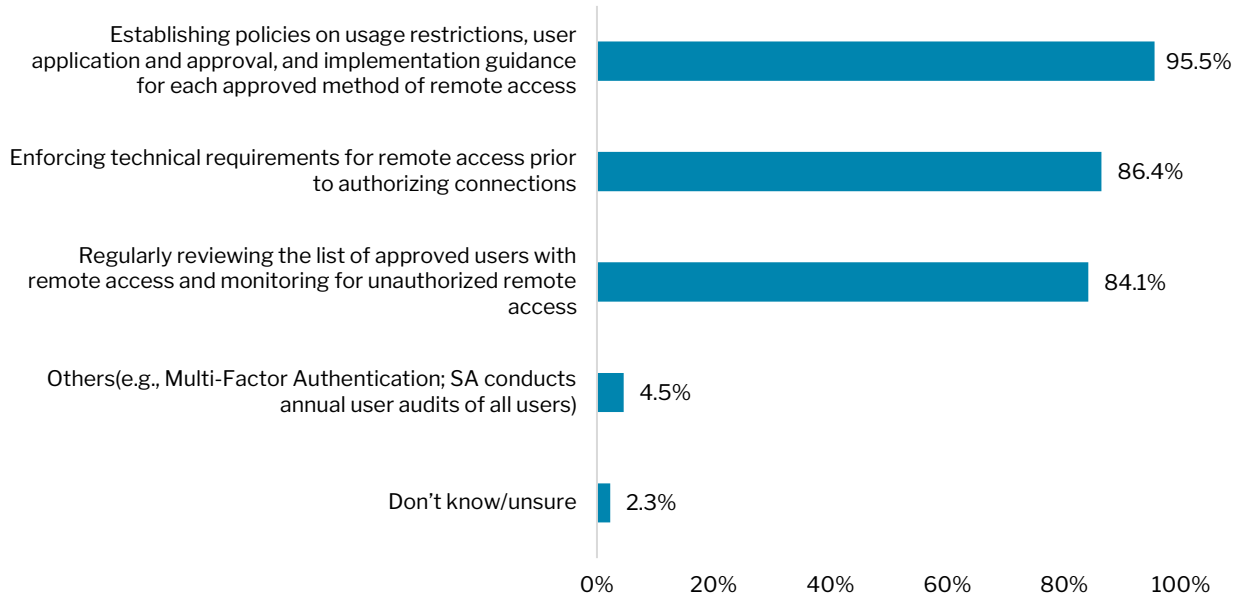
Exhibit 3-9 | Whether SAs Allow Employees Remote Access to Systems Containing PII



Notes: Findings about whether SA allow employees remote access to systems containing the PII are based on the responses from 46 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 4.4.

Regarding the procedures SAs have implemented to allow state or county employees remote access to PII (see Exhibit 3-10), a large proportion of SAs (95.5 percent) have established policies on usage restrictions, user application and approval, and implementation guidance for each approved method of remote access. A sizable number of SAs (86.4 percent) reported that they enforce technical requirements for remote access prior to authorizing connections. Nearly 84 percent of SAs (n= 37 SAs) indicated they regularly review the list of approved users with remote access and monitor for unauthorized remote access.

Exhibit 3-10 | Procedures SA Implemented for Providing State or County Employees with Remote Access to PII



Notes: Findings about procedures SA implemented for providing state or county employees with remote access to PII are based on the responses from 44 SAs; total sample size = 47. Additional procedures were specified in an open-text response; one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 4.5.

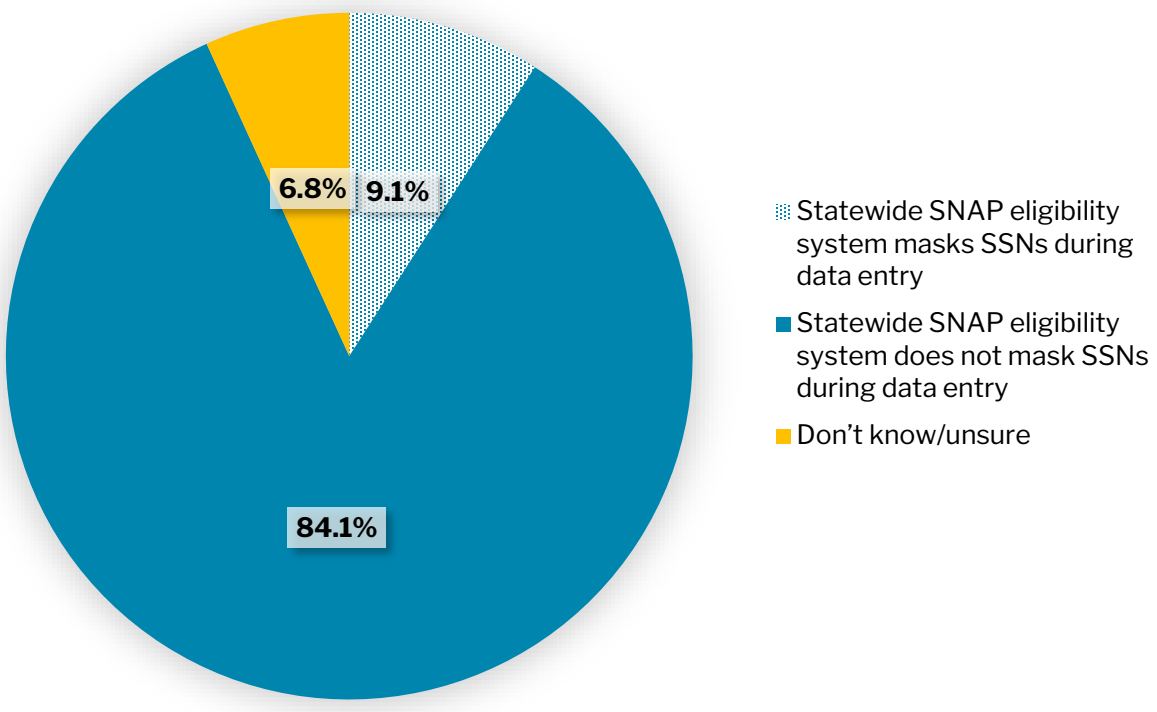
Safeguarding Practices Used During Program Operations

This section highlights the SA's security practices used during program operation, including the various processes and procedures associated with administering SNAP, such as masking, or timeout features used when collecting data from program participants; use of secure data systems when processing PII data to administer program benefits; and matching PII to other data sources to enhance program integrity or verify eligibility.

Masking Procedures Used by SAs during Data Entry

Exhibit 3-11 provides a summary of masking procedures used by SAs to safeguard SNAP PII during data entry. NIST defines masking as "the process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym," As shown, 84.1 percent of SAs (n=37 SAs) reported that they do not mask Social Security numbers during data entry. Only 9.1 percent of SAs (n= 4 SAs) reported that they have a statewide SNAP eligibility system that masks Social Security numbers. Three SAs were unsure whether they mask Social Security numbers during data entry.

Exhibit 3-11 | Masking Social Security Numbers During Data Entry

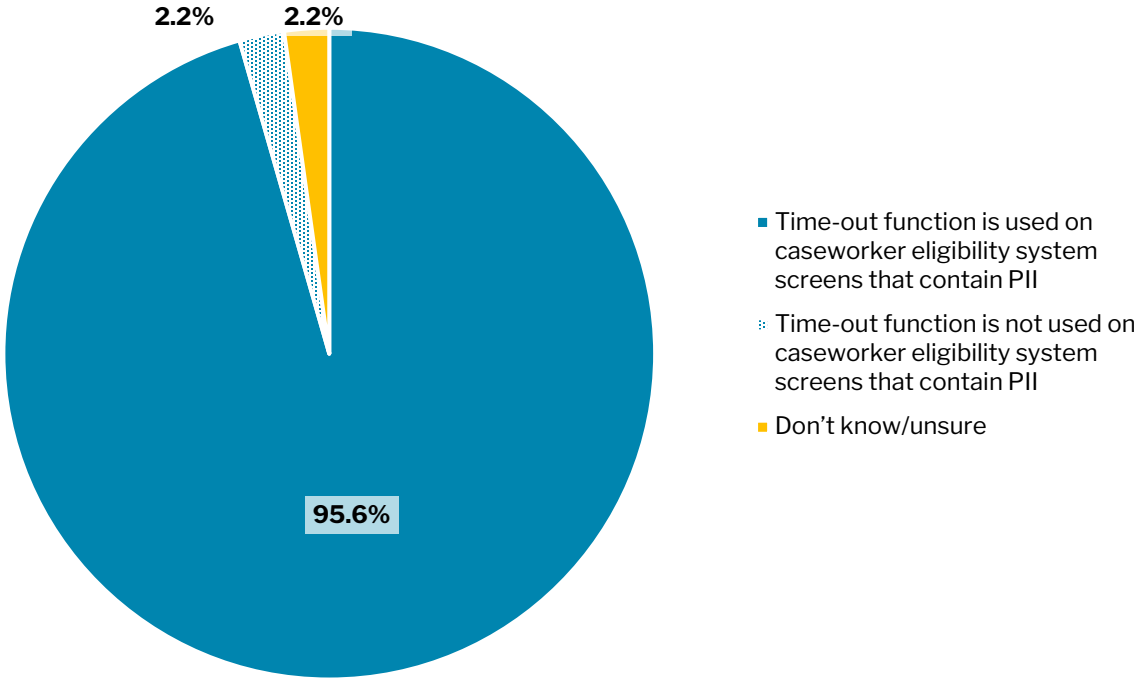


Notes: Findings about masking social security numbers during data entry are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 5.4.

Timeout Functions Used on Application Screens Containing PII

Nearly all SAs (95.6 percent) reported that they use timeout functions (Exhibit 3-12). Thirty-six SAs reported that there is a time limit for their timeout functions. Only 1 SA indicated that it does not use a timeout function. The distribution of the reported time limits varied with the minimum time limit of 3 minutes and maximum time of 120 minutes, with the average and median time limits for timeout being 19.5 minutes and 15 minutes respectively.

Exhibit 3-12 | Timeout Function Used on Application Screens that Contain PII



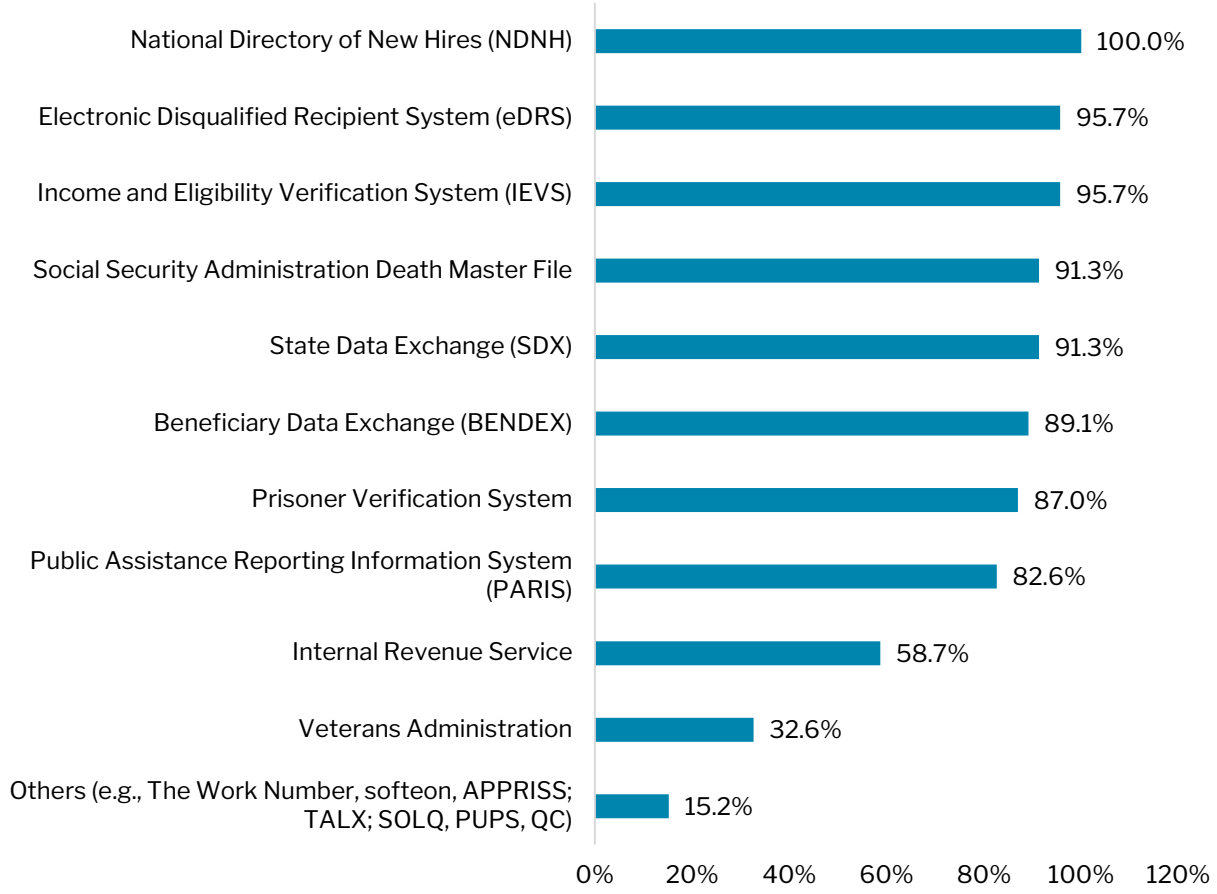
Notes: Findings about whether the timeout function is used on application screens that contain PII are based on the responses from 45 SAs; total sample size = 47. 43 SAs indicated that they use timeout functions, and 36 of them reported time limits of their timeout functions. The distribution of the 36 reported time limits is displayed with a boxplot on the right.
Source: SNAP PII State Agency Survey, questions 5.11 and 5.12.

SA's Procedure for Safeguarding PII during Data Matching

SAs use both national and state data sources to match SNAP applicant and recipient data (Exhibits 3-13 and 3-14). For the national data sources, all the SAs (n= 46 SAs) reported that they use the National Directory of New Hires for data matching. Other common national data sources are the Electronic Disqualified Recipient System (95.7 percent), and Income and Eligibility Verification System (95.7 percent). SAs also have access to state data sources to match SNAP PII applicant and recipient data. Nearly all the SAs (97.8 percent) reported that they use state workforce data for data matching. Other state data sources used frequently by SAs include the state Child Support Payment System (n=89.1 SAs), State New Hire Directory (n= 78.3 SAs) and State Death Records (n= 67.4 SAs).

Exhibit 3-15 provides a summary of the types of recipient/applicant data commonly used to perform data matching. Nearly all SAs (n=40 SAs; 88.9 percent) reported using Social Security numbers to perform data matching. Approximately 87 percent of SAs (n= 39 SAs) indicated using names for data matching. The use of case numbers and unique identifiers (n= 15 SAs) such as PID numbers and SNAP client ID are among the least-reported variables for data matching.

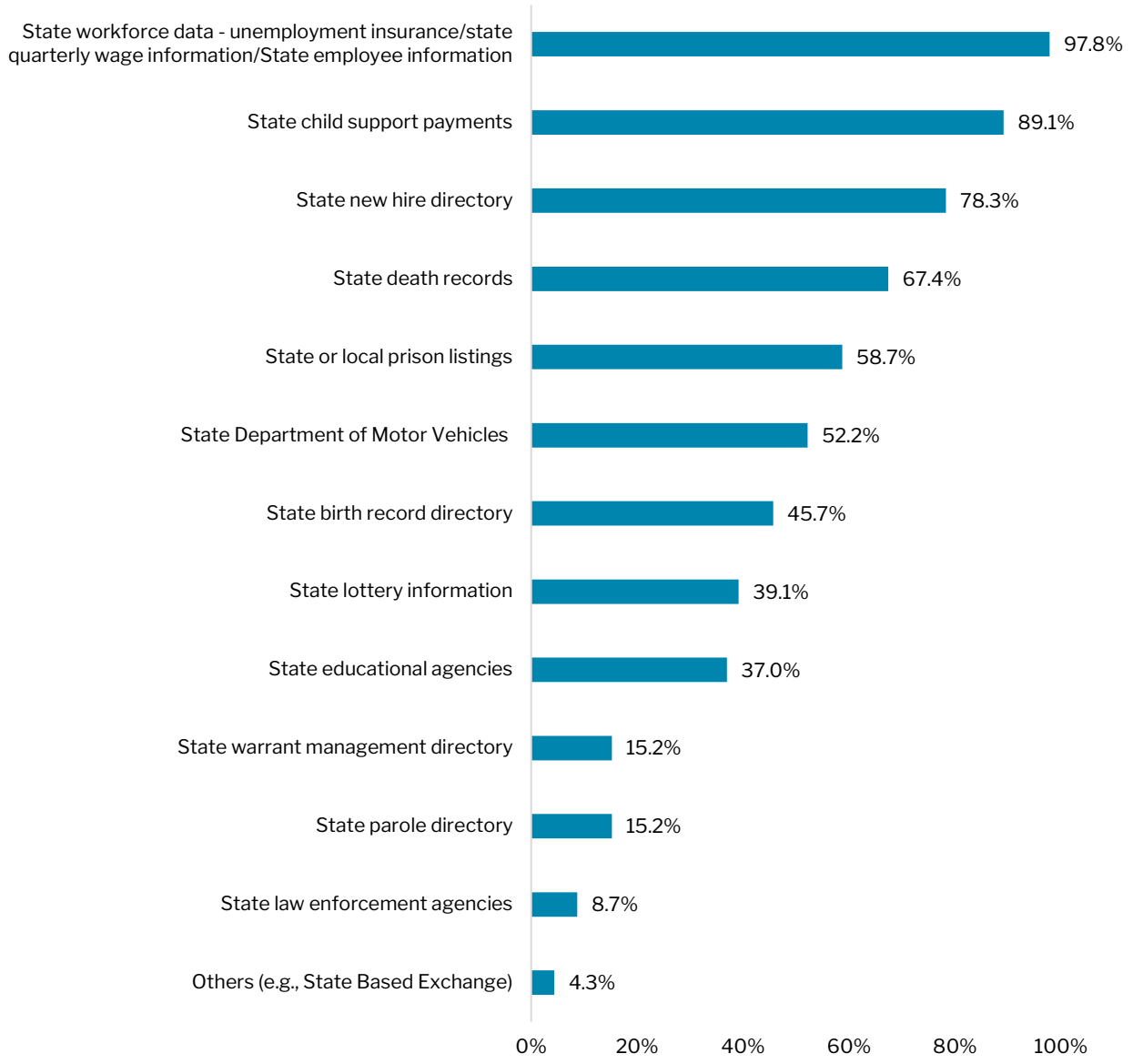
Exhibit 3-13 | National Data Sources that SAs Match SNAP Applicant and Recipient Data



Notes: Findings about data sources that SAs match SNAP applicant and recipient data are based on the self-reported responses from 46 SAs; total sample size = 47. Additional data sources were specified in an open-text response; one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.

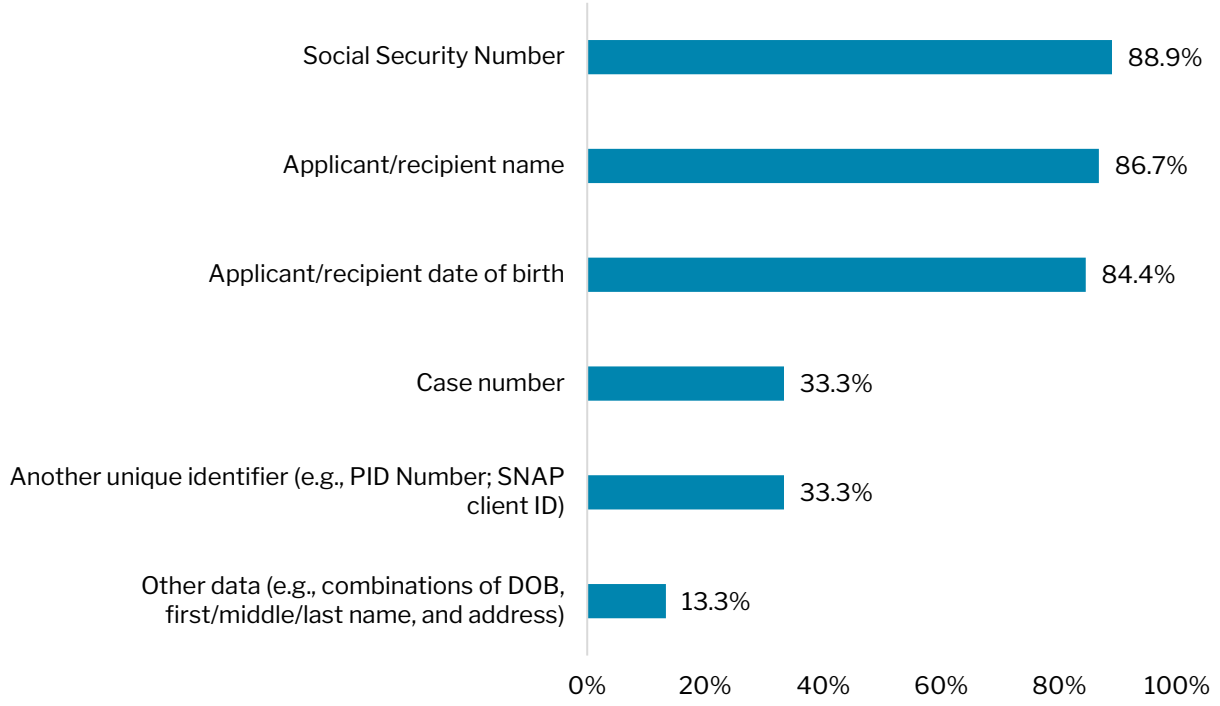
Percentages <100% reported for mandatory verification were found to be reporting errors from some respondents, and do not reflect noncompliance.

Exhibit 3-14 | State Data Sources that SAs Match SNAP Applicant and Recipient Data



Notes: Findings about data sources that SAs match SNAP applicant and recipient data are based on the responses from 46 SAs; total sample size = 47. Additional data sources were specified in an open-text response; one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.

Exhibit 3-15 | Types of Data Commonly Used to Perform Data Match

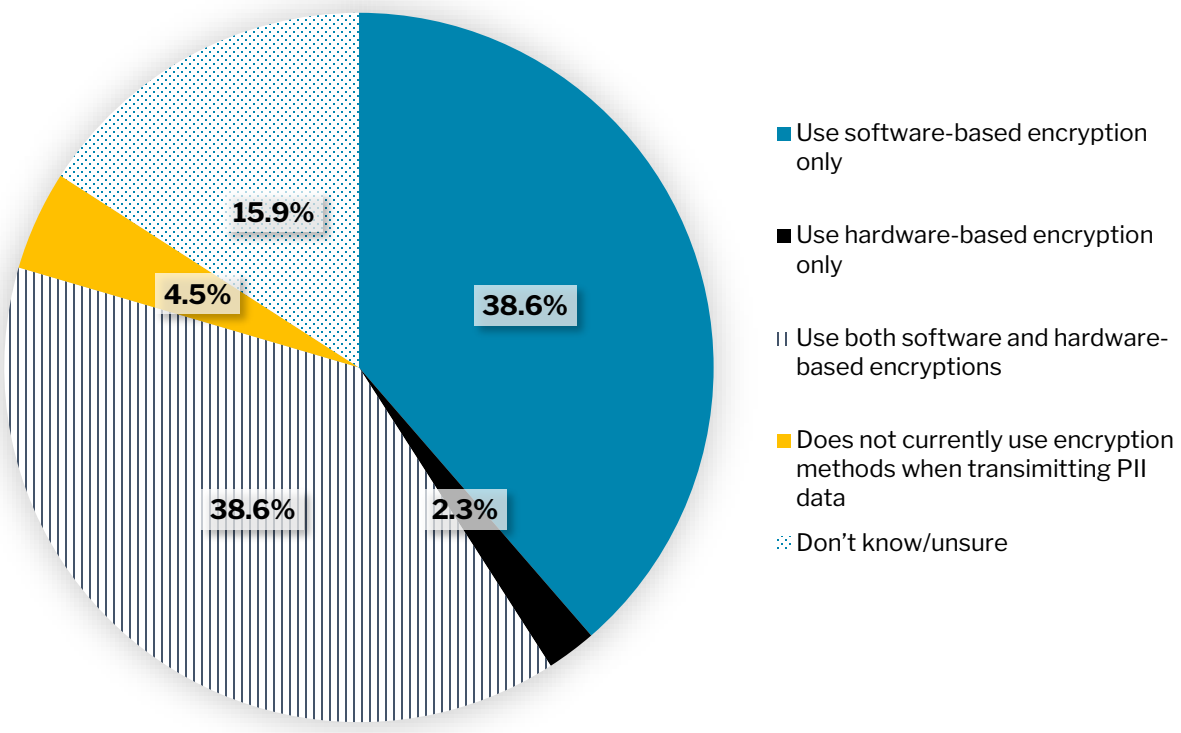


Notes: Findings about types of data commonly used to perform data matching are based on the responses from 45 SAs; total sample size = 47. Additional types of data were specified in an open-text response; one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 1.9.

SA's Procedure for Sharing and Transferring PII

The encryption methods employed by SAs to transmit PII data varied across the 44 SAs that responded to the question (Exhibit 3-16). Almost 39 percent of SAs (n=17 SAs) indicated that they use only software-based encryption to transmit PII data. The same number of SAs (n=17 SAs) indicated that they use both software- and hardware-based encryption to transmit PII data. Software-based encryption uses a software tool to encrypt data without requiring any additional hardware. Examples include BitLocker and AxCrypt. Whereas hardware-based encryption uses a device's on-board security to perform encryption and decryption. Examples include encrypted USB, external hard drives, and self-encrypting solid-state drives. Only 1 SA reported it uses hardware-based encryption. Finally, 15.9 percent of SAs (n=7 SAs) do not use any encryption method to transmit data.

Exhibit 3-16 | Encryption Methods Used for Sharing and Transferring PII Data

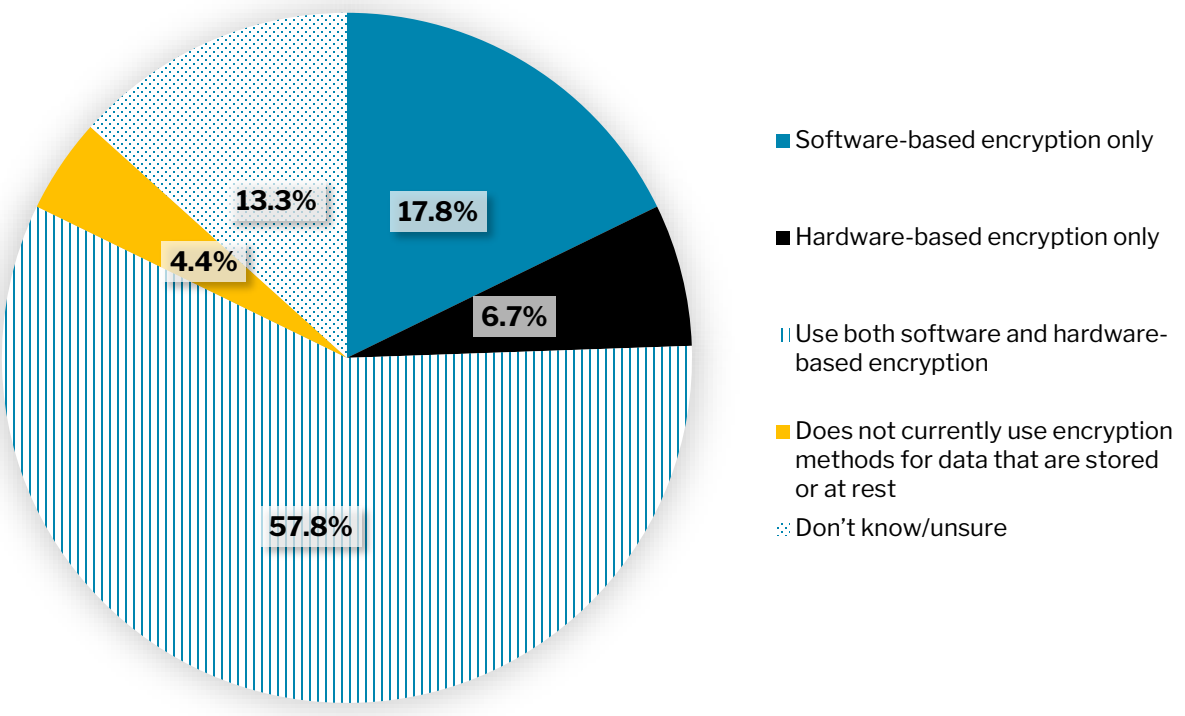


Notes: Findings about encryption methods used for transmitting PII data are based on responses from 44 SAs; findings about encryption methods used for storing PII data are based on responses from 45 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 6.2 and 7.4.

SA's Procedure for Maintaining and Storing PII

In addition to the procedures for sharing and transferring PII, SAs reported the procedures they have employed to maintain and store PII data. As shown in Exhibit 3-17, 17.8 percent of SAs (n=8 SAs) indicated that they use only software-based encryption while 6.7 percent of SAs (n=3 SAs) indicated that they use only hardware-based encryption to store PII data. Approximately 58 percent of SAs (n=26 SAs) reported that they use both software- and hardware-based encryption. Only 4.4 percent of SAs (n=2 SAs) reported that they do not currently use any encryption method to store PII data. These findings are based on responses from 45 SAs.

Exhibit 3-17 | Encryption Methods Used for Maintaining and Storing PII Data



Notes: Findings about encryption methods used for transmitting PII data are based on responses from 44 SAs; findings about encryption methods used for storing PII data are based on responses from 45 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 6.2 and 7.4.

Industry experts identified barriers to compliance with data security policies, including the age of data systems used; limited resources for IT system security; focus on other high-priority work; lack of alignment with other SAs; and specific features of the systems that involve PII. First, experts identified potential barriers to compliance based on the age of the data system being used. With technological advancements, data encryption and security need to be advanced to secure data, meaning that older data systems (if not well maintained and updated) may be vulnerable to security threats as potential intruders become more advanced in their methods. Most states recently upgraded their data systems when the Affordable Care Act provided funding to upgrade their Medicaid data systems, which often shared data with SNAP. According to one expert, some states are still using old "legacy" systems that may contain inherent security vulnerabilities that grow worse over time, especially if the technology is not updated.

Experts noted the importance of continuously providing resources to IT system security. As new methods to attack data systems continue to evolve, methods to increase security to prevent attacks also must be adapted. Developing methods to prevent these attacks requires resources such as continuous training and system upgrades. Additionally, experts

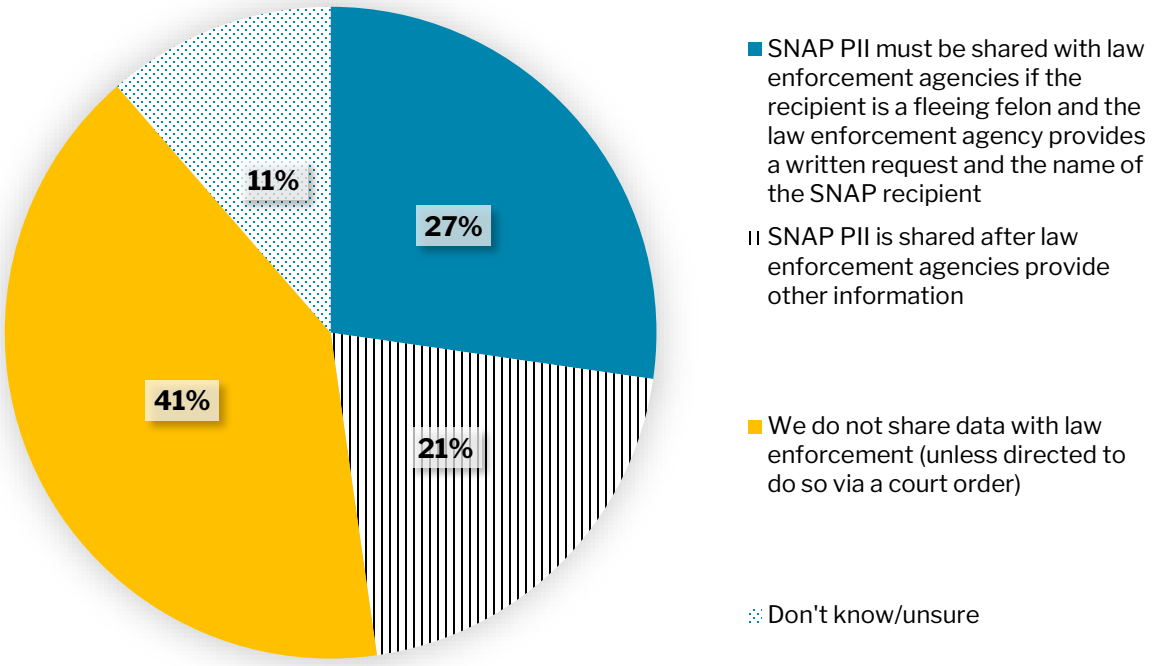
describe that when there is a lack of infrastructure and available resources supporting data security, other, more critical work—such as primarily administering SNAP services/benefits—is prioritized. This is a more common issue when there is an emergency, such as during the pandemic. The experts believed that if SAs had infrastructure supporting data security in place, data security would not have been affected from the urgency to provide services during that time.

Experts identified a lack of alignment with other state social service agencies (such as Medicaid) as a barrier to compliance, noting that because SAs share data, an agency with an older system would have less privacy safeguards and less advanced encryption. The respondent explained that if there was a data breach, the potential intruder could use the weak system to infiltrate the other, more advanced systems it is sharing data with. Another respondent noted that the system features could contain PII and described the dangers of data sharing or combining datasets, saying, "We want to share the data, but as we keep sharing and putting datasets together, we increase our risk of being exposed."

SA's Procedure for Responding to Law Enforcement Requests for PII

Exhibit 3-18 provides findings on the procedures employed by SAs to respond to law enforcement requests for PII. Almost 41 percent of SAs (n= 18 SAs) indicated that they do not share PII data with law enforcement. Almost one-fifth of SAs (n= 9 SAs) reported requesting additional information before sharing PII data with law enforcement agencies, and 27.3 percent of SAs (n= 12 SAs) indicated that they only share the PII of a SNAP recipient who is a fleeing felon. In a situation like this, SAs request the law enforcement agency to provide a written request and the name of the SNAP recipient.

Exhibit 3-18 | SA's Procedure to Responding to Law Enforcement Requests for PII



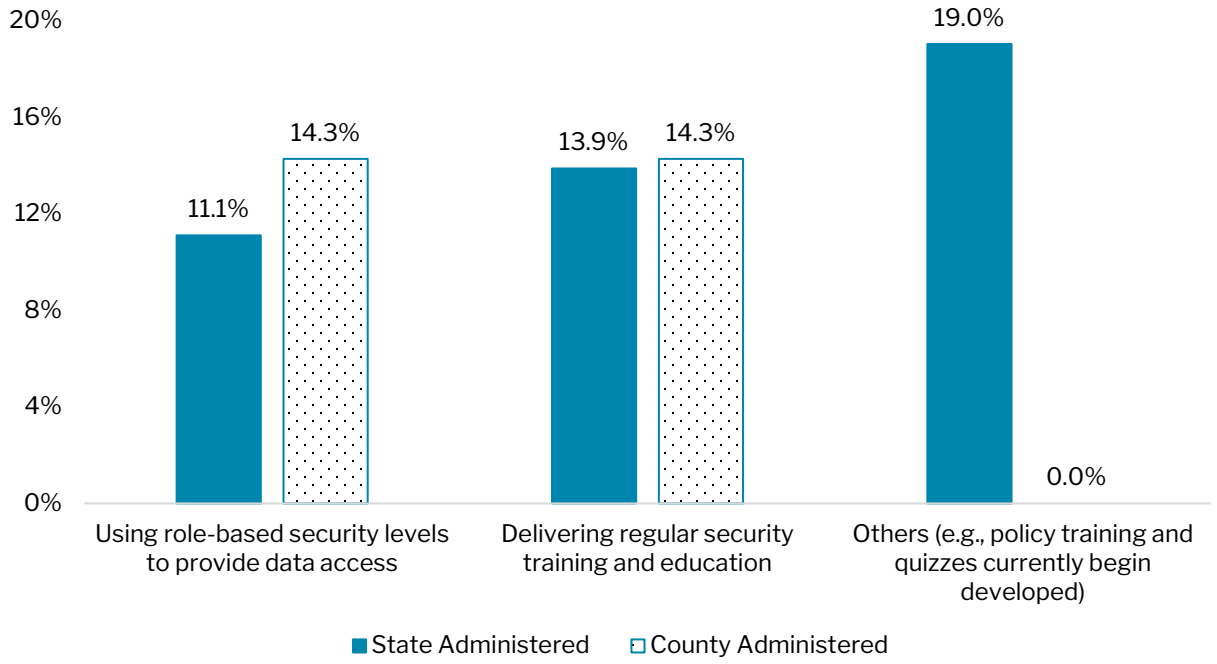
Notes: Findings about SA's procedure to respond to law enforcement requests for PII are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 7.5.

SAs Likelihood to Upgrade Their Safeguarding Practices

In this section, we present the results of the likelihood of SAs to undertake efforts to upgrade their formal safeguarding policies and procedures within the next 2 years, if not already in place. We present these findings by the type of administration (state-administered SAs vs. county-administered SAs), and across the three domains of *personnel policies and procedures*, *security policies,* and *program operations*.

For personnel policies and procedures, almost 14 percent of county-administered SAs would upgrade practices related to role-based security levels to provide data access, compared to 11 percent of state-administered SAs (see Exhibit 3-19). State and county-administered SAs provide equal emphasis on upgrades to regular security training to personnel.

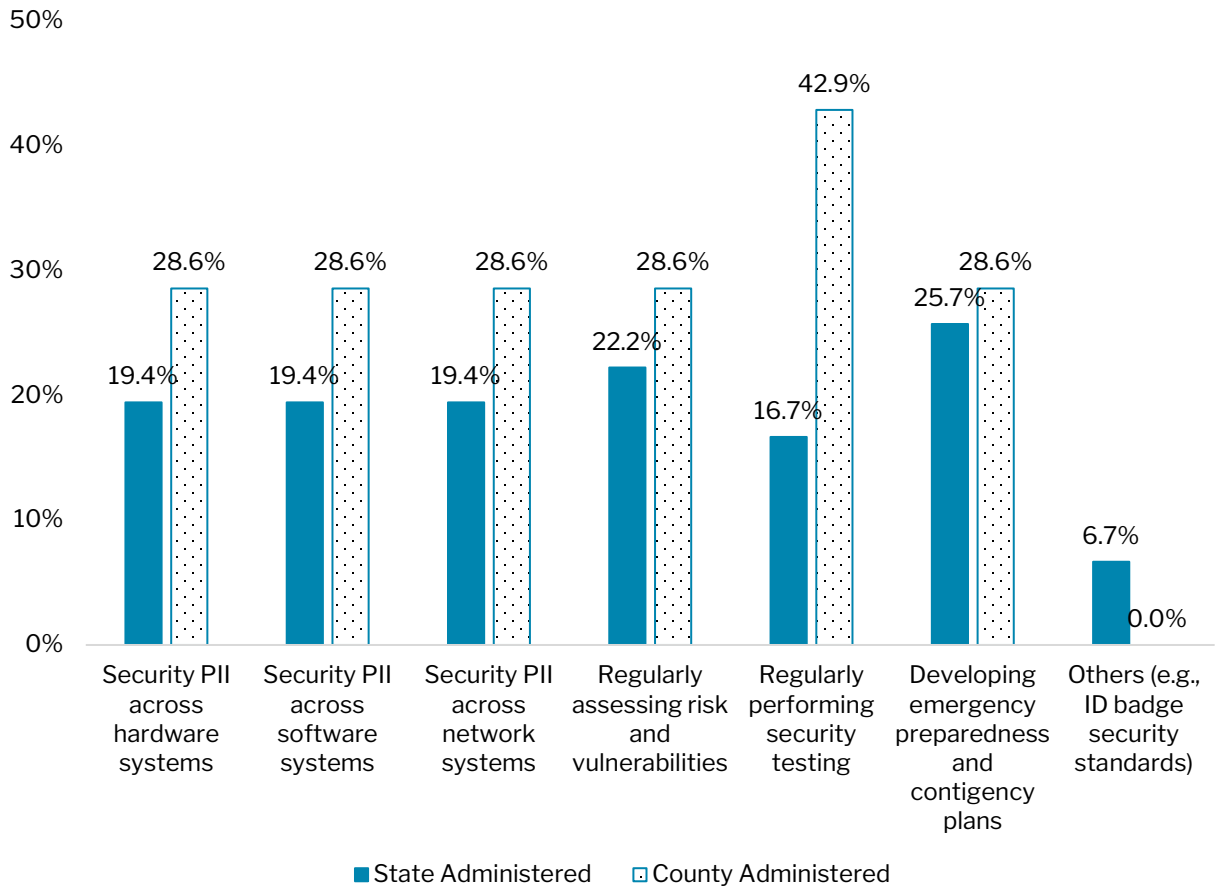
Exhibit 3-19 | SAs Likelihood to Upgrade Their Safeguarding Practices, by Type of Administration: Personnel Policies and Procedures



Notes: Number of responses for each safeguarding practice varies, it is reported in Table 14a; total sample size = 47. Additional practices were specified in an open-text response; one or two open-text responses were listed in the bracket.
Source: SNAP PII State Agency Survey, question 2.5.

For the Security policies, larger variations in upgrades to safeguarding practices is witnessed in the security policies and procedures domain. Almost 43 percent of the county-administered SAs prefer upgrades to security testing compared to 17 percent of the state-administered SAs (Exhibit 3-20). This difference is also visible across multiple practice areas, like security PII across hardware, software, and network systems (28.6 percent county-administered SAs vs 19.4 percent of state-administered SAs).

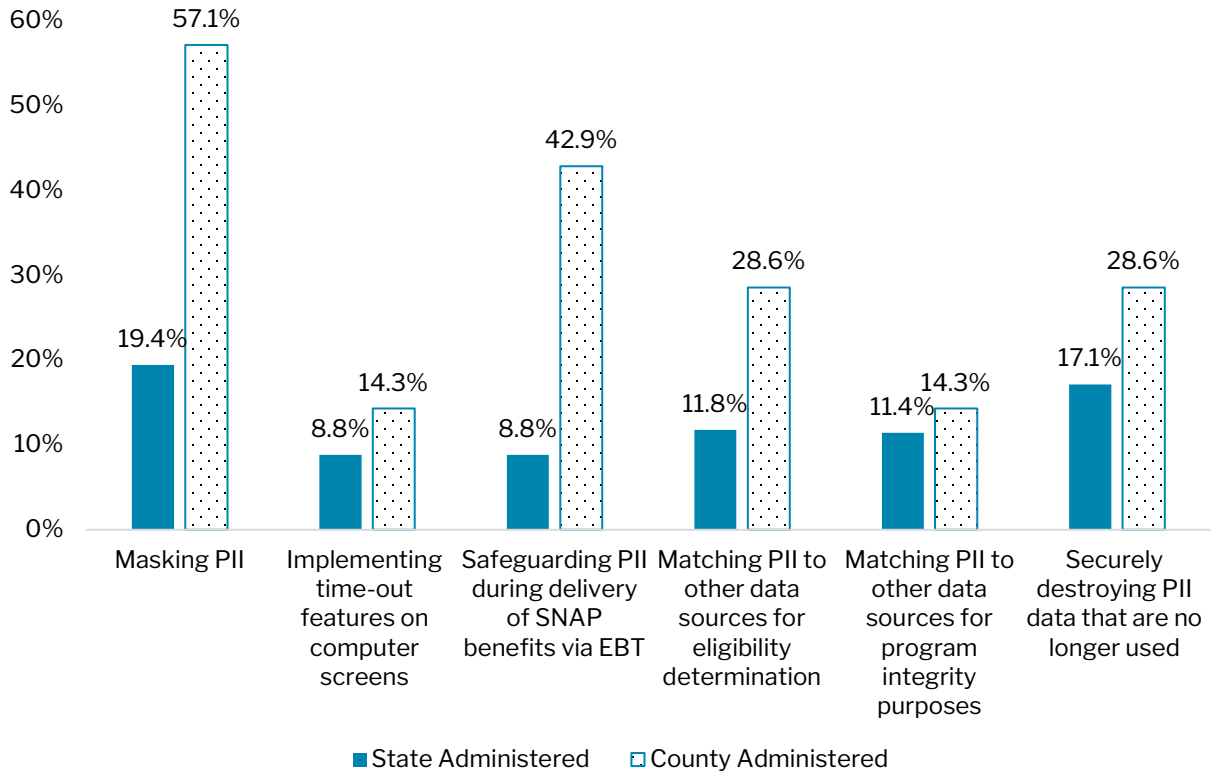
Exhibit 3-20 | SAs Likelihood to Upgrade Their Safeguarding Practices, by Type of Administration: Security Policies and Procedures



Notes: Number of responses for each safeguarding practice varies, it is reported in Table 14a; total sample size = 47. Additional practices were specified in an open-text response, one or two open-text responses were listed in the bracket.
Source: SNAP PII State Agency Survey, question 2.5.

The largest difference in upgrades to the practices followed by state- and county-administered SAs is visible in the program operations domain, where almost 57 percent of county-administered SAs are likely to upgrade practices related to masking PII versus 19 percent of state-administered SAs (see Exhibit 3-21). In addition, county-administered SAs reported higher upgrade needs in the areas of safeguarding PII during delivery of SNAP benefits (about 43 percent vs. almost 9 percent for state-administered SAs) and matching PII to other data sources for eligibility determination (about 29 percent vs. almost 12 percent for state-administered SAs).

Exhibit 3-21 | SAs Likelihood to Upgrade Their Safeguarding Practices, by Type of Administration: Program Operations



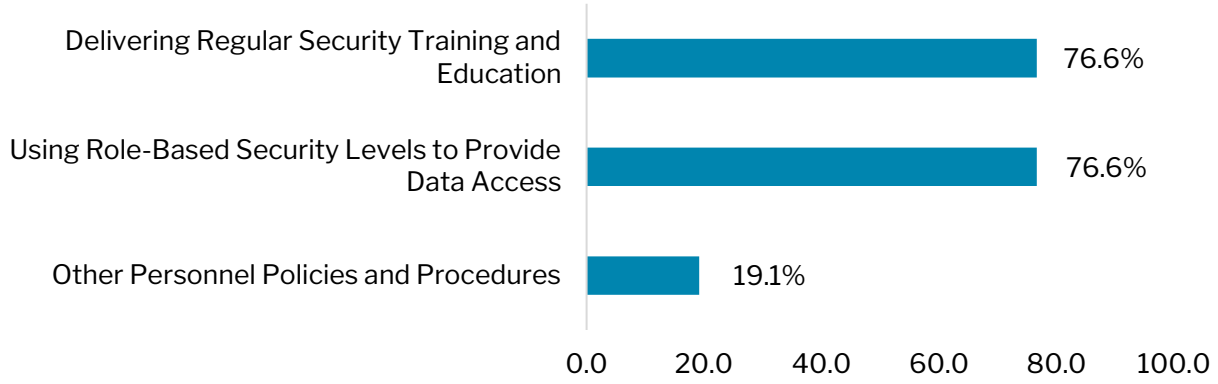
Notes: Number of responses for each safeguarding practice varies, it is reported in Table 14a; total sample size = 47. Additional practices were specified in an open-text response; one or two open-text responses were listed in the bracket.
Source: SNAP PII State Agency Survey, question 2.5.

Safeguarding Practices That are Most Often Practiced Within State Agencies

Safeguarding practices fall into one of the following three domains: (1) personnel policies and procedures: (2) security policies and procedures: and (3) security practices used in program operations. For personnel policies and procedures, nearly 77 percent of SAs (n=36 SAs) reported that they use role-based security levels to provide data access and deliver regular security training (Exhibit 3-22). SAs further indicated the common security policies and procedures they have employed to develop a robust security plan to safeguard SNAP PII. As depicted in Exhibit 3-23, 68.1 percent of SAs (n=32 SAs) reported that they secure PII across hardware systems. The same number of SAs (n=32 SAs) reported that they secure PII across software and network systems. Another 66 percent of SAs (n=31 SAs) indicated that they regularly assess risk and vulnerabilities, while 61.7 percent of SAs (n=29 SAs) regularly perform security testing. For security practices used in program operations, 72

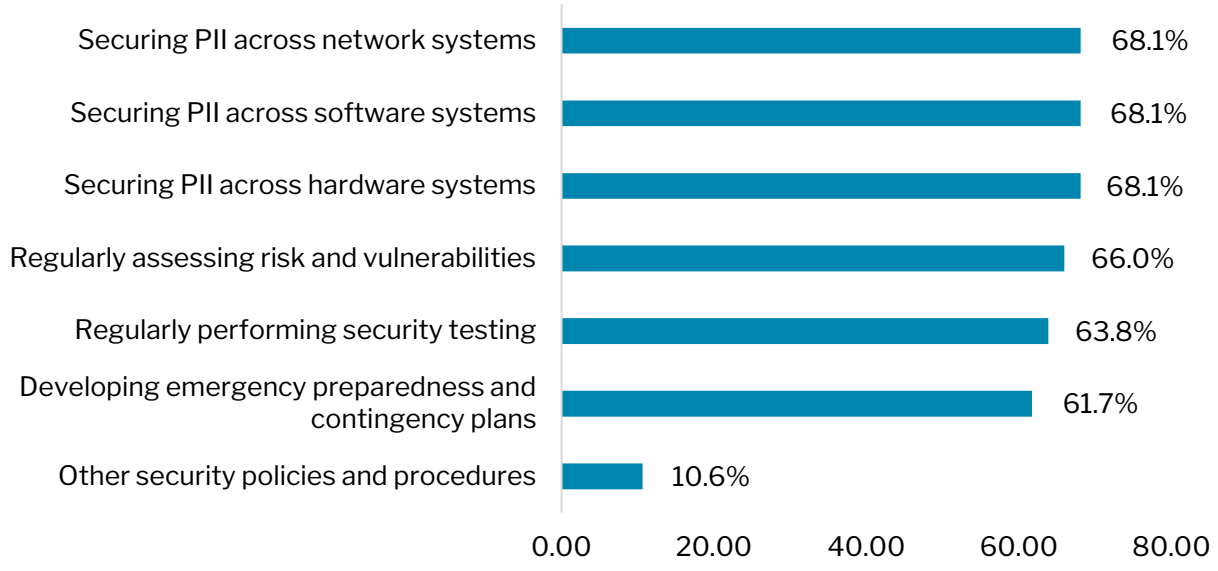
percent of SAs (n=34 SAs) indicated that they implement time-out features on computer screens to safeguard SNAP PII (Exhibit 3-24). Two other practices: safeguarding PII during delivery of SNAP benefits via EBT and matching PII to other data sources for program integrity purposes are also commonly employed by SAs, 68 percent of SAs (n=32 SAs) implementing both practices.

Exhibit 3-22 | Safeguarding Practices Followed by SAs: Personnel Policies and Procedures



Notes: Findings about safeguarding practices followed by SAs in the Personnel Policies and Procedures domain are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.5.

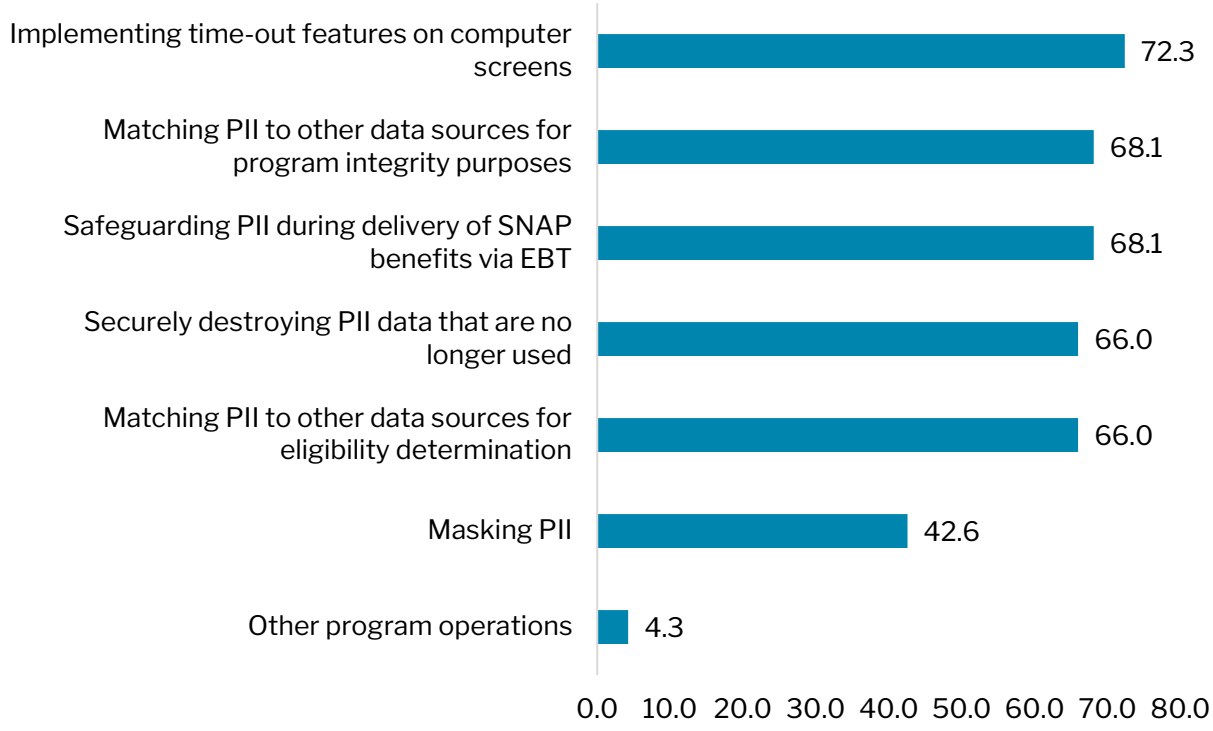
Exhibit 3-23 | Safeguarding Practices Followed by SAs: Security Policies and Procedures



Notes: Findings about How agencies structured its approach for using systems security professionals are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text

response, one or two open-text responses were listed in the bracket. Two respondents selected the "Others" option, they provided the following other approaches: We leverage Accenture system security professionals; Our agency utilizes a combination of system security professionals located within our agency and systems security professionals located within another state agency.
Source: SNAP PII State Agency Survey, question 2.5.

Exhibit 3-24 | Safeguarding Practices Followed by SAs: Program Operations

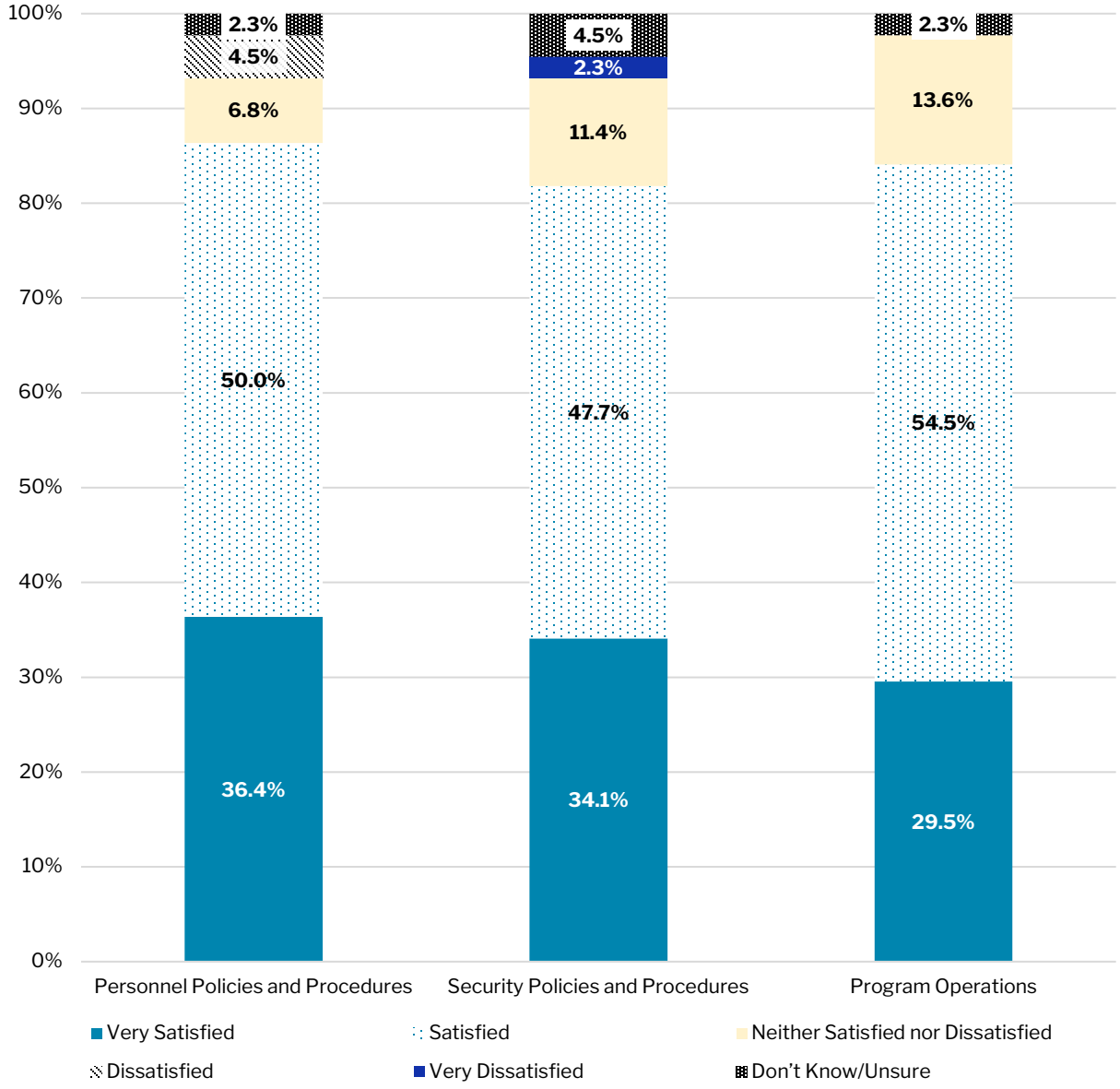


Notes: Findings about safeguarding practices in the Program Operations domain are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.5.

Areas in Which State Agencies have the Most Difficulty Implementing Safeguards

Generally, SAs reported a high level of satisfaction with the safeguards they have employed for the three domains. Overall, 86.4 percent of SAs (n= 40 SAs) indicated that they are very satisfied/satisfied with the personnel policies and procedures they have employed to safeguard SNAP PII. The descriptive results in Exhibit 3-25 indicate that nearly 82 percent of SAs (n= 38 SAs) and 84 percent of SAs (n= 39 SAs) are satisfied/very satisfied with the security policies and procedures and program operations in place to safeguard SNAP PII, respectively.

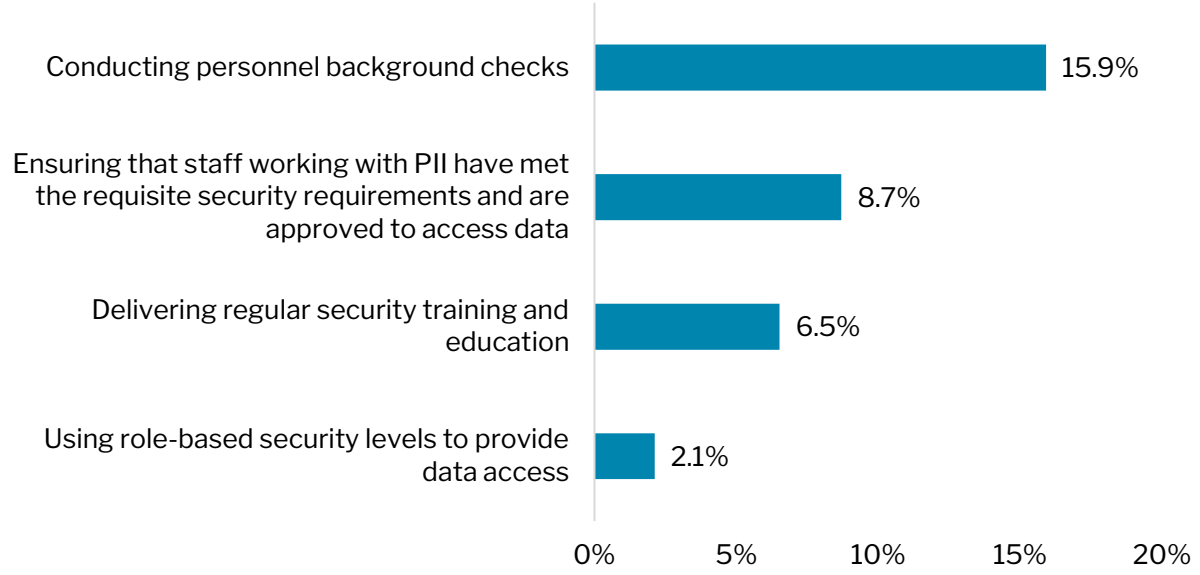
Exhibit 3-25 | SA's Rating of Safeguarding Practices



Notes: Findings about SA's rating of safeguarding practices are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 8.1.

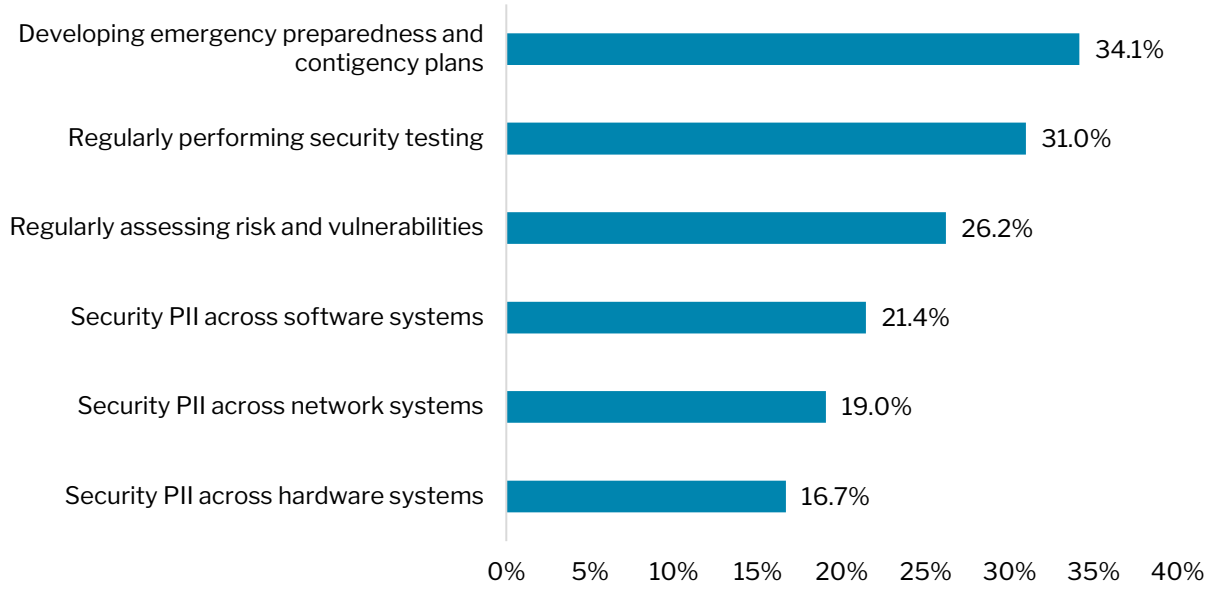
Exhibit 3-26 provides the descriptive results of SAs' self-assessment of the safeguarding practices they need to improve. On personnel policies and procedures, 15.9 percent of SAs (n= 7 SAs) reported that they need to improve how they conduct personnel background checks. Another 8.7 percent of SAs (n= 4 SAs) reported that they need to improve security protocols to ensure staff working with PII meet requisite security requirements.

Exhibit 3-26 | Personnel Policies and Procedures Most in Need of Improvement



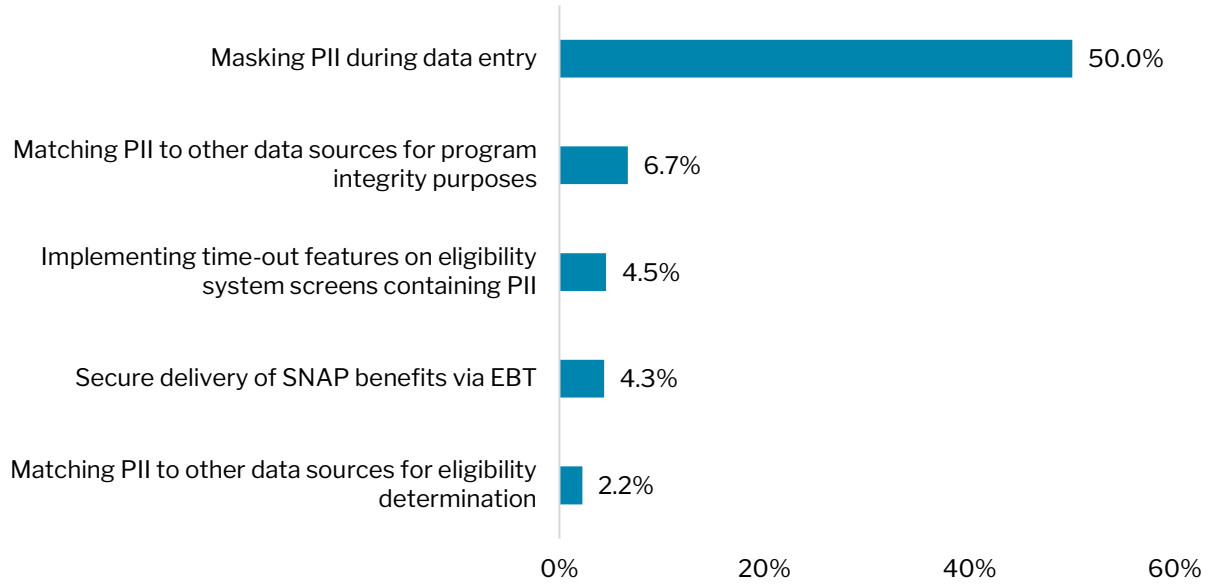
Notes: Findings about Personnel Policies and Procedures in need of improvement are based on the responses from 44 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 3.9, 4.8, 5.19.

Exhibit 3-27 | Security Policies and Procedures Most in Need of Improvement



Notes: Number of responses for each security plan varies, it is reported in Appendix C, Table 16a; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 3.9, 4.8, 5.19.

Exhibit 3-28 | Program Operations Most in Need of Improvement



Notes: Number of responses for each security plan varies, it is reported in Table 16a; total sample size = 47.
Source: SNAP PII State Agency Survey, questions 3.9, 4.8, 5.19.

Challenges Faced by State Agencies While Implementing Safeguard Policies to Protect PII

The interviews with exemplary SAs provided nuanced understanding of the challenges faced while implementing policies to protect PII. We present some of the key identified challenges below.

Inadequate budget. Staff from several SAs suggested as not-for-profit enterprises, agencies always lack funds. Staff from one SA explained that it is difficult to get more money because of the legislative process involved. However, it is becoming easier for agencies to be more proactive than reactive to protect systems. Apart from receiving funding from states, agencies have been able to build on necessary technical skills to improve the system and have system scans that run to check laptops, servers, and even disaster recovery sites.

Lack of available cybersecurity talent. An SA staff noted that acquiring quality security staff for the organization and SA vendors is challenging. Another staff added the talent pool in the public sector doesn't match to that of the private sector, albeit they acknowledged being audited by a bigger organization is helpful. For instance, staff noted that the state's Office of Homeland Security (OHS) provides additional security tools and requirements necessary to accomplish the goals set in the statewide information security manual. Additionally, the staff noted that the tools provided by the state's OHS such as "Crowdstrike" for end point detection and response and "InsightVM" for vulnerability testing have increased the agencies' capability to resolve issues.

Relatedly, SAs noted the pace at which newer technologies are introduced and quickly outdated, making hiring well-trained individuals difficult. There is therefore lack of interest in such courses

among graduates due to limited growth opportunities. Some agencies chose a basic system set up and try to minimize exposure by allowing access to only necessary individuals. However, SAs that have experienced a data breach have developed a strong cybersecurity team with the required support to protect themselves against future risks.

Processes and procedures used by county IT offices. The integration of security professionals between the project and state partners has been critical for SAs to stay updated on security changes. For example, heavy collaboration and communication between users of the security system, the county professionals who manage and maintain the eligibility system and the state partners has enabled SAs to stay current on security changes, broadcasts, etc. However, too many partners involved in the process could increase vulnerabilities and can also make it difficult to ensure security parameters are followed. It also proves to be expensive for the county's extranet partners since they provide necessary equipment. The only risk is the potential challenges to management by the county partners.

SAs noted counties can find their own funding and are more likely to make updates to the data system as necessary. The state partners are now trying to increase their investment in a better data system to bring everyone on one single system.

"*[the security plan] is such a large document. You'll look at all the NIST controls. I think after you have all you information, that document is about 800 pages. So, to go through all that again is a monumental effort and that's actually what we have to do right now as part of our space's compliance; is relooking at that and what's changed. So, I think trying to find an automated way is the best way you could really overcome that*."

Updating and complying with security plan. Subject matter experts in the earlier phases of the study suggested that SAs may find it challenging to keep their security plans up to date. We asked SAs to describe the extent to which they struggled with updating, understanding, and/or complying with its security plan, and how they have overcome the challenges. SAs noted the primary challenge they face is to coordinate between the agency and the outsourcing entities. Outsourcing entities do not prioritize detailed documentation and the need to ensure the review of controls. SAs further noted there is limited support from the outsourcing entities, making it necessary for agencies to enforce/encourage compliance with the policies and controls established in their security plan. One SA staff also noted they utilize regular review models to ensure that the security requirements are addressed and updated as necessary. Another SA added that their primary plan is to conduct disaster recovery tests on the mainframe.

Updating security plans has been a challenge for some SAs because of limited resources. One staff mentioned, "*it is a complex process to update their internal security plans and there aren't enough resources to get it done*." But they mentioned ways to overcome these challenges. Staff from one SA suggested explaining the importance and need for updates to the frontline workers. They mentioned that they have been successful in updating the security system because all staff involved in the process understood the need for it.

4. BEST PRACTICES FOR SAFEGUARDING PII

The study team employed interview questions to ascertain industry best practices for safeguarding PII that SAs should consider implementing during distinct phases of the data lifecycle, such as information collection, information processing, information transmission and dissemination, information storage, and information destruction. In addition, the study team asked experts to share their views on PII safeguarding best practices to ensure that staff working with PII have met the security requirements to access data at approved security levels and have received regular security training and education. Industry experts identified general best practices for safeguarding PII that are common to the different areas of the data lifecycle, some of which include:

1. Minimizing the use, collection, and retention of PII and restricting it to what is necessary to fulfill their business goals.
2. Regular training and educating of users that have access to PII about the risks associated with PII and how to protect it.
3. Restricting user access to relevant information as defined by their business purpose.
4. Developing incident response plans that include elements such as determining when and how individuals are notified and how a breach is reported, in addition to some remedial services.

According to experts, these are preliminary considerations for SAs to effectively protect PII. Below, the study team provides a description of these safeguarding methods under each stage in the data lifecycle.

Personnel Security

Use the principle of "least privilege," which limits users' access rights to only what are strictly required to do their job. The experts overwhelmingly indicated this is the most valuable security concept. Experts said this ensures that only approved users have access to the minimum amount of PII needed to perform their duties. In line with this, one expert noted the importance of audits or testing controls that ensure SAs are continuously assessing users who need access to various levels of information, and that they are closing out access to individuals when they no longer use the information.

Vet individuals before hiring, based on their access to varying levels of sensitive information. Even before initial access to information is provided to users, experts identified the need to appropriately vet candidates before they hired by SAs. Industry experts explained SAs can assign a risk level to all positions and establish screening criteria for individuals filling those positions. In line with NIST SP 800-53 (McCallister et al., 2010), experts stated the screening methods should reflect laws, policies and directives that are applicable to specific positions based on their risk levels. For example, one expert noted SAs could require that individuals with access to a system that stores, processes, or transmits

PII information must go through more rigorous background checks, such as criminal history, credit checks or other elements, including foreign threats. Those requiring only physical access to a facility may not need such in-depth security checks.

Update personnel security controls when staff transfer from one position to another within the same agency. Experts described that it is important to ensure staff no longer have access to sensitive information once they leave their previous position. If this is not tracked appropriately, staff can end up accumulating access to different systems in state datasets as they go from one role to another in an organization. Thus, SAs should periodically review staff access levels and remove access if it is no longer necessary for their work duties.

Establish a set of safeguarding rules for terminated personnel. These rules can include disabling system access within a reasonable period, terminating or revoking authenticators and credentials, and retrieving all security-related organizational property. To enhance security, some experts recommended the need for SAs to define actions like returning old and issuing new keys, identification cards and building passes; closing system accounts and opening new ones; and changing system access privileges, etc., for specific types of transfers. SAs should also maintain access agreements with personnel to ensure that any individual granted access to PII has valid authorization and satisfies all associated security requirements.

Information Collection

Limit PII data collection to the minimum necessary to provide the service or establish eligibility for SNAP. By limiting PII data collection to the least amount necessary to conduct its mission, the agency may limit potential negative consequences in the event of a data breach involving PII (McCallister et al., 2010). To effectively implement the "minimum necessary" principle, SAs should first consider the total amount as well as the types and categories of PII used, collected, and maintained (McCallister et al., 2010).

Provide notification to obtain consent from applicants prior to the collection of their data.[21] The purposes for which personal data are collected about the applicant should be specified in the application, not later than at the time of data collection. This gives applicants the opportunity to understand what is being collected about them. Experts often referred to the widely recognized "Fair Information Practices," also referred to as the "Privacy Principles"[22] in NIST SP 800-53 Rev. 5, on which a lot of federal requirements on privacy control are based.

[21] For online applications, information about consent must be provided at the beginning of the application.
[22] The Fair Information Practices, also known as Privacy Principles, are the framework for most modern privacy laws around the world. Several versions of the Fair Information Practices have been developed through

Provide guidance on where to conduct interviews with applicants when PII will be collected. Make sure that there is privacy when conducting interviews, even if in a SNAP office. One expert also noted applicants should be given the option of where to conduct the interview, especially if it is to be conducted in-person in a SNAP office.

Coordinate guidance from federal agencies on jointly processing applicant information to streamline and ensure a more user-centered experience in accessing public assistance. An expert acknowledged that in the process of applying for SNAP benefits, participants may be applying for other benefits at the same time that may require additional information. As a result, the expert noted some SAs are moving toward a process similar to the "Motor Voter Act,"[23] where applicants must answer additional questions if they want to complete a SNAP application online. By collecting additional information, the expert indicated that these states are multiplying the PII that is getting passed through the SNAP SAs. Accordingly, this may create a more complex and fragmented regulatory environment for SAs to navigate, and may even lead to adverse outcomes, such as more difficulty in accessing programs by applicants or potential privacy breaches.

Information Processing

Ensure users only have access to the information and the records they need to perform the function. For example, one expert described that if users are searching for an applicant or looking up an applicant's information, the system should only display the specific pieces of information that they need to know. Specifically, any systems that pull up information or allow for searching must have audit logs to ensure there is logging of user and administrator activities, and that only minimum amount of PII is presented, specific to the function that SA users are performing.

Develop policies around the removal or purging of PII when no longer required. For example, if benefit administration requires employment verification where SAs collect several documentations from applicants, once that verification is done, is it necessary to retain all of the PII that was collected for that verification process or can that all be purged? To effectively implement a purging standard, experts noted SAs should regularly review their holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting their business purpose and mission.

Protect PII through the life cycle within systems. This includes encryption of PII in transit and at rest, effective access controls around any repository or system that processes PII, and logging and monitoring of activities related to the processing of PII. Experts also

---

government studies, Federal agencies, and international organizations. These different versions share common elements, but the elements are divided and expressed differently. The most commonly used versions are discussed in Appendix D in NIST SP 800-53 Rev. 5 which is available here: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[23] Commonly referred to as the Motor Voter Act, the National Voter Registration Act allows American citizens to register to vote when they are issued a driver's license.

referred to NIST SP 800-122 and 53, which provide a full set of controls related to information processing. Examples of such information processing controls include:

1. Processing information at the lower levels of the computer system—network level, the server level, and the storage area.
2. A strong multifactor authentication for any terminal or system that is able to view PII.
3. Ensuring there is no open storage of any hard copy PII. Any PII contained in hard copy format needs to be secured in a locked cabinet, behind doors, and shredded when no longer needed.

Information Transmission and Dissemination

Use least-privileged encryption, de-identification, and obfuscation actions to protect PII when it is transmitted between end-user computers or between state agencies within a state. The main goal is to keep the utility of a dataset intact as much as possible while reducing the risk of exposure from that dataset. On encryption, an expert explained that the specifics and best ways to implement would vary, but at a higher level, suggesting that SAs should ensure they are encrypting the connection or the session that is involved in that information transmission. More specifically, SAs would need to authenticate or appropriately restrict the end points involved in that transmission, and appropriately secure access to those endpoints so that a party could not impersonate a receiver and inappropriately receive a transmission. Another expert noted encryption could be used cryptographically[24] with "one-way hashes" so that receivers can confirm, from a benefits perspective, they have the needed information about the same individual without the SAs using any clear text or any actual PII in its transmission of information.

Follow the Federal Information Processing Standards Publication 140 (FIPS 140)[25] which establishes secure encryption mechanisms and algorithms to ensure the level of encryption is appropriate to provide protection and is implemented in a way they can rely on to protect their data. FIPS 140 provides good, generalized recommendations because

[24] Cryptography-based security systems are used in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). However, conformance to these standards is not sufficient to secure information. The operator of a cryptographic module is responsible for ensuring that the security provided by a module is sufficient and acceptable to the owner of the information that is being protected and that any residual risk is acknowledged and accepted.

[25] This standard is used in designing and implementing cryptographic modules used by these agencies. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. Specific areas that are covered under these levels are cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operating environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. For details on the security requirements covered in FIPS 140, please see: https://csrc.nist.gov/CSRC/media/Publications/fips/140/3/archive/2009-12-11/documents/fips140-3-draft-2009.pdf

the publication is updated regularly as computing power continues to increase. Another respondent suggested if SAs want to make sure their encryption and cryptography is universally used in a sound and safe manner, it is important for them to regularly use cryptographic modules that are validated to align to that of the FIPS 140-3. The respondent also noted that NIST has transitioned to not just that publication, but also to testing new modules that are developed.

Use de-identification practices such as removing enough PII and obscuring or masking PII in data so that the remaining information may not be used to identify the individual directly. According to the experts, a good practice to de-identify PII is provided in the NIST SP 800-122. McCallister et al. (2010) provides two examples in NIST SP 800-122 of how de-identification could be effectively accomplished:

1. By removing account numbers, names, SSNs, and any other identifiable information from a set of financial records.
2. By removing all identifying PII fields and obscuring applicant/participant ID numbers using pseudo-random data that is associated with a cross-reference table located in a separate system. The only means to reconstruct the original (complete) PII records is through authorized access to the cross-reference table.

Adopt and implement the concept of "differential privacy," whereby SAs would devise means to not increase participants' risk of exposure for including them in a dataset shared with third parties. To implement this concept, SAs "first need to identify how to quantify participants' risk and how to bound the risk level such that for each person in the dataset, that person's risk level doesn't exceed that boundary." A basic way to achieve the goal of differential privacy is to "inject noise"[26] into the data. It is important to note that the Census Bureau has recently adopted differential privacy as its main disclosure-avoidance technique. In line with this approach, the Bureau stated that for the 2020 Census, the total population in each state will be "as enumerated," but that all other levels of geography—including congressional districts down to townships and census blocks—could have some variance from the raw data.[27]

Information Storage

Encrypt PII or any sensitive information at rest or stored within a database. This prevents administrators or individuals with access to the database from the ability to access, view, or copy the PII. One respondent noted that instead of trying to selectively encrypt certain data elements, it would be a good practice for SAs to broadly encrypt data when it is at rest. As mentioned in the information processing section, SAs should ensure IT staff are using sound

[26] Statistically, adding noise to a dataset suggests slight alterations to mask the dataset. The noise hides PII, ensuring that the privacy of personal information is protected, but it's small enough to not materially impact the accuracy of the output of an analysis of the dataset.
[27] For details of how the Census Bureau uses the Differential Privacy concept, please see: https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx

and secure cryptography to perform encryption such that it would not be easily broken. Further, experts noted when information is stored in the cloud, SAs should set up access controls so that only authorized individuals and groups can access it and ensure that it is not directly addressable or accessible over the internet.

Information Destruction

Destroy data, either in hard copy or electronic format, after an established period of time. For data in hard copy format, experts referred to a federal government standard, NIST SP 800-88, Guidelines for Media Sanitization,[28] which provides certain minimum levels of physical destruction that should be adhered to when destroying PII data. For electronic media, experts identified methods to sanitize media that would make data recovery infeasible, even when state-of-the-art laboratory techniques are utilized. The first approach is to overwrite the logical storage location of a file and all user-addressable locations using software or hardware products to overwrite space on the media with non-sensitive data. The second method that could be used is purging (also mentioned in the "information processing" section), which includes overwriting, block erasing and cryptographic erasing using dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands (Kissel et al., 2014). To effectively implement these procedures, there is a need for monitoring and compliance to ensure that records are being destroyed in a timely manner and that SAs are following up for adequate evidence thereof.

In addition to the best practices described above, experts identified a number of broadly applicable legislation, regulations, and policies, as well as international security standards that govern the collection and use of PII data. Of those, NIST guidelines such as SP 800-122, SP 800-53 Rev. 5, and SP 800-88 Rev. 1, had the broadest applicability, with the majority of experts noting that these federally established guidelines apply to the de-identification of PII, PII processing and transparency as well as personnel security, and storage media sanitization. The Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E), and the FIPS 140-3 were the next most commonly identified federal regulations applicable to safeguard PII. The Payment Card Industry Data Security Standard (PCI DSS), the International Standards Organization (ISO) 27001, and Institute of Electrical and Electronics Engineers (IEEE) Standard for Big Data Business Security Risk were each identified as applicable in operations of SNAP.

SAs' Capacity to Implement Identified Best Practices

Through the interviews with exemplary SAs, the study team ascertained the extent SAs have adopted safeguarding practices identified by industry experts and asked SA staff to

[28] For details on media sanitization techniques, minimum sanitization requirements, and guidelines for cryptographic erase device, please see: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

share their views on how these practices have contributed to the security of PII. Staff from all five SAs indicated they use the identified industry best practices in several ways. In **Exhibit 4-1**, we provide examples of how the SAs implement the safeguards.

Exhibit 4-1 | Extent of Usage of Identified Best Practice

Best Practice	Examples of How SAs Approach Practice
Third-party security or vulnerability testing	SA executes periodic vulnerability testing in conjunction with Office of Homeland Security and Preparedness best practices. SA utilizes third-party penetration testing and security control assessments (SOC-2/NIST). In addition to third-party penetration testing, SSA and IRS spend a week with SA to perform their own penetration testing and system liability assessment.
Monitoring email communications among staff	All 5 SAs have an email scanning application that ensures staff are not releasing, outside of their network, any private, personal information. An SA specified they have a traditional firewall; a Mimecast net that flags for Social Security information.
Resting encryption	All SA systems use encryption for sensitive data at rest. The specific implementation varies by technology/platform. One SA noted they have BitLocker where the hard drive is encrypted.
Patch management	For many SAs, patches are applied on a regular basis, in accordance with established policies for patch remediation, aligned with the risk and impact of related security vulnerabilities. Infrastructure is regularly evaluated for new vulnerabilities. Software developed for the system is regularly tested for security flaws and appropriate patches are developed and released based on the impact of those defects.
Multifactor authentication	For many SAs, multifactor authentication is required for all non-public (privileged) access to systems containing sensitive data. All access-controlled sites used by public users allow for multifactor authentication as an opt-in. For one SA, they only use multifactor authentication for parts of their system, such as when users log onto their main system from an unknown device. On devices that do not require multifactor authentication, when users reset their passwords every 60 days, which is a requirement, they are asked to reauthenticate.
NIST cybersecurity framework	All SAs heavily utilize NIST standards and frameworks as a baseline for security policies and system security plans. Examples of such NIST documents are NIST CSF, NIST 800-53, NIST 800-37.

In addition to ascertaining the extent to which SAs use the identified best practices, exemplary SAs identified factors that can be considered necessary “ingredients” for ensuring SAs have the capacity to adapt and implement the best practices identified by the

industry experts. Below we present these critical factors about the processes and the key steps that contributed to exemplary SAs achieving a high level of success in safeguarding PII.

Culture of security. Staff from one SA noted everyone at the agency plays a part in safeguarding PII. As a result, data security is regarded as a core value of the SA, and they make sure the various safeguarding standards and their sensitivity are "*drilled into staff from day one of hiring*." To demonstrate the culture of security and how data security is a priority, the staff stated they have a unit that manages employee fraud by thoroughly investigate complaints of data breach, and that "*everybody probably knows somebody who was fired for not using the information appropriately*."

Cybersecurity education. Staff from some county-administered SNAP pointed to the significant role cybersecurity education played in enhanced safeguarding practices among their staff and within the SA. Staff stated, "*I think from the county worker's standpoint, cybersecurity education is the biggest thing*." For example, the SA now offers security awareness training to county offices, that the counties did not have access to before such as training in phishing scams.

Effective partnerships with technology vendors and state and county agencies. Staff from one SA stated partnering with technology vendors, such as Amazon Web Services (AWS), has been remarkably effective at increasing the knowledge and expertise available to both contractors working with those platforms and the organizational staff supporting them. This has enabled them to rapidly advance their security in the cloud and establish standards for architecture and security that promote the safeguarding of PII. Staff acknowledged having an effective partnership with their state and county agencies is vital. These partnerships ensure agency staff are diligent and follow through on their security obligations and controls. It ensures data security is at the forefront of program operations, and is a key part of the development and implementation of the program.

Advancements in Technology. Partnerships with technology vendors and leveraging statewide resources have led to advancements in technology. For instance, partnership with AWS has led to some SAs migrating onto the AWS cloud environment. Staff from one SA explained they have integrated their identity and access management tool with all their applications, making it easier for users to log in with their credentials and not have to remember different usernames and passwords across all their different applications. From a security perspective, identity and access management authenticates the user who is accessing the application. Staff from another SA noted the installation of the software to scan emails and alert staff of data breaches is helpful. The advancement in technology has implications on talent acquisition, especially for younger people.

Rigorous federal audits. Staff from some SAs attributed their success in safeguarding PII to the rigorous federal audits they are subjected to. These SAs have their federal audits every three years through IRS and SSA. They have a set of plans of action and milestones that

they follow as an offshoot of the federal audits. Thus, these audits themselves and any of the SAs or subcontractors that use the data have to follow through and make sure it conforms to the standards implicit in their rules and regulations. As one staff puts it: "*We are one of those five states that are up there on our security game, probably because we are so heavily audited from IRS. We have a state bank on the same network, too. So now we have all the financial regulations too, on top of that. So that puts us in a prime position just for the fact of who we are as who we serve for our customers*."

Strong state leadership support. SAs spoke of the role of their state leadership support as a key feature in their safeguarding pursuits. Staff from one SA stated they are considered leaders in safeguarding PII because security is one of the top priorities of their governor and for their SA. While some SAs acknowledged challenges with budget, this SA experienced no such challenge. This staff noted, "*I think if my IT director told our state director that we needed money for such to prevent a security aspect, then that issue I think could be presented to the governor where it would be approved*."

5. CONCLUSIONS

The study findings provide insight into the vulnerabilities and threats to PII that SAs encounter, as well as factors that affect the ability of SAs to safeguard PII. Findings from the web survey, and interviews with industry experts and five selected, exemplary SAs helped identify the challenges and threats faced by SAs, measures to safeguard PII, and factors that affect their ability to safeguard PII.

Industry experts identified a lack of clear and consistent guidance concerning compliance with data security protocols as a general vulnerability. They described a large amount of variability across states in terms of how data security compliance is implemented and prioritized, which hindered the implementation of necessary policies to safeguard PII. A general threat identified by experts was the lack of awareness among employees surrounding data privacy and IT attacks. To overcome this challenge, most SAs provide adequate training to personnel to ensure better understanding of their role in protecting PII. SAs conduct regular onsite and offsite backups of stored data to mitigate some of the challenges and prevent unauthorized physical access to stored SNAP PII. Most SAs also use software- and hardware-based encryption to protect data. They recently upgraded their data systems when the Affordable Care Act provided funding to upgrade their Medicaid data systems, which often shared data with SNAP. States also developed methods to prevent attacks on data systems using resources such as continuous training and system upgrades. SAs also noted that they must have a set of safeguarding rules for personnel when their position is terminated.

The expert interviews helped identify best practices in various areas of PII protection, including collecting, using, sharing, storing, and destroying PII data. The experts noted it is necessary to minimize the use, collection, and retention of PII and restrict it to what is necessary to fulfill their business goals. They also focused on the need for regularly training and educating users with access to PII about the risks associated with PII and how to protect it. Restricting user access to relevant information as defined by their business purpose could also be a helpful mechanism to protect PII.

SAs provided suggestions for FNS and other SNAP SAs on improving safeguarding practices. SAs suggested having adequate funding, in addition to clear compliance directives would help agencies provide better security. Staff from one SA noted it is important to provide regular training, ensure all contractors sign agreements, and educate staff on the importance of PII.

While applicants are asked to apply with just their name, address and signature, agencies need to communicate with applicants via email/telephone to collect more information, thereby exposing them to additional risks. Staff recommended modifying the application process to involve collecting more details such as having income and employment information, date of birth, and SSN as the current process causes extra work for the client

and agency. This delays the application processing time since it requires SAs to verify the applicant information and identify the right person. Another staff member further elaborated that for them to verify the identity of the applicant with just the name of the applicant as done with the current process requires them to access the address of several other individuals with the same/similar name, and this exercise is a potential threat to PII. Generally, the SAs agreed providing additional data during the application process on income, household composition, SSN, date of birth and phone number are all basic requirements to establish eligibility and will limit applicants' exposure to threats.

REFERENCES

Kissel, R., A. Regenscheid, M. Scholl, and K. Stine. 2014. “NIST Special Publication 800-122 Rev.1: Guidelines for media sanitization (800-88)." *US Department of Commerce, National Institute of Standards and Technology*, Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

McCallister, E, T. Glance, and K. A. Scarfone. 2010. “NIST Special Publication 800-122.: Guide to protecting the confidentiality of personally identifiable information (PII).” *US Department of Commerce, National Institute of Standards and Technology,* Gaithersburg, MD. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final#pubs-documentation

APPENDICES

Appendix A: Responses to Objective 1 Questions

Appendix B: Details of Analytical Methods

Appendix C: SA Survey Supplemental Tables

Appendix D: Web Survey for State Agencies

Appendix E: Semi-structured Interview Protocol for Industry Experts

Appendix F: Semi-structured Interview Protocol for Exemplary States

APPENDIX A: PRELIMINARY RESPONSES TO RESEARCH OBJECTIVE I QUESTIONS

In accordance with Objective 1 of the project, this document describes the legislation, regulations, and policies that address safeguarding of SNAP PII data. The document is organized around the five research questions associated with Objective 1.

Objective 1: Describe legislation, regulations, and policy that address safeguarding SNAP Participant Data

1.1. What Federal legislation addresses State and Federal government agencies' handling of PII? What legislation specifically addresses SNAP participant PII?

Broadly Applicable Privacy and Information Security Laws

The Federal Government has implemented two major laws pertaining to PII, that are particularly relevant to safeguarding the PII of SNAP participants. These laws consist of the **Privacy Act of 1974**[29] and the **Federal Information Security Modernization Act (FISMA) of 2014**[30]. The Privacy Act of 1974 was implemented to balance the Federal government's need to collect and maintain information about individuals with the right protect individuals against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and disclosure of PII by the Federal government. A primary policy objective of the Privacy Act focuses on restricting the disclosure of Federally maintained information retrieved by the name of an individual or by some identifier assigned to the individual. FISMA provides a comprehensive framework to protect government information, operations and assets against natural or man-made threats. The act requires each Federal agency to develop, document, and implement an agency-wide program to protect information security for systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. Of particular importance, FISMA is recommended by FNS[31] as a best practice for State Agencies (SAs) using Federal financial reimbursement, or Federal Financial Participation (FFP), to administer federal programs.

The **E Government Act of 2002**[32] requires Privacy Impact Assessments (PIA) for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in

[29] Privacy Act of 1974. 5 U.S.C. § 552a (2015). https://www.justice.gov/opcl/privacy-act-1974
[30] FISMA 2014. 44 U.S. Code § 3541 (2014). https://www.congress.gov/bill/113th-congress/senate-bill/2521
[31] USDA FNS (2017). FNS handbook 901 v2.0. Retrieved from https://fns-prod.azureedge.net/sites/default/files/apd/FNS_HB901_v2.2_Internet_Ready_Format.pdf
[32] E Government Act of 2002. 44 U.S.C. § 208 (2002). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

identifiable form. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system.

Laws Focused on Protecting SNAP PII

The **Food and Nutrition Act of 2008** authorizes the administration of SNAP by the Department of Agriculture's Food and Nutrition Service (USDA-FNS). The Food and Nutrition Act requires safeguards to protecting participant information. The recently enacted **Agriculture Improvement Act of 2018**[33] further expands regulations on safeguarding SNAP participant PII. The Act includes several new requirements for the administration of SNAP, such as the creation of the National Accuracy Clearinghouse, new FNS auditing requirements, and creation of a longitudinal participation database.

Section 7(h) of the Food and Nutrition Act of 2008[34] requires food stores using mobile technologies to redeem benefits to protect recipient privacy **(7 U.S.C. 2016(h)(14))**.

Section 11(a) (7 U.S.C. 2020 (a))[35] requires States to have records available for inspection and audit by FNS that are subject to data and security protocols agreed to by the State agency and Secretary.

Section 11(e) of the Food and Nutrition Act of 2008 (7 U.S.C. 2020(e))[36] requires that States shall provide safeguards in protecting participant data and limiting the disclosure of data to outside entities, such as other Federal agencies and law enforcement. Demonstration mobile redemption projects must also protect participant data.

Section 11(x) (7 U.S.C. 2020 (x))[37] now requires States to make available SNAP participants' PII to the new National Accuracy Clearinghouse (NAC) for determining dual enrollment across States. NAC requires meeting the security standards set by FNS in protecting the identity and location of vulnerable individuals.

Section 17 (7 U.S.C. 2026)[38] allows States to develop a longitudinal database for research and operational purposes. The data must have security and privacy protections, as required

[33] Agriculture Improvement Act of 2018. 7 U.S.C. § 2011-2036c (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/2/text
[34] Food and Nutrition Act of 2008. 7 U.S.C. § 2016(h) (2018). Retrieved from http://uscode.house.gov/view.xhtml?req=(title:%20section:2016%20edition:prelim)%20OR%20(granuleid:USC-prelim-title-section2016)&f=treesort&edition=prelim&num=0&jumpTo=true
[35] Ibid
[36] Food and Nutrition Act of 2008. 7 U.S.C. § 2020(e) (2018). Retrieved from http://uscode.house.gov/view.xhtml?req=(title:7%20section:2020%20edition:prelim)
[37] Agriculture Improvement Act of 2018. 7 U.S.C. § 2011-2036c (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/2/text
[38] Ibid

by Federal law and consistent with other appropriate practices, shall be implemented and maintained. PII must not be included in the longitudinal database.

1.2. What Federal regulations address State and Federal government agencies' handling of PII? What regulations specifically address SNAP participant PII?

The **OMB Circular No. A-130: Managing Information as a Strategic Resource**[39] establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the Federal information life cycle. Importantly, it represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at Federal agencies.

Regulations Specific to SNAP Participant PII

The **USDA Office of the Chief Information Officer (OCIO)** is responsible for all aspects of developing, delivering, and defending USDA information technologies. OCIO provides regulations on handling of PII breaches in the **Department Regulation (DR) 3505-005 Cyber Security Incident Management Policy**.[40] It provides guidance on roles and responsibilities of responsible parties in the event of a security incident. It requires the Agriculture Security Operations Center (ASOC) Computer Security Incident Response Team (CSIRT) to communicate and coordinate cyber security incident management for all systems, assets, and data with internal and external entities, as required, to manage USDA incidents.

US Code of Federal Regulations (CFR) Title 7 – Agriculture contains the rules and regulations issued by federal agencies regarding USDA programs, including SNAP. Title 7 describes the role of FNS and the administrative requirements of SNAP.

7 CFR 272.1 - General terms and conditions[41] states that SAs must adequately protect information from unauthorized disclosures. It restricts the disclosure of PII to several instances, including verifications, immigration status, local law enforcement, and certifying the eligibility of school-aged children for the National School Lunch Program. Each instance must meet the conditions described in 7 C.F.R. 272.1.

---

[39] OMB (1996). Circular No. A-130: Managing information as a strategic resource. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf This A-130 link should be updated to https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[40] USDA (2013). Cyber Security Incident Management Policy. Retrieved from https://www.ocio.usda.gov/sites/default/files/docs/2012/DR3505-005_Cyber_Security_Incident_Management_Policy_v.pdf

[41] Agriculture, 7 C.F.R. § 272.1 (2014). Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?SID=68a7eadfb7bf7a96da3a49d92a159bc0&mc=true&node=pt7.4.272&rgn=div5#se7.4.272_11

To facilitate eligibility verifications, **7 CFR 272.8 – State Income and eligibility verification system**[42] limits the disclosure of participant data to specific Federal programs, including Medicaid, Temporary Assistance for Needy Families, and Unemployment Insurance. It requires States to execute data exchange agreements with other SAs that manage these programs. The agreements must specify the information to be exchanged and the procedures which will be used in the exchange of information.

7 CFR 274.5 – Record retention and forms security[43] requires State agencies to maintain participant records for a minimum of three years. These records, including Electronic Benefit Transfer (EBT) cards, must meet minimum security and control procedures regarding storage and access.

7 CFR 274.8 – Functional and technical EBT system requirements[44] requires States to have system security protocols for EBT systems such as PIN verification and message encryption. States must conduct periodic risk analyses of their EBT systems. In submitting an Advanced Planning Document (APD), a separate EBT security component must be included.

7 CFR 277.18(m) - State Systems Advance Planning Document (APD) process[45] holds States responsible for the security of all information system (IS) projects. State agencies are required to implement an IS security program and conduct periodic risk analyses and security reviews.

1.3. What additional guidance has FNS provided State agencies on handling PII?

The FNS State Systems Office published the **FNS Handbook 901: The Advanced Planning Document Process: A State Systems Guide to America's Food Programs**[46], to assist SAs with navigating FNS requirements for securing approval and obtaining funding for modernizing their eligibility systems and EBT benefit delivery services. The APD process requires SAs to describe their methods in safeguarding PII, and specifies management, operational, technical, privacy, and EBT specific controls that SAs must implement throughout the APD process and throughout the lifecycle of their newly implemented

[42] Agriculture, 7 C.F.R. § 272.8 (2014). Retrieved from https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=2&SID=4eb917122fbdc3394689bc6f3b251c4d&ty=HTML&h=L&mc=true&r=PART&n=pt7.4.272#se7.4.272_18

[43] Agriculture, 7 C.F.R. § 274.5 (2014). Retrieved from https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=00adc66f7ee77b3af0f6203e5b1d5d54&ty=HTML&h=L&mc=true&r=PART&n=pt7.4.274#se7.4.274_15

[44] Agriculture, 7 C.F.R. § 274.8 (2014). Retrieved from https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=00adc66f7ee77b3af0f6203e5b1d5d54&ty=HTML&h=L&mc=true&r=PART&n=pt7.4.274#se7.4.274_18

[45] Agriculture, 7 C.F.R. § 277.18 (2014). Retrieved from https://www.ecfr.gov/cgi-bin/text-idx?SID=1b35ea97d208028e8f7ffc4d664857ea&node=se7.4.277_118&rgn=div8

[46] USDA FNS (2017). FNS handbook 901 v2.0. Retrieved from https://fns-prod.azureedge.net/sites/default/files/apd/FNS_HB901_v2.2_Internet_Ready_Format.pdf

systems. In addition to regularly updating the Handbook, the State Systems Office provides technical assistance to SAs in preparing the APD, reviews and decides on funding proposals for Federal Financial Assistance for EBT and eligibility system upgrades for all FNS programs, and provides technical assistance and monitoring of projects that are funded. The Office is a virtual team of experts in systems and the APD process in various FNS regional offices, with a core group of staff in Denver, CO.[47]

In 2018, FNS released the *SNAP Insider Threat Detection and Prevention Guidance* to State agencies. This supplemental guide to the SNAP Fraud Framework is a roadmap to assist States to effectively prevent and detect employee fraud through detection, prevention, and investigation strategies such as reducing access to recipient PII and providing guidance for States on following-policy and laws that govern the use of PII[48]

1.4. What State legislation and regulations govern State government agencies' handling of PII?

The table below provides a sample of State legislation and regulations that govern the handling of PII. The subset of States identified in the table include county- and State-administered SNAP agencies, agencies that vary considerably in size, and agencies residing within various FNS regions. Through the SA survey, the research team will gather additional information from all 53 SNAP SAs.

State	FNS Region	SNAP Program Administration	Governing IS Body	Legislation/ Regulation	Description
California	Western Region	County	Office of Information Security	California Civil Code 1798-1798.78[49]	Requires SAs to establish appropriate and reasonable administrative, technical, and physical safeguards, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury
Maryland	Mid-Atlantic Region	State	Department of Information Technology	State Government Article, §10-1301 et seq., Annotated	Requires meeting the Federal Information Processing Standards

[47] USDA FNS (2018). FNS Oversight: State Systems & Advance Planning Document Process. Retrieved from https://www.fns.usda.gov/apd/fns-oversight-state-systems-advance-planning-document-process.
[48] USDA FNS (2018). SNAP Insider Threat Detection and Prevention Guidance.
[49] California Civil Code 1798-1798.78. Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=5.

State	FNS Region	SNAP Program Administration	Governing IS Body	Legislation/ Regulation	Description
				Code of Maryland, Governmental Procedures-Security and Protection of Information, (SB 676) of 2013	issued by the National Institute of Standards and Technology (NIST)
New York	Northeast Region	County	Office of Information Technology Services	Personal Privacy Protection Law (Public Officers Law, Article 6-A, sections 91-99) [50]	Requires SAs to establish appropriate administrative, technical and physical safeguards to ensure the security of records
South Carolina	Southeast Region	State	Department of Administration Division of Technology	Title 30 - Public Records / Chapter 2 - Family and Personal Identifying Information Privacy Protection[51]	Requires SAs to develop privacy policies and procedures to protect PII. It limits the sharing of data to other agencies
Texas	Southwest Region	State	Department of Information Resources	Texas Cybersecurity Act[52]	Requires agencies to assess their cybersecurity practices and provide cybersecurity training and simulation exercises

The **National Conference of State Legislatures (NCSL)**[53] finds that all 50 States, DC, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving PII.[54] As of November 2018, NCSL finds that at least 22 states have enacted 52 cybersecurity bills.[55] Some key areas of legislative activity include:

[50] Public Officers Law, Article 6-A. Retrieved from https://www.dos.ny.gov/coog/pppl.html
[51] Title 30 - Public Records / Chapter 2 - Family and Personal Identifying Information Privacy Protection. Retrieved from https://www.scstatehouse.gov/code/t30c002.php
[52] Texas Cybersecurity Act. Retrieved from https://capitol.texas.gov/tlodocs/85R/billtext/pdf/HB00008I.pdf#navpanes=0
[53] http://www.ncsl.org/
[54] NCSL (2018). Security breach notification laws. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[55] NCSL (2018). Cybersecurity legislation 2018. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx#Additional

- Improving government security practices.
- Providing funding for cybersecurity programs and initiatives.
- Restricting public disclosure of sensitive government cybersecurity information.
- Promoting workforce development and training and economic development.

The **National Association of State Chief Information Officers (NASCIO)**[56] and Deloitte recently conducted a national State level cybersecurity study.[57] The study finds that more than half of States do not have a program for managing privacy compliance and lack formal processes for dealing with complaints from the public about information privacy such as a privacy hotline. The study also finds that external web applications and malicious code are the leading sources of security breaches.

1.5. Describe the National Institute of Standards and Technology (NIST) guidelines.

The **NIST** is responsible for developing information technology (IT) security standards and guidelines for Federal ISs. For these guidelines, NIST defines PII in accordance with the **GAO definition**[58]: "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

In 2006, NIST published the **Federal Information Processing Standards Publication (FIPS PUB) 200 Minimum Security Requirements for Federal Information and Information Systems**[59] and *a risk-based process for selecting the security controls necessary to satisfy the minimum security requirement*. These guidelines consist of 17 security-related areas related to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:

[56] https://www.nascio.org/
[57] Deloitte & NASCIO (2018). Cybersecurity study states at risk: Bold plays for change. Retrieved from https://www.nascio.org/Portals/0/Publications/Documents/2018/2018DeloitteNASCIOCybersecurityStudyfinal.pdf
[58] GAO (2008). Privacy. Alternatives exist for enhancing protection of personally identifiable information. Retrieved from https://www.gao.gov/new.items/d08536.pdf
[59] NIST (2006). Minimum security requirements for federal information and information systems. Retrieved from https://csrc.nist.gov/publications/detail/fips/200/final

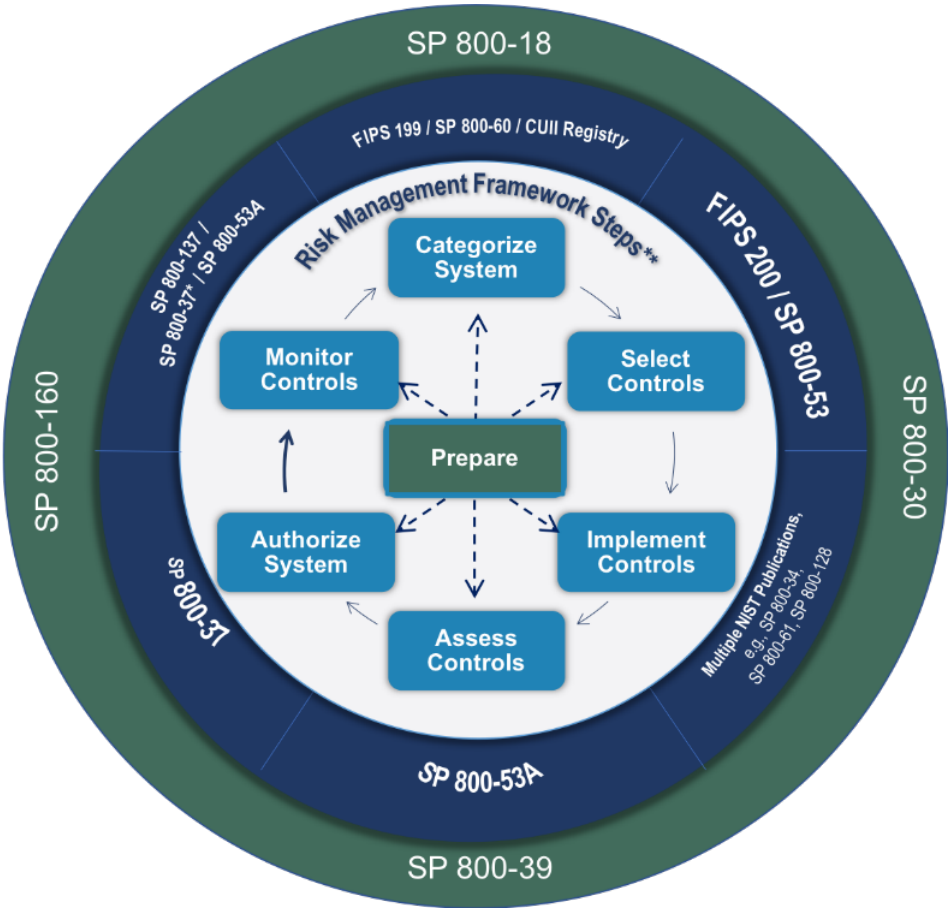
Defined in FIPS 200: Security Control Families and Their Identifiers			
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Certification, Accreditation, and Security Assessments	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information integrity
MA	Maintenance		

In 2010, NIST released the **Guide to Protecting the Confidentiality of PII**.[60] This document provides several pertinent recommendations:

- Organizations should identify all PII residing in their environment.
- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Organizations should categorize their PII by the PII confidentiality impact level.
- Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.
- Organizations should develop an incident response plan to handle breaches involving PII.
- Organizations should encourage close coordination among their chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII.

In addition, NIST developed the Risk Management Framework (RMF) in **Special Publication (SP) 800-37 Rev. 1**.[61],[62]. RMF provides a comprehensive process for integrating security and risk management activities into the system development life cycle. The six-step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring.

[60] NIST (2010). Guide to protecting confidentiality of personally identifiable information (PII). Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
[61] NIST (2010). Guide for applying the risk management framework to federal information systems. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final
[62] Special Publication (SP) 800-37 Rev. 2 is currently in draft: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft



Finally, the FNS Handbook 901 identifies several NIST guides that are pertinent for protecting the PII of SNAP participants:

- Guide for Conducting Risk Assessments: Information Security
- Contingency Planning Guide for Federal Information Systems
- Guide to Information Technology Security Services
- Security and Privacy Controls for Federal Information Systems and Organizations
- Computer Incident Handling Guide
- Security Considerations in the System Development Life Cycle: Information Security
- National Checklist Program for IT Products – Guidelines for checklist Users and Developers
- Guidelines for Media Sanitization
- Technical Guide to Information Security Testing and Assessment
- Guidelines for Managing the Security of Mobile Devices in the Enterprise

APPENDIX B: DETAILS OF ANALYTICAL METHODS

This appendix summarizes the analytical approach undertaken by the study team for the analysis of data collected from the interviews of industry experts and exemplary SAs, and from the web survey.

Qualitative Data Analysis

The study team utilized information gathered from in-depth interviews of exemplary SAs chosen to reflect best practices in various areas of PII protection, and from interviews of industry experts provided insights into gaps in knowledge, practices, and policies identified in the SA surveys, as well as perspective on how PII security is handled in other settings. This section provides further details on the methods of data collection and qualitative analysis.

Interviews with Industry Experts

Data Collection

The study team conducted interviews with eight experts to discuss their broader views of PII protection from private industry and public sector perspectives, and to clarify both private industry and public sector benchmarks for information security, thereby informing recommendations for SNAP SAs for improving their procedures and processes for safeguarding SNAP participants' PII. 2M used a modified snowball sampling approach to identify industry experts in the fields of IT, data privacy protection, SNAP outreach, and EBT and SNAP benefit redemption. A preliminary list of experts was developed from a list recommended by the USDA Food and Nutrition Service (FNS); the study's subject matter experts; and industry experts identified by the 2M study team. 2M contacted those on the preliminary list through recruitment emails, LinkedIn messaging, and follow-up phone calls describing the study and informing the respondent that other staff had recommended them as experts who could provide valuable insight into how to handle and safeguard PII. Experts who agreed to participate in the interviews were asked to provide their availability for the interview; those who declined as they were not the right person for an interview were encouraged to recommend other experts who might be willing to participate. During the interviews, the study team inquired about additional experts from the interviewee's organization or from their network whom the study team may want to interview. FNS and the study team reviewed the names provided and interviewed experts who were deemed appropriate for the project.

Prior to the selection of experts and the development of an interview protocol, the study team conducted three informal exploratory interviews with FNS and SA staff to obtain greater insight into key concepts associated with safeguarding SNAP participants' PII. The goal of these informal discussions was to obtain greater insight and understanding of (1)

how states organize systems to safeguard SNAP participants' PII and how states' safeguarding methods are integrated with other state efforts; (2) issues to consider related to safeguarding SNAP PII during different phases of the data lifecycle, such as SNAP application, reapplication, data sharing, and data storage and how these phases may depend on state contexts (e.g., State application processes, existing IT systems); and (3) identification of potential candidates for the semi-structured interviews with staff at five exemplary SAs and with industry experts. The information and insights obtained through these discussions played a critical role in the subsequent development of the interview protocols for the industry experts.

Semi-Structured Interviews

The study team incorporated the insights and information obtained during the exploratory interviews with FNS staff and other pertinent stakeholders to develop a semi-structured interview protocol for the interviews with industry experts. In collaboration with FNS, the study team developed the interview protocol to capture primarily information on best practices associated with safeguarding SNAP PII. Other question domains that the study team examined through the interview included the policies and practices in public agencies versus private companies, as well as a discussion on key gaps, applicable best practices, and opportunities for improvement. We provide in **Exhibit B-1** a list of domains captured in the interview protocol.

Data Collection Procedures

In collaboration with FNS, the study team developed recruiting materials for industry experts. These materials described the purpose of the study, the participation requirements, the data collection period, and the estimated time required to complete the interview. The study team implemented our recruitment processes to track up to four email recruitment attempts and follow-up phone calls when applicable to reach those industry experts who wish to participate.

The study team conducted telephone and video interviews lasting approximately 1 hour each using the semi-structured interview protocol. Prior to conducting each interview, the study team sought permission to record the interview to supplement notetaking and subsequent qualitative analysis. The semi-structured format gave the study team a standard set of questions that they asked of all interviewees while allowing flexibility for the study team to ask probing questions about pertinent details to obtain further clarity and capture critical details on significant or new information.

Exhibit B-1 | Industry Expert Interview Domains

- Gaps in knowledge and implementation
- Vulnerabilities and threats to PII
- Areas SAs have the most difficulties implementing safeguards.
- Barriers to compliance
- Age of data systems
- Use of security services from vendor companies
- Lack of alignment with other SAs
- Limits to resources for IT security development
- Focus on other high priority work
- Unclear or inadequate federal requirements
- Industry best practices, in the areas of—
- Personnel security
- Information collection
- Information processing
- Information transmission
- Information storage
- Information destruction
- Important supports for maintaining PII security
- Personnel policies and procedures
- Security policies and operations
- Program operations

Interviews with Exemplary SAs

Selection of Exemplary SAs

This section describes the study team's process for identifying and selecting SNAP state agencies (SAs) that the study team recognizes as "exemplary" in protecting personally identifiable information (PII) based on the information gathered through the SA web survey.

Given contextual factors (e.g., IT systems, SNAP application processes), it was important to identify SAs that address safeguarding PII in multiple contexts to increase the generalizability of the findings. Thus, we began the process for selecting the exemplary SAs by developing a set of indicators from the survey instrument that reflect best practices in various areas of PII protection. These indicators were based on an array of critical questions (Exhibit B-2) from the survey that represent the following primary domains:

- Personnel policies and procedures
- Security policies and procedures
- Program operations

Exhibit B-2 | Critical Questions Identified from the Web Survey

Survey Chapter	Question Number	Survey Question
Context	2.4	How long has it been since your SA's system security plan for safeguarding PII of SNAP applicants and participants was last updated?
	2.8	To what extent has your SA faced challenges with understanding, complying with, testing or validating, or updating its system security plan for safeguarding PII of SNAP applicants and participants? ○ Understanding the system security plan ○ Complying with the system security plan ○ Testing or validating the system security plan ○ Updating the system security plan
Personnel Policies and Procedures	3.9	To what extent does your SA's security plan meet and/or exceed the safeguarding requirements for personnel that are in FNS Handbook 901 and associated FNS regulations? ○ Ensuring that staff working with PII have met the requisite security requirements and are approved to access data ○ Conducting personnel background checks ○ Using role-based security levels to provide data access ○ Delivering regular IT security training and education
Security Policies and Procedures	4.1	To what extent has your SA encountered the following vulnerabilities and threats to SNAP PII? ○ Improper storage or disposal of physical materials that contain PII (such as printouts or other paper documents) ○ Improperly secured systems with access to PII ○ Improperly secured mobile devices with access to PII ○ Unauthorized use of system resources by SA employees to access PII or unauthorized manipulation of PII data by SA employees ○ Unauthorized disclosure of PII data by SA employees or a trusted partner ○ Macro-level system failures

Survey Chapter	Question Number	Survey Question
		○ Failures or decreases in the reliability of hardware ○ Failures or decreases in the reliability of software ○ Denial of service attacks ○ Phishing, spoofing, or pharming ○ Introduction of malicious code (such as viruses, spyware, or malware)
	4.3	Has your SA implemented the following firewall safeguards, policies, and procedures? ○ Use of a hardware-based firewall ○ Use of a software-based firewall ○ Maintaining audit records of all security-related events/ Limiting firewall access to network security analysts or other approved users ○ Regularly reviewing the list of approved users with access to the firewall ○ Timely installation of security-related updates, fixes, or modifications that have been tested and approved
	4.4	Does your SA allow employees remote access (such as a VPN connection) to systems containing the PII of SNAP applicants and participants?
	4.5	Which of the following procedures has your SA implemented for providing employees remote access to PII?
	4.7	Disasters and other emergencies pose a formidable challenge to safeguarding the PII of SNAP applicants and participants. In your opinion, are the following components present within your SA's disaster recovery plan to protect PII during disasters or other emergency situations? ○ It effectively details how the SA will recover and restore the system to normal operations. ○ It specifies a process for protecting PII from internal and external threats until the system is restored to normal operations. ○ It is effectively integrated into the SA's security plan.

Survey Chapter	Question Number	Survey Question
		○ It provides a process for training staff in their specific response to a disaster according to their roles. ○ It specifies a process for maintaining Local Area and Wide Area Networks. ○ It specifies a process for maintaining desktops and personal computers. ○ It specifies a process for maintaining SA websites. ○ It specifies a process for maintaining distributed and mainframe systems. ○ It specifies alternative physical locations for operations in the event that original facilities are unavailable. ○ It can be activated on its own and does not require that other contingency plans be activated first.
	4.8	To what extent does your SA's security plan meet and/or exceed the safeguarding requirements that are in FNS Handbook 901 and associated FNS regulations? ○ Hardware-specific controls ○ Software-specific controls ○ Network-specific controls ○ Regularly assessing risk and vulnerabilities ○ Regularly performing security testing ○ Developing emergency preparedness and contingency plans
SA's Procedures that Involve Safeguarding PII throughout the SNAP Application and Recertification Processes	5.4	Does your eligibility system mask Social Security numbers during data entry?
	5.11	Is there a time-out function used on caseworker eligibility system screens that contain PII?
	5.13	Does your SA's security plan have a specific policy for responding to security incidents?
	5.14	Does your plan include required steps for incident response, including required reports to FNS and other agencies?
	5.15	To your knowledge, has your SA's SNAP eligibility system or application website ever had a security incident where PII was compromised by internal users or external entities?
	5.19	We are interested in understanding the extent to which your SA's application and recertification procedures meet the safeguarding

Survey Chapter	Question Number	Survey Question
		requirements specified in FNS Handbook 901 and FNS regulations and policy memos. o Masking PII during data entry o Implementing time-out features on eligibility system screens containing PII o Secure delivery of SNAP benefits via EBT o Matching PII to other data sources for eligibility determination o Matching PII to other data sources for program integrity purposes
SA's Operations associated with the maintenance and storage of PII	6.1	Which of the following safeguards has your SA implemented to prevent unauthorized physical access to stored SNAP PII? o Conducting regular risk assessments of a facility's physical resources o Identifying critical areas within a facility for implementing physical safeguards (such as areas containing system hardware or software) o Assessing risk among supporting services (e.g., electrical power); backup media; and other elements required for system operations o Conducting regular onsite and offsite backups of stored data o Securely disposing of data after established archiving or retention periods have passed o Implementing facility-wide security measures on the basis of the level of risk to physical resources o Regularly reviewing the list of persons with physical access to SNAP PII o Periodically reviewing physical safeguards for effectiveness o Periodically reviewing reports and documents that can be printed with PII
	6.2	Which encryption methods are used by your SA to safeguard data when they are stored or when the data are "at rest"?
SA's Operations Associated with Sharing	7.4	Which encryption methods are used by your SA to transmit PII data? o Software-based encryption o Hardware-based encryption

Survey Chapter	Question Number	Survey Question
and Transferring PII		○ My SA does not currently use encryption methods when transmitting PII data ○ Don't know/unsure
SA's opportunities and Challenges for Safeguarding PII	8.1	How would you rate your level of satisfaction with your SA's approach to the following domains for safeguarding PII? ○ Personnel Policies and Procedures: Approaches used to ensure that staff working with PII have met the requisite requirements to access data at approved security levels and receive regular security training and education ○ Security Policies and Procedures: Approaches for implementing a robust security plan; securing PII across hardware, software, and systems; and regularly assessing risk and vulnerabilities and performing security testing ○ Program Operations: Safeguards associated with administering SNAP such as masking or time-out features, using secure data systems to process information, secure delivery of SNAP benefits via EBT, and protected matching of PII to other data sources for eligibility determination or program integrity purposes

Based on these critical questions, the study team constructed a score that helped rank the SAs by their performance across the three domains. To create a score and assign ranks to the SAs based on their responses, we recoded the survey responses to a binary number. This method is similar to the one used to construct the Food Insecurity Index, where affirmative responses were assigned a value of 1, and defined as those responses that indicate SAs followed best practices in safeguarding PII. The negative responses—those that indicate that SAs did not follow best practices—were assigned a value of 0. For example, in question 2.8 below, all the SAs who faced significant challenges with understanding, complying testing or validating the security system and selected responses "To a great extent" or "Somewhat" were assigned a value of 0, and those that chose "Very Little or "Not at all" were assigned a value of 1.

2.8. To what extent has your SA faced challenges with understanding, complying with, testing or validating, or updating its system security plan for safeguarding PII of SNAP applicants and participants? SELECT ONE RESPONSE PER ROW

	To a Great Extent	Somewhat	Very Little	Not at All
Understanding the system security plan	○	○	○	○
Complying with the system security plan	○	○	○	○
Testing or validating the system security plan	○	○	○	○
Updating the system security plan	○	○	○	○
Other (Please specify) _____	○	○	○	○

Similarly, SAs that responded with "Meeting requirements" or "Especially Successful at Meeting Requirements" for survey question 3.9 were assigned 1, and otherwise 0.

3.9. To what extent does your SA's security plan meet and/or exceed the safeguarding requirements for personnel that are in FNS Handbook 901 and associated FNS regulations? Please give us your best assessment of the following: SELECT ONE RESPONSE PER ROW.

	Meeting Requirements, with Room for Improvement	Meeting Requirements	Especially Successful at Meeting Requirements
Ensuring that staff working with PII have met the requisite security requirements and are approved to access data	○	○	○
Conducting personnel background checks	○	○	○
Using role-based security levels to provide data access	○	○	○
Delivering regular IT security training and education	○	○	○

Once the questions were recoded to binary responses, we summed the affirmative responses to obtain a final score for each SA. The final score was ranked from highest to lowest. The maximum possible score that an SA could obtain is 60 for state-administered surveys and 24 for county-administered surveys (summing affirmative response to all critical questions). In cases where SAs obtained the same rank, both were included in the sample for further input from FNS. Further, we distinguish between the smaller and larger states to maintain diversity in the sample. The states are identified as small or large based on their population size.[63] We present in **Exhibit B-3** SAs that received the highest score and have been identified as exemplary SAs. Of the 11 SAs selected based on their score, FNS

[63] Size of a state is determined using population estimates from the 2020 Census. The population range was used to obtain the median population across states. Small states are defined as those with population less than the median population, and larger states are those with population greater than the median population across states. Source: https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html#par_textimage_1574439295

selected the following five SAs for interview: Oklahoma, South Carolina, North Dakota, California, and New Jersey.[64]

Exhibit B-3 | Exemplary States

Exemplary States
State Administered – Small Size SAs - Oklahoma, Nebraska, District of Columbia
State Administered – Large Size SAs - Indiana, Missouri, Kentucky, South Carolina
County Administered – Small Size SAs – North Dakota
County Administered – Large Size SAs -California, North Carolina, New Jersey

We followed a similar procedure to identify domain-specific, exemplary SAs (see **Exhibit B-4**). The scores for SAs by domain are based on affirmative responses to specific domain-based survey questions. For example, responses to survey questions 3.9 and 8.1 are used to determine the score for the Personnel Policies domain with a maximum possible score of 5. Similarly, the score for the Security Policies domain is determined using questions 2.4, 2.8, and other questions related to security policies, with a maximum possible score of 75. Scores for the Program Operations domain is obtained using questions 6.1, 6.2, and others, with the maximum possible score being 4.

Exhibit B-4 | Exemplary States by Domain

Exemplary States
Personnel Policies
State Administered – Small Size SAs - Oklahoma, Nebraska
State Administered – Large Size SAs - Indiana, Missouri
County Administered – Small Size SAs – North Dakota
County Administered – Large Size SAs -California, North Carolina
Security Policies
State Administered – Small Size SAs – Oklahoma, Nebraska
State Administered – Large Size SAs – Indiana, Kentucky
County Administered – Small Size SAs – North Dakota
County Administered – Large Size SAs – California, North Carolina
Program Operations
State Administered – Small Size SAs - Oklahoma, Nebraska
State Administered – Large Size SAs - Indiana, Kentucky
County Administered – Small Size SAs – North Dakota
County Administered – Large Size SAs – California, North Carolina, Colorado, New Jersey

[64] Nebraska, Indiana, Missouri, and Kentucky were potential back-ups that the study team did not contact.

Data Collection for Interview with Exemplary SAs

Prior to 2M contacting the SAs, FNS sent a request to the five SAs to participate in the study. The 2M Team followed that email with an invitation packet to the SAs. The packet contained background information on this phase of the study, guidance on which types of personnel could most effectively answer specific sections of the interview questions, and instructions for participating in the interviews. For states in which several staff worked with the SA director to complete the web survey, we encouraged the SA director to invite all relevant staff to participate in the follow-up interview, which was conducted by group conference call.

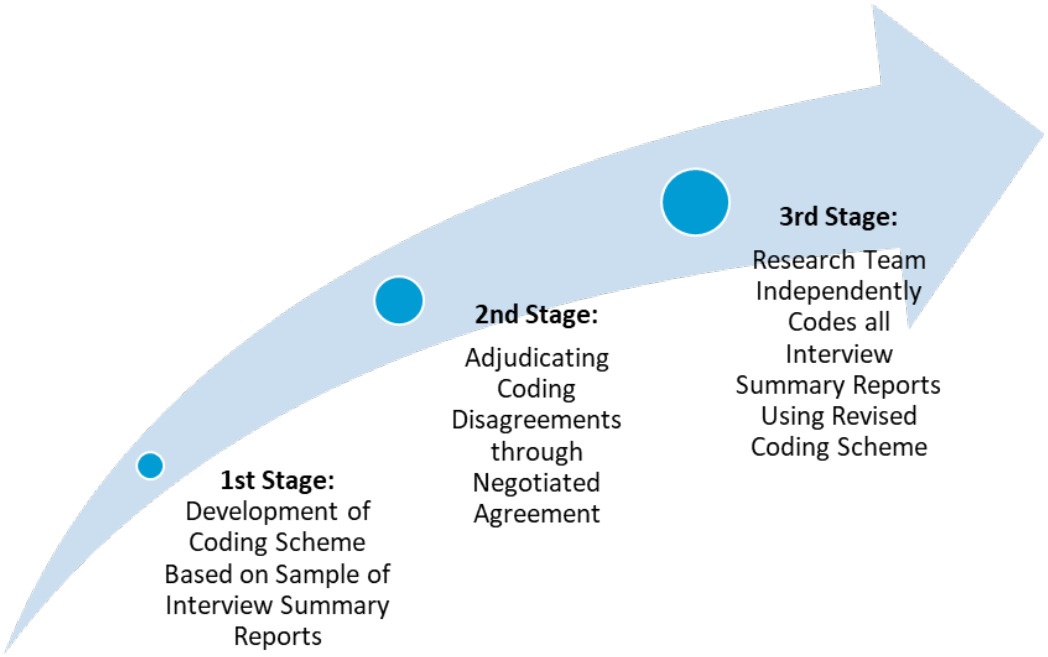
2M designed the semi-structured interviews with exemplary SAs to discover lessons learned, uncover information about staff experiences protecting PII, and glean on-the-ground insights that can be used to create strategies for improving PII-protection practices. To corroborate and elaborate on SA strategies and practices, 2M worked with the SAs to identify the most relevant staff members with whom to conduct the interviews, including staff with direct access to SNAP IT systems and staff who have considerable experience with the State's data security plans. We present findings from the interviews with staff from exemplary SAs in the next section.

Analysis of Qualitative Data

After the data collection phase was complete, the study team conducted a qualitative analysis of the industry expert and exemplary SAs interview data to ensure the subsequent findings provide FNS a clear picture of the industry best practices associated with safeguarding SNAP PII. Similar approach was used to analyze data from the interviews of exemplary SAs. The study team used a multistep coding process to analyze the data related to the gaps in knowledge, practices, and policies identified in the SA surveys, as well as perspective on how PII security is managed in other settings. The team cleaned the interview transcripts, de-identified them, and uploaded them to NVivo to facilitate the qualitative analysis. A researcher coded the interviews using the multistep process for developing coding schemes for semi-structured interview transcripts.

Exhibit B-5 provides an overview of the three-stage procedure used to develop the coding scheme. The first stage of this process focused on developing a deductive coding scheme based on a sample of transcripts to address a key objective of this component of the study, which is to identify best practices and guidelines for improving current practices to safeguard PII that can be made available to all SAs. The second stage focused on adjudicating any coding disagreements through negotiation among the coders. While the first stage focused on achieving a high level of reliability, the second stage focused on establishing a high level of intercoder agreement. In the third stage, the study team coded nine interview transcripts using the revised coding scheme.

Exhibit B-5 | Coding Process



Upon completion of all coding, the study team ran structured queries to explore and matrix data based on emergent themes.[65] The team then conducted a thematic analysis of the coded data to identify themes relevant to the associated research questions and to extract key learnings regarding best practices for safeguarding SNAP PII.

Quantitative Data Analysis

This section provides the methods used to collect data from the web survey and analyze it to provide a better understanding of survey response rates including the number of completed web surveys; the number of surveys completed by Food and Nutrition Service (FNS) region; the proportion of survey questions completed by state agency (SA); and SA responses by survey question. We begin by providing information on the web survey population.

SA Web Survey Sample

Fifty-three SAs were selected to participate in the web survey, including SAs for the 50 States, District of Columbia, and two U.S. territories: Guam and the U.S. Virgin Islands. The Study Team sent out email invitations for the web survey to all 53 SA Directors on September 10, 2021, and the survey closed on January 31, 2022. 2M sent multiple email and

[65] Themes are patterns in the coded qualitative data related to the research question. Themes are usually broader than codes. Often a single theme can consist of multiple codes. For more information see: https://www.scribbr.com/methodology/thematic-analysis/.

phone reminders to those who had not completed the survey during the data collection period.

Survey Response Rate and Sample Distributions

The web survey was conducted using a final sample size of 53 SAs. While the goal was to obtain responses from all 53 SAs, the 2M Team obtained a total of 47 completed surveys (an 88.7 percent response rate) by the closing date for the SA survey (Exhibit B-6), which completed at least more than 60% percent of survey questions. Among these SAs completing surveys, 39 SAs were state administered and eight were county administrated. The 53 SAs are distributed almost equally across the seven FNS regions; as shown in Exhibit B-7, all SAs in the Mountain Plains Region and Southwest Region completed the web survey, while only 75 percent of SAs in the Western Region completed the web survey.

Exhibit B-6 | SA Survey Data Collection Summary

Administration Type	Number of SAs Completing Survey*	Number of SAs Not Completing Survey **	Response Rate***
All	47	6	88.7%
State-Administered SAs	39	4	90.7%
County-Administered SAs	8	2	80.0%

* Includes surveys where SA respondents completed 60% or more of the survey items.
**Includes surveys where SAs respondents completed fewer than 60% of the survey items.
***Equals the number of completed cases divided by the total number of that type of SAs.

Exhibit B-7. Number of SAs and Surveys Completed by FNS Region

FNS Regions	Number of SAs	Number of Completed Surveys	Response Rate
Western Region	8	6	75.0%
Midwest Region	7	6	85.7%
Mid-Atlantic Region	7	6	85.7%
Northeast Region	8	7	87.5%
Southeast Region	8	7	87.5%
Mountain Plains Region	8	8	100.0%
Southwest Region	7	7	100.0%

Survey Completeness by SA

The web survey consisted of 65 survey questions, though because many survey questions included multiple sub-questions, the total number of survey items potentially requiring a response was 157. Exhibit B-8 summarizes completeness of survey questions by SA. Among the state-administered SAs that were considered to have completed the survey, Wyoming SA completed the most survey questions (100 percent), while Connecticut SA

completed the fewest (60.6 percent). Among county- administered SAs that completed the survey, California, North Carolina, and North Dakota SAs all completed 95.2 percent of survey questions, followed by Wisconsin SA, which completed 94.6 percent.

Overall, the completion rates of survey questions were relatively high across the 47 SAs that completed the survey: 39 SAs completed more than 80 percent of survey questions. For the six SAs that were categorized as failing to complete their surveys, rates ranged from Maryland SA's completion of 38.4 percent of the survey questions to New York SA's completion of just 1.3 percent.

Exhibit B-8. Number of Survey Questions Completed by SAs

Administration Type				Completeness Rates**
Average		**129.2**	**146.1**	**88.4%**
County-Administered SAs	New Jersey	113	157	72.0%
	Virginia	115	142	81.0%
	Ohio	139	152	91.5%
	Colorado	138	147	93.9%
	Wisconsin	139	147	94.6%
	California	140	147	95.2%
	North Carolina	140	147	95.2%
	North Dakota	140	147	95.2%
Average		**133.0**	**148.3**	**89.8%**
SAs that Did Not Complete the Survey (*n* = 6)				
State-Administered SAs	Washington	18	150	12.0%
	Oregon	33	140	23.6%
	Tennessee	54	142	38.0%
	Maryland	58	151	38.4%
Average		**40.8**	**145.8**	**28.0%**
County- Administered SAs	New York	2	157	1.3%
	Minnesota	47	147	32.0%
Average		**24.5**	**152.0**	**16.7%**

* The total number of questions varied by SA, because some questions did not apply to some SAs based on answers they had provided earlier.
** Equals the number of completed questions divided by the number of applicable survey question

Analysis of Survey Data

The study team tabulated survey responses across all SAs. The analysis resulted in an overview of the prevalence and variation in specific practices and the degree to which SA staff are aware of legislation, regulations, and guidelines regarding safeguarding PII. While multiple staff members contributed information on the survey for their SA, the SA is the unit

of analysis and only one survey is obtained from each SA.[66] We had a response rate of 88.7 percent and did not conduct a nonresponse bias adjustment.

The study team generated descriptive statistics like frequency tables and percent of responses for all survey items. Additional statistics like means, minimum and maximum values were also included for some of the survey items. Profiles of practices were described for each SA, to identify variation in practices of SAs in specific domains. For example, an SA may implement strong practices regarding the collection and destruction of PII but have weak practices regarding sharing PII with other organizations and preventing the disclosure of PII via derived or aggregated data. Another SA may implement strong practices for collecting, sharing, and destroying PII but have poor implementation of practices protecting PII from unauthorized access. In other words, there could be a variation in SAs with similar practice profiles.

[66] Therefore, there is no need to weight the sample for unequal probability of selection or to adjust for clustered sampling statistically. We do not plan on weighting the sample.

APPENDIX C: SURVEY SUPPLEMENTARY TABLES

Study Objective 2: Describe methods that can be used to safeguard PII

2.1 What measures are established to prevent unauthorized users from accessing PII?

Table 1. Measures Implemented by SAs to Prevent Unauthorized Physical Access to Stored SNAP PII

Safeguarding Measures	Frequency	Percentage
Conducting regular onsite and offsite backups of stored data	41	91.1%
Conducting regular risk assessments of a facility's physical resources	38	84.4%
Identifying critical areas within a facility for implementing physical safeguards (such as areas containing system hardware or software)	38	84.4%
Securely disposing of data after established archiving or retention periods have passed	38	84.4%
Regularly reviewing the list of persons with physical access to SNAP PII	36	80.0%
Periodically reviewing physical safeguards for effectiveness	35	77.8%
Assessing risk among supporting services (e.g., electrical power); backup media; and other elements required for system operations	34	75.6%
Implementing facility-wide security measures on the basis of the level of risk to physical resources	34	75.6%
Periodically reviewing reports and documents that can be printed with PII	26	57.8%
Others (e.g., identifying critical areas and conducting regular onsite)[a]	1	2.2%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a] One respondent selected the "Others" option and provided the following other safeguarding measure: identifying critical areas and conducting regular onsite.
Source: SNAP PII State Agency Survey, question 6.1.

2.2 Are appropriate role permissions established to limit PII access to authorized individuals only? If so, what are they?

Table 2. Type of Role Permissions Established to Limit Access to PII Data

Type of Role Permissions	Frequency	Percentage
Staff need approval to modify or edit participant data	41	93.2%
Staff need approval to view participant data	37	84.1%
Staff have access to participant data on an as needed basis, with supervisor approval	31	70.5%
Others (e.g., confidential cases are worker and supervisor specific)a	2	4.5%
Total number of respondents	**44**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Two respondents selected the "Others" option, they provided the following other type of role permissions: confidential cases are worker and supervisor specific; information security policies and standards.
Source: SNAP PII State Agency Survey, question 3.2.

2.3 Does the State allow remote access to systems containing PII? If so, what is the process?

Table 3. SA's Policies Regarding Remote Access to Systems Containing PII

Remote Access Policy	Frequency	Percentage
Remote access to systems containing PII		
Employees can use remote access but only when using authorized agency equipment	32	69.6%
Employees can use remote access when using authorized agency equipment or personal devices	13	28.3%
No remote access allowed to access to systems containing PII	1	2.2%
Total number of respondents	**46**	**100.0%**
Procedures implemented for providing employees with remote access to PII		
Establishing policies on usage restrictions, user application and approval, and implementation guidance for each approved method of remote access	42	95.5%
Enforcing technical requirements for remote access prior to authorizing connections	38	86.4%
Regularly reviewing the list of approved users with remote access and monitoring for unauthorized remote access	37	84.1%
Others (e.g., Multi-Factor Authentication; SA conducts annual user audits of all users)a	2	4.5%
Don't know/unsure	1	2.3%
Total number of respondents	**44**	**100.0%**

Notes: Survey question 4.5 allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Two respondents selected the "Others" option, they provided the following other procedures: Multi-Factor Authentication; SA conducts annual user audits of all users.
Source: SNAP PII State Agency Survey, questions 4.4 and 4.5.

2.4 Is masking used in PII data entry, particularly for SSNs?

Table 4. Masking Social Security Numbers During Data Entry

Masking of Social Security Numbers	Frequency	Percentage
Statewide SNAP eligibility system masks SSNs during data entry	4	9.1%
Statewide SNAP eligibility system does not mask SSNs during data entry	37	84.1%
Don't know/unsure	3	6.8%
Total number of respondents	**44**	**100.0%**

Source: SNAP PII State Agency Survey, questions 5.4.

2.5 Is there a time-out function used on application screens that contain PII? If so, what is the time limit for the time-out? What policy or guidance covers time-out functions?

Table 5. Time-out Function Used on Application Screens that Contain PII

Time-out Function Polices	Frequency	Percentage
SA's require time-out functions		
Time-out function is used on caseworker eligibility system screens that contain PII	43	95.6%
Time-out function is not used on caseworker eligibility system screens that contain PII	1	2.2%
Don't know/unsure	1	2.2%
Total number of respondents	**45**	**100.0%**
Time limit for time-out		
Average number (in minutes)	19.5	
Median number (in minutes)	15	
Minimum number (in minutes)	3	
Maximum number (in minutes)	120	
Total number of respondents	**36**	

Source: SNAP PII State Agency Survey, questions 5.11 and 5.12.

2.6 Are encryption methods used for transmitting and storing PII? If so, what are the methods in place?

Table 6. Encryption Methods Used for Transmitting and Storing PII Data

Type of Encryption Methods	Frequency	Percentage
Encryption methods used for transmitting PII data		
Use software-based encryption only	17	38.6%
Use hardware-based encryption only	1	2.3%
Use both software and hardware-based encryption	17	38.6%
Does not currently use encryption methods when transmitting PII data	2	4.5%
Don't know/unsure	7	15.9%
Total number of respondents	**44**	**100.0%**
Encryption methods used for storing PII data		
Use software-based encryption only	8	17.8%
Use hardware-based encryption only	3	6.7%
Use both software and hardware-based encryption	26	57.8%
Does not currently use encryption methods for data that are stored or at rest	2	4.4%
Don't know/unsure	6	13.3%
Total number of respondents	**45**	**100.0%**

Source: SNAP PII State Agency Survey, questions 6.2 and 7.4.

Study Objective 3: Describe how States currently safeguard participant PII

3.1 What vulnerabilities and threats to privacy have States encountered?

Table 7. SA's Rating of Internal Vulnerabilities and External Threats They Have Encountered

Types of Internal Vulnerabilities and External Threats	Number of Responses	Ratings			
		Often/ Very Often	Sometimes	Never/ Rarely	Don't Known/Unsure
Types of Internal Vulnerabilities					
Improper storage or disposal of physical materials that contain PII	46	2.2%	13.0%	78.3%	6.5%
Improperly secured systems with access to PII	46	0.0%	2.2%	93.5%	4.3%
Improperly secured mobile devices with access to PII	46	0.0%	2.2%	89.1%	8.7%
Unauthorized use of system resources by SA or county employees to access PII	46	2.2%	10.9%	82.6%	4.3%
Unauthorized disclosure of PII data by employees or a trusted partner	45	0.0%	2.2%	88.9%	8.9%
Failures or decreases in the reliability of hardware	45	0.0%	4.4%	88.9%	6.7%
Failures or decreases in the reliability of software	46	4.3%	6.5%	82.6%	6.5%
Types of External Threats					
Denial of service attacks[a]	46	4.3%	8.7%	76.1%	10.9%
Phishing, spoofing, or pharming[b]	46	10.9%	21.7%	63.0%	4.3%
Introduction of malicious code (such as viruses, spyware, or malware)	46	2.2%	6.5%	89.1%	2.2%

Notes: [a]An external attack that attempts to make computer resources, such as a website or web service, unavailable to users
[b]Methods commonly used by cyber criminals to exploit individuals and gain access to private information. These methods consist of sending a malicious email that is disguised as an email from a legitimate, trustworthy source (i.e., phishing); impersonating another individual or organization (i.e., spoofing); or creating a malicious website that resembles a legitimate website (i.e., pharming).
Source: SNAP PII State Agency Survey, question 4.1.

3.2 When States perform data matches of State SNAP administrative data with other administrative data, what data files do States perform matches with? What PII is used for linking the files? How do States protect confidentiality in files produced by data matching? How does PII and confidentiality protection vary among different data matches?

Table 8a. Data Sources that SAs Match SNAP Applicant and Recipient Data

Data Sources	Frequency	Percentage
National data sources		
National Directory of New Hires (NDNH)	46	100.0%
Electronic Disqualified Recipient System (eDRS)	44	95.7%
Income and Eligibility Verification System (IEVS)	44	95.7%
Social Security Administration Death Master File	42	91.3%
State Data Exchange (SDX)	42	91.3%
Beneficiary Data Exchange (BENDEX)	41	89.1%
Prisoner Verification System	40	87.0%
Public Assistance Reporting Information System (PARIS)	38	82.6%
Internal Revenue Service	27	58.7%
Veterans Administration	15	32.6%
Others (e.g., The Work Number, softeon, APPRISS; TALX; SOLQ, QC)[a]	7	15.2%
Total number of respondents	**46**	**100.0%**
State data sources		
State workforce data - unemployment insurance/state quarterly wage information/State employee information	45	97.8%
State child support payments	41	89.1%
State new hire directory	36	78.3%
State death records	31	67.4%
State or local prison listings	27	58.7%
State Department of Motor Vehicles	24	52.2%
State birth record directory	21	45.7%
State lottery information	18	39.1%
State educational agencies	17	37.0%
State warrant management directory	7	15.2%
State parole directory	7	15.2%
State law enforcement agencies	4	8.7%
Others (e.g., State Based Exchange)[b]	2	4.3%
Total number of respondents	**46**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.

[a]Seven respondents selected the "Others" option, they provided the following other national data sources: The Work Number, softeon, APPRISS, TALX, SOLQ, QC, SOLQ_SVES, Fed CMS FDSH Data sharing hub, SAVE Systems Alien Verification Entitlements. [b]Two respondents selected the "Others" option, they provided the following other state data sources: State Based Exchange, Dept of Aging, Dept of Rehabilitation Services, Dept of Revenue, DHS Accounts Receivable. Percentages <100% reported for mandatory verification were found to be reporting errors from some respondents, and do not reflect noncompliance.

Source: SNAP PII State Agency Survey, question 1.6.

Table 8b. Types of Data that are Commonly Used to Perform Data Match

Types of Data	Frequency	Percentage
Social Security Number	40	88.9%
Applicant/recipient name	39	86.7%
Applicant/recipient date of birth	38	84.4%
Case number	15	33.3%
Another unique identifier (e.g., PID Number; SNAP client ID)[a]	15	33.3%
Other data (e.g., combinations of DOB, first/middle/last name, and address)[b]	6	13.3%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
A matching technique that is typically applied to records that cannot be exactly matched using unique identifiers. This approach compares several variable values between two records and then assigns a weighted probability on the likelihood of a match.
[a]15 respondents selected the "Another unique identifier" option, they provided the following other identifiers: PID Number, Kansas has a Master Person Index that cross references multiple different IDs, Master Customer Index (MCI), SNAP client ID, Recipient ID, DCN, gender, address, city/state, Primary Master Index (PMI), Case ID, Person ID, CNDS ID, Unique Person Identification Number issued by our Eligibility System
[b]Six respondents selected the "Other data" option, they provided the following other data: first name; last name; gender; combinations of DOB, first/middle/last name, and address; combinations of name, DOB, and gender.
Source: SNAP PII State Agency Survey, question 1.9.

Table 8c. Frequency of Data Sharing Agreements

If SAs have Data Agreements	Frequency	Percentage
Yes, have data-sharing agreements with each of the agencies your SA shares data with	42	91.3%
No, have data-sharing agreements with each of the agencies your SA shares data with	4	8.7%
Total number of respondents	**46**	**100.0%**

Frequency of Data Sharing Agreements	Frequency	Percentage
When the data-sharing agreement is renewed or there is a change in the data sharing processes used by one of the agencies	28	68.3%
Other (e.g., 5 year agreements with annual monitoring; as required by the specific agreement)	9	22.0%
Once a year	8	19.5%
Don't know/unsure	4	9.8%
Every 6 months	0	0.0%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Findings about how often data-sharing agreements updated are based on the responses from 41 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Nine respondents selected the "Others" option, they provided the following other answers: 5 year agreements with annual monitoring; sharing agreements usually specify within the agreement itself the term of the agreement, a typical agreement is usually a year to five years in duration; the frequency of updates and modifications to data-sharing agreements are often project specific; dependent on the MOU/sharing agreement; as required by the specific agreement; every 5 years; etc.
Source: SNAP PII State Agency Survey, questions 1.7 and 1.8.

Table 9. SA Procedure to Responding to Law Enforcement Requests for PII

PII Data Sharing Procedures	Frequency	Percentage
SNAP PII is shared after law enforcement agencies provide the name of a SNAP recipient	0	0.0%
SNAP PII must be shared with law enforcement agencies if the recipient is a fleeing felon and the law enforcement agency provides a written request and the name of the SNAP recipient	12	27.3%
SNAP PII is shared after law enforcement agencies provide other information	9	20.5%
We do not share data with law enforcement (unless directed to do so via a court order)	18	40.9%
Don't know/unsure	5	11.4%
Total number of respondents	**44**	**100.0%**

Notes: The frequency of the first option in the table is 0, it is not displayed in Exhibit 9.
Source: SNAP PII State Agency Survey, question 7.5.

3.4 Do States follow the Federal Information Security Management Act (FISMA) or NIST guidelines?

Table 10. Federal and State Policy Guidelines for SAs

Types of Guideline	Frequency	Percentage
Federal SNAP regulations	36	83.7%
National Institute of Standards and Technology (NIST)[b] Guidelines	33	76.7%
The Health Insurance Portability and Accountability Act (HIPAA)[c]	32	74.4%
State SNAP laws and regulations	31	72.1%
Federal Information Security Management Act (FISMA)[a]	17	39.5%
Others (e.g., CMS Regulations MARSe 2.0)[d]	9	20.9%
Total number of respondents	**43**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]FISMA is federal legislation that provides a comprehensive framework for protecting government information, operations, and assets against man-made and natural threats.
[b]NIST is responsible for developing information technology (IT) security standards and guidelines for the Federal Government. Pertinent examples include the Guide to Protecting Confidentiality of PII and the minimum security requirements for federal information and information systems.

Table 11c. Who Provides PII Training for Staff

Training Providers	Frequency	Percentage
SNAP SA	32	71.1%
Other agency in the State	17	37.8%
Others (e.g., state agency security liaison)[a]	10	22.2%
Commercial off the shelf training provider	3	6.7%
Contractor for eligibility system	2	4.4%
Total number of respondents	**45**	**100.0%**

[c]HIPAA is a federal legislation that provides data privacy and security provisions for safeguarding medical information.
[d]Nine respondents selected the "Others" option, they provided the following other guidelines: Center of Medicare and Medicaid Services (CMS) Regulations MARSe 2.0, NITC, Texas Administrative Code (TAC) Chapter 202, Texas Government Code Chapter 2054, Social Security Administration, CDC, Texas Business and Commerce Code, IRS, NIST.
Source: SNAP PII State Agency Survey, question 2.2.

3.5 What is the training process to ensure personnel understand their responsibilities in protecting PII?

Table 11a.1 Staff Who Have Direct Access to SNAP PII

Type of Staff	Frequency	Percentage
Program integrity/quality control staff	43	97.7%
Clerical/administrative workers	39	88.6%
SNAP data analysts	39	88.6%
Staff from another SA (such as Medicaid, TANF, Low Income Home Energy Assistance Program)	36	81.8%
Other (e.g., Contractor Staff; IT, Business Analysts)	11	25.0%
Total Number of Respondents	**44**	**100.0%**

Notes: Findings about staff having direct access to SNAP PII are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100. 11 respondents selected the "Staff from other agencies in the State" option, they provided the following other answers: Contractor Staff; IT, Business Analysts (BA); Tribal partners, Hospitals, Comagine Health, Conduent; Eligibility System Help Desk staff; E&T contractors, childcare eligibility specialists; etc.
Source: SNAP PII State Agency Survey, question 3.1.

Table 11a.2 Staff Who Have Direct Access to SNAP PII

Type of Staff	Frequency	Percentage
Staff need approval to modify or edit participant data	41	93.2%
Staff need approval to view participant data	37	84.1%
Staff have access to participant data on an as needed basis, with supervisor approval	31	70.5%
Other type of role permissions established to limit access to PII data	2	4.5%
Total number of respondents	**44**	**100.0%**

Notes: Findings about staff having direct access to SNAP PII are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100. 11 respondents selected the "Staff from other agencies in the State" option, they provided the following other answers: Contractor Staff; IT, Business Analysts (BA); Tribal partners, Hospitals, Comagine Health, Conduent; Eligibility System Help Desk staff; E&T contractors, child care eligibility specialists; etc.
Source: SNAP PII State Agency Survey, question 3.2.

Table 11a.3 Staff by Type that Receive Training on PII

Type of Staff	Frequency	Percentage
Managers	45	97.8%
Line staff who process applications or recertifications in person, online, or as part of a telephone center	45	97.8%
IT/IS professionals	45	97.8%
Members of the Incident Response Team	38	82.6%
Staff of EBT contractors	34	73.9%
Other staff (e.g., all staff)[a]	12	26.1%
Total number of respondents	**46**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]12 respondents selected the "Other staff" option, they provided the following other staff: all staff, contractor staff, anyone with access to the EIS legacy system, employment and training vendors, anyone who has access to the information receives training, employment and training specialists.
Source: SNAP PII State Agency Survey, question 3.3.

Table 11b. Frequency of Training the Majority of Staff with Access to PII

Frequency of Training	Frequency	Percentage
Annually	44	95.7%
On hire	38	82.6%
Whenever major systems changes are implemented	19	41.3%
Others (e.g., quarterly; not often; as needed)[a]	4	8.7%
Total number of respondents	**46**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Four respondents selected the "Other" option, they provided the following other frequency: quarterly; not often; as needed.
Source: SNAP PII State Agency Survey, question 3.5.

Table 11c. Who Provides PII Training for Staff

Training Providers	Frequency	Percentage
SNAP SA	32	71.1%
Other agency in the State	17	37.8%
Others (e.g., state agency security liaison)[a]	10	22.2%
Commercial off the shelf training provider	3	6.7%
Contractor for eligibility system	2	4.4%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]10 respondents selected the "Others" option, they provided the following other training providers: state agency security liaison, agency's Information Security Office, application development vendor, HHS information security awareness and training, HHS privacy training, department's Information Security Office.
Source: SNAP PII State Agency Survey, question 3.6.

Table 11d. Mode of Providing PII Training

Training Mode	Frequency	Percentage
Self-paced online trainings	40	88.9%
Online training in a group setting	18	40.0%
Webinar	14	31.1%
In-person training in a group setting	13	28.9%
Others (e.g., in-person training is available in a group or individual setting upon request)[a]	3	6.7%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Three respondents selected the "Others" option, they provided the following other training modes: Work in Progress; in-person training is available in a group or individual setting upon request; not in person since COVID.
Source: SNAP PII State Agency Survey, question 3.7.

Table 11e. Major Components of the PII Training

Components	Frequency	Percentage
Procedures for reporting violations to management	43	97.7%
Procedures when PII has been inappropriately disclosed	43	97.7%
Protecting accidental disclosure of PII on screens or papers in SNAP office	43	97.7%
What is PII, and why does it need to be protected?	43	97.7%
Penalties for not protecting PII	42	95.5%
Protection of PII during data analysis, transmission, and storage	39	88.6%
Updates on efforts to protect PII	38	86.4%
Limits on use of mobile devices to safely access PII	37	84.1%
Using matched data and resolving any issues with matching results	26	59.1%
Protection of PII used to issue EBT cards	25	56.8%
Others (e.g., insider threat awareness)[a]	3	6.8%
Total number of respondents	**44**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Three respondents selected the "Others" option, they provided the following other components: insider threat awareness, telework/remote checklist.
Source: SNAP PII State Agency Survey, question 3.8.

3.6 Which States have had data breaches? What has been the response?

Table 12. SA's Plans/Policies for Responding to Security Incidents

SA's Plans/Policies	Number of Responses	Yes/No		
		Yes	No	Don't know/unsure
SA has specific policy for responding to security incidents	45	97.8%	2.2%	0.0%
SA has plans that include required steps for incident response	45	86.7%	6.7%	6.7%
SA has had data breaches	43	20.9%	55.8%	23.3%

Source: SNAP PII State Agency Survey, questions 5.13, 5.14, and 5.15.

3.7 How secure is the transmission of online application data? How is the confidentiality of paper applications secured?

Table 13a. Entities SAs Share or Transfer PII Data With

Entities	Number of Responses	Yes/No		
		Yes	No	Don't Know/ Unsure
Federal entities	46	95.70%	4.30%	0.00%
EBT contractors	46	95.70%	0.00%	4.30%
Other agencies in the State	46	93.50%	6.50%	0.00%
State education agencies or school districts	45	77.80%	11.10%	11.10%
Other entities (e.g., USDA/FNS Studies)[a]	6	66.70%	16.70%	16.70%
Research entities	46	54.30%	34.80%	10.90%
Law enforcement agencies	44	36.40%	50.00%	13.60%

Notes: [a]Six respondents selected the "Others" option, they provided the following other entities: tribal partners, hospitals, Comagine Health, Conduent, DOL, USDA/FNS studies, Internal Data Warehouse.
Source: SNAP PII State Agency Survey, question 7.1.

Table 13b. Methods of Transferring PII Data with Requesting Agencies

Data Transfer Methods	Frequency	Percentage
SFTP sites	38	84.4%
Direct access to the SNAP system (such as application-to-application access) for approved users	30	66.7%
Password encrypted files	24	53.3%
Direct email	7	15.6%
Fax	4	8.9%
Others (e.g., state drives)[a]	3	6.7%
Physical storage devices (CDs, USB drives, etc.) with requested information	2	4.4%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]Three respondents selected the "Others" option, they provided the following other methods: state drives, API interfaces using certification controls, DoIT's Mainframe MOVEit Secure FTP utility, encrypted PII provided via Sharepoint site to external auditors.
Source: SNAP PII State Agency Survey, question 7.2.

Table 13c. Methods of Entering Paper Applications into SA's Eligibility Systems

Data Entry Methods	Frequency	Percentage
County staff manually enter paper applications into eligibility system only	18	39.1%
County staff scan and upload paper applications into eligibility system only	4	8.7%
County staff manually enter, scan and upload paper applications into eligibility system	24	52.2%
Total number of respondents	**46**	**100.0%**

Source: SNAP PII State Agency Survey, question 5.6.

Table 13d. Methods of Storing Paper Applications While the Applications are Pending

Storage Methods	Frequency	Percentage
In a file cabinet in a locked room	24	53.3%
Others (e.g., scanned and stored in Electronic Case File)[a]	23	51.1%
In Caseworker's/Eligibility Counselor's locked drawer in the desk	16	35.6%
In buckets/baskets in an open office behind a restricted area	11	24.4%
On Caseworker's/Eligibility Counselor's desk	6	13.3%
Located with a designated staff member	3	6.7%
Total number of respondents	**45**	**100.0%**

Notes: This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
[a]23 respondents selected the "Others" option, the provided the following methods: scanned and stored in Electronic Case File (ECF); scanned into the system and shredded; scanned document imaging system and then destroyed; electronically stored; destroyed after it is data entered into the eligibility system, etc.
Source: SNAP PII State Agency Survey, question 5.7.

3.8 How do safeguarding practices differ between States with county-administered SNAP versus those with Statewide administration?

Table 14a. SA's Safeguarding Practices that are likely to be upgraded, by Type of Administration

Safeguarding Practices	Number of Responses	Type of Administration	
		State Administered	County Administered
Personnel Policies and Procedures			
Using role-based security levels to provide data access	43	11.6%	14.3%
Delivering regular security training and education	43	14.0%	14.3%
Others (e.g., policy training and quizzes currently begin developed)[a]	25	16.0%	0.0%
Security Policies and Procedures			
Security PII across hardware systems	43	19.4%	28.6%
Security PII across software systems	43	19.4%	28.6%
Security PII across network systems	43	19.4%	28.6%
Regularly assessing risk and vulnerabilities	43	22.2%	28.6%
Regularly performing security testing	43	16.7%	42.9%
Developing emergency preparedness and contigency plans	42	25.7%	28.6%
Others (e.g., ID badge security standards)[b]	17	6.7%	0.0%
Program Operations			
Masking PII	43	19.4%	57.1%
Implementing time-out features on computer screens	41	8.8%	14.3%
Safeguarding PII during delivery of SNAP benefits via EBT	41	8.8%	42.9%
Matching PII to other data sources for eligibility determination	41	11.8%	28.6%
Matching PII to other data sources for program integrity purposes	42	11.4%	14.3%
Securely destroying PII data that are no longer used	42	17.1%	28.6%
Other program operations	11	0.0%	0.0%

Notes: The last option "other program operations" in Table 14a is not likely to be upgraded, so it is not displayed in Exhibit 14a_3.
[a]25 respondents selected the "Others" option, and four of them provided the following other personnel policies and procedures: policy training and quizzes currently begin developed; working towards annual review and updates; we are drafting Background Investigation Policy and Procedure (PS-1) documents.
[b]17 respondent selected the "Others" option, and one of them provided the following other security policies and procedures: ID badge security standards.
Source: SNAP PII State Agency Survey, question 2.5.

Table 14b. SA's Self-Assessment of the Extent of Their Security Plan Meet and/or Exceed Safeguarding Requirements for Personnel, by Type of Administration

		State Administered			County Administered		
SA's Security Plan	**Total Number of Responses**	**SAs meet requirements, with room for improvement**	**SAs meet requirements**	**SAs are especially successful at meeting requirements**	**SAs meet requirements, with room for improvement**	**SAs meet requirements**	**SAs are especially successful at meeting requirements**
Ensuring Staff Working with PII have Met the Requisite Security Requirements and are Approved to Access Data	46	7.9%	63.2%	28.9%	12.5%	75.0%	12.5%
Conducting Personnel Background and Check	44	19.4%	52.8%	27.8%	0.0%	62.5%	37.5%
Using Role-Based Security Levels to Provide Data Access	47	2.6%	48.7%	48.7%	0.0%	50.0%	50.0%
Delivering Regular IT Security Training and Education	46	7.9%	52.6%	39.5%	0.0%	37.5%	62.5%

Source: SNAP PII State Agency Survey, question 3.9.

Table 14c. Extent SA's Security Plan Meet and/or Exceed Safeguarding Requirements, by Type of Administration

SA's Security Plan	Total Number of Responses	State Administered			County Administered		
		SAs meet requirements, with room for improvement	SAs meet requirements	SAs are especially successful at meeting requirements	SAs meet requirements, with room for improvement	SAs meet requirements	SAs are especially successful at meeting requirements
Hardware-Specific Controls	42	17.6%	64.7%	17.6%	75.0%	12.5%	12.5%
Software-Specific Controls	42	20.6%	64.7%	14.7%	62.5%	12.5%	25.0%
Network-Specific Controls	42	20.6%	64.7%	14.7%	62.5%	25.0%	12.5%
Regularly Assessing Risk and Vulnerabilities	42	29.4%	52.9%	17.6%	37.5%	50.0%	12.5%
Regularly Performing Security Testing	42	32.4%	52.9%	14.7%	37.5%	37.5%	25.0%
Developing Emergency Preparedness and Contingency Plans	41	36.4%	51.5%	12.1%	62.5%	12.5%	25.0%

Source: SNAP PII State Agency Survey, question 4.8.

Table 14d. Extent SA's Security Plan Meet and/or Exceed Safeguarding Requirements, by Type of Administration

SA's Security Plan	Total Number of Responses	State Administered			County Administered		
		SAs meet requirements, with room for improvement	SAs meet requirements	SAs are especially successful at meeting requirements	SAs meet requirements, with room for improvement	SAs meet requirements	SAs are especially successful at meeting requirements
Masking PII During Data Entry	40	47.1%	41.2%	11.8%	66.7%	33.3%	0.0%
Matching PII to Other Data Sources for Program Integrity Purposes	45	8.1%	67.6%	24.3%	0.0%	50.0%	50.0%
Implementing Time-Out Features	44	5.6%	66.7%	27.8%	0.0%	62.5%	37.5%
Secure Delivery of SNAP Benefits via EBT	46	5.3%	65.8%	28.9%	0.0%	62.5%	37.5%
Matching PII to Other Data Sources for Eligibility Purposes	45	2.7%	70.3%	27.0%	0.0%	50.0%	50.0%

Study Objective 4: Examine the consistency of safeguarding practices across States

4.1 What are the safeguarding practices that vary the most among States?

4.2 What are the safeguarding practices that are most often practiced within States?

Table 15. Safeguarding Practices by State Agency

State Agency	Personnel Policies and Procedures			Security Policies and Procedures							Program Operations						
	Using Role-Based Security Levels to Provide Data Access	Delivering Regular Security Training and Education	Other Personnel Policies and Procedures	Securing PII across hardware systems	Securing PII across software systems	Securing PII across network systems	Regularly assessing risk and vulnerabilities	Regularly performing security testing	Developing emergency preparedness and contingency plans	Other security policies and procedures	Masking PII	Implementing time-out features on computer screens	Safeguarding PII during delivery of SNAP benefits via EBT	Matching PII to other data sources for eligibility determination	Matching PII to other data sources for program integrity purposes	Securely destroying PII data that are no longer used	Other program operations
Alaska																	
Alabama	•	•													•	•	
Arkansas	•	•		•		•		•	•	•	•	•		•	•	•	
Arizona	•	•				•	•	•	•	•	•				•	•	•
Connecticut	•	•		•		•		•	•	•	•	•			•	•	•
District of Columbia																	
Delaware	•	•		•		•	•	•	•	•				•		•	•
Florida		•	•	•		•	•	•	•	•	•	•	•	•	•		•
Georgia	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Guam																	
Hawaii	•			•		•	•	•	•	•	•	•		•	•	•	•

State Agency	Personnel Policies and Procedures			Security Policies and Procedures							Program Operations						
	Using Role-Based Security Levels to Provide Data Access	Delivering Regular Security Training and Education	Other Personnel Policies and Procedures	Securing PII across hardware systems	Securing PII across software systems	Securing PII across network systems	Regularly assessing risk and vulnerabilities	Regularly performing security testing	Developing emergency preparedness and contingency plans	Other security policies and procedures	Masking PII	Implementing time-out features on computer screens	Safeguarding PII during delivery of SNAP benefits via EBT	Matching PII to other data sources for eligibility determination	Matching PII to other data sources for program integrity purposes	Securely destroying PII data that are no longer used	Other program operations
Iowa	•	•					•				•	•			•	•	•
Idaho																	
Illinois	•	•		•													
Indiana	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Kansas	•	•	•	•		•	•	•	•	•	•	•			•	•	•
Kentucky	•	•	•	•		•	•	•	•	•	•	•		•	•	•	•
Louisiana	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Massachusetts	•	•					•								•	•	•
Maryland																	
Maine	•	•		•		•	•	•	•	•	•	•			•		•
Michigan	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Missouri	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Mississippi																	
Montana	•	•				•	•	•	•	•	•			•	•	•	
Nebraska	•	•		•		•	•	•	•	•	•	•		•	•	•	•
New Hampshire	•	•	•	•		•	•	•	•	•	•	•	•		•	•	•
New Mexico	•	•	•	•		•	•	•	•	•	•	•		•	•	•	•
Nevada	•	•		•		•	•	•	•			•			•	•	•
Oklahoma	•	•		•		•	•	•	•	•	•	•			•	•	•
Oregon																	
Pennsylvania	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Rhode Island	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

State Agency	Personnel Policies and Procedures			Security Policies and Procedures							Program Operations						
	Using Role-Based Security Levels to Provide Data Access	Delivering Regular Security Training and Education	Other Personnel Policies and Procedures	Securing PII across hardware systems	Securing PII across software systems	Securing PII across network systems	Regularly assessing risk and vulnerabilities	Regularly performing security testing	Developing emergency preparedness and contingency plans	Other security policies and procedures	Masking PII	Implementing time-out features on computer screens	Safeguarding PII during delivery of SNAP benefits via EBT	Matching PII to other data sources for eligibility determination	Matching PII to other data sources for program integrity purposes	Securely destroying PII data that are no longer used	Other program operations
South Carolina																	
South Dakota	•	•	•	•		•	•	•	•	•	•	•		•	•	•	•
Tennessee																	
Texas	•	•		•		•	•	•	•	•	•	•			•	•	•
Utah	•	•		•		•	•	•	•	•	•				•	•	•
Virgin Islands																	
Vermont																	
Washington																	
West Virginia	•	•	•	•		•	•	•	•	•	•	•	•	•		•	
Wyoming	•	•		•		•	•	•	•	•	•	•			•	•	•
California																	
Colorado	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Minnesota																	
North Carolina	•	•		•		•	•	•	•	•	•	•		•	•	•	•
North Dakota	•	•		•		•		•	•	•		•			•		
New Jersey	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•
New York																	
Ohio	•	•		•		•	•	•	•	•	•	•		•	•	•	•
Virginia																	
Wisconsin	•	•					•								•		•

Table 15. Safeguarding Practices by SAs

Safeguarding Practices	Frequency	Percentage
Personnel Policies and Procedures		
Using Role-Based Security Levels to Provide Data Access	36	76.6%
Delivering Regular Security Training and Education	36	76.6%
Other Personnel Policies and Procedures	9	19.1%
Security Policies and Procedures		
Securing PII across hardware systems	32	68.1%
Securing PII across software systems	32	68.1%
Securing PII across network systems	32	68.1%
Regularly assessing risk and vulnerabilities	31	66.0%
Regularly performing security testing	30	63.8%
Developing emergency preparedness and contingency plans	29	61.7%
Other security policies and procedures	5	10.6%
Program Operations		
Masking PII	20	42.6%
Implementing time-out features on computer screens	34	72.3%
Safeguarding PII during delivery of SNAP benefits via EBT	32	68.1%
Matching PII to other data sources for program integrity purposes	32	68.1%
Matching PII to other data sources for eligibility determination	31	66.0%
Securely destroying PII data that are no longer used	31	66.0%
Other program operations	2	4.3%

Notes: Findings about How agencies structured its approach for using systems security professionals are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. Two respondents selected the "Others" option, they provided the following other approaches: We leverage Accenture system security professionals; Our agency utilizes a combination of system security professionals located within our agency and systems security professionals located within another state agency.
Source: SNAP PII State Agency Survey, question 2.5.

4.3 In which areas are the safeguarding practices of States most in need of improvement?

Table 16a. SA's Self-Assessment of Safeguarding Practices Most in Need of Improvement

Safeguarding Practices	Frequency	Percentage
Personnel Policies and Procedures		
Conducting personnel background checks	44	15.9%
Ensuring that staff working with PII have met the requisite security requirements and are approved to access data	46	8.7%
Delivering regular security training and education	46	6.5%
Using role-based security levels to provide data access	47	2.1%
Security Policies and Procedures		
Developing emergency preparedness and contingency plans	41	34.1%
Regularly performing security testing	42	31.0%
Regularly assessing risk and vulnerabilities	42	26.2%
Security PII across software systems	42	21.4%
Security PII across network systems	42	19.0%
Security PII across hardware systems	42	16.7%
Program Operations		
Masking PII during data entry	40	50.0%
Matching PII to other data sources for program integrity purposes	45	6.7%
Implementing time-out features on eligibility system screens containing PII	44	4.5%
Secure delivery of SNAP benefits via EBT	46	4.3%
Matching PII to other data sources for eligibility determination	45	2.2%

Source: SNAP PII State Agency Survey, questions 3.9, 4.8, 5.19.

Table 16b. SA's Rating of Safeguarding Practices

Safeguarding Practices	Number of Responses	Ratings					
		Very Satisfied	Satisfied	Neither Satisfied nor Dissatisfied	Dissatisfied	Very Dissatisfied	Don't Know/Unsure
Personnel Policies and Procedures	44	36.4%	50.0%	6.8%	4.5%	0.0%	2.3%
Security Policies and Procedures	44	34.1%	47.7%	11.4%	0.0%	2.3%	4.5%
Program Operations	44	29.5%	54.5%	13.6%	0.0%	0.0%	2.3%

Source: SNAP PII State Agency Survey, question 8.1.

Additional Tables

Section 1: SA Systems in Context

Table A.1. Agency's Approach for Using Systems Security Professionals

	Frequency	Percentage
Developing emergency preparedness and contingency plans	8	18.2%
Regularly performing security testing	12	27.3%
Regularly assessing risk and vulnerabilities	22	50.0%
Security PII across software systems	2	4.5%
Security PII across network systems	44	100.0%
Security PII across hardware systems	8	18.2%

Notes: Findings about How agencies structured its approach for using systems security professionals are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. Two respondents selected the "Others" option, they provided the following other approaches: We leverage Accenture system security professionals; Our agency utilizes a combination of system security professionals located within our agency and systems security professionals located within another state agency.
Source: SNAP PII State Agency Survey, question 1.1.

Table A.2. Staff Members Responsible for Protecting SNAP PII

Staff Members	Frequency	Percentage
SNAP IT Director	27	60.0%
Lead Applications Developer	31	68.9%
Systems cybersecurity specialists within the agency that administers the SNAP program (often along with other programs)	35	77.8%
Data analysts	30	66.7%
IT Contractor staff	30	66.7%
Staff from a central state agency (such as the State CIO or CISO Office)	39	86.7%
Other (e.g., all staff, eligibility staff, GRC Manager)	11	24.4%
Total number of respondents	**45**	**100.0%**

Notes: Findings about staff member(s) that are responsible for protecting SNAP PII are based on the responses from 45 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100. 11 respondents selected the "Others" option, they provided the following other staff members: all staff, eligibility staff, GRC Manager, Contractors such as FIS, DHS General Counsel Privacy Officer.
Source: SNAP PII State Agency Survey, question 1.2.

Table A.3. Time Period When Main SNAP Eligibility was Implemented

Implementation	Frequency	Percentage
Before 1990	12	26.7%
1990–1999	8	17.8%
2000–2009	7	15.6%
2010–2019	16	35.6%
2020–2021	2	4.4%
Total number of respondents	**45**	**100.0%**

Notes: Findings about time period the main SNAP eligibility system implemented are based on the responses from 45 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 1.3.

Table A.4. SNAP Eligibility to Be A Legacy System

Safeguarding Practices	Number of Responses	Percentage
Yes, consider your main SNAP eligibility system to be a legacy system	21	46.7%
No, does not consider your main SNAP eligibility system to be a legacy system	24	53.3%
Total number of respondents	**45**	**100.0%**

Notes: Findings about if SAs considering their main SNAP eligibility system to be a legacy system are based on the responses from 45 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 1.4.

Table A.5 SNAP Eligibility Integrated with Eligibility of Other Programs

Safeguarding Practices	Number of Responses	Percentage
Women, Infants, and Children (WIC)	3	6.7%
The state's child welfare system	9	20.0%
Other (e.g., Parts of child welfare system; Aid to the Aged, Blind, and Disabled (AABD))	14	31.1%
Low Income Home Energy Assistance Program (LIHEAP)	16	35.6%
The state's child care program	21	46.7%
Medicaid	36	80.0%
Temporary Assistance for Needy Families (TANF)	44	97.8%
Total number of respondents	**45**	**100.0%**

Notes: Findings about programs SNAP eligibility system integrated with are based on the responses from 45 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 1.5.

Table A.6 Interaction of County Eligibility System with SA's Statewide Eligibility System

Eligibility System Interactions	Frequency	Percentage
None of the county offices	5	62.5%
A minority of county offices	1	12.5%
A majority of county offices	0	0.0%
All county offices	2	25.0%
Total number of respondents	**8**	**100.0%**

Notes: Findings about extent county offices developed their own SNAP-eligibility systems are based on the responses from 8 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 1.10.

Section 2: System Security Plan Information

Table A.7 Source for SA's Security Plan to Protect PII

Sources	Frequency	Percentage
Standards from central State Information Security (IS)/IT agency	38	90.5%
Other (e.g., CMS MARSe 2.0; NIST; IRS Pub1075)	18	42.9%
Standards from systems contractor	6	14.3%
Total number of respondents	**42**	**100.0%**

Notes: Findings about sources SA's system security plan for protecting PII based on are based on the responses from 42 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
18 respondents selected the "Others" option, they provided the following other sources: CMS MARSe 2.0; CMS MARS-E; HIPAA, NIST Guidelines, Texas Administrative Code (TAC) Chapter 202, Texas Government Code Chapter 2054, Social Security Administration; IRS, FNS; SA standards; etc.
Source: SNAP PII State Agency Survey, question 2.1.

Table A.8 Familiarity of Agency's Security Professionals with FNS Guidance on Protecting PII

Guidance	Number of Responses	Levels of Familiarity			
		Somewhat Familiar	Not Aware of this Resource	Very Familiar	Not Really Familiar
Privacy Act of 1974	42	35.7%	4.8%	57.1%	2.4%
FNS Handbook 901: The Advance Planning Document Process	40	37.5%	2.5%	47.5%	12.5%
7 CFR 274.5 – Record retention and forms security	40	27.5%	2.5%	67.5%	2.5%
7 CFR 274.8 – Functional and technical EBT system requirements	39	28.2%	0.0%	64.1%	7.7%
Other guidance provided by USDA, FNS State Systems Office	40	37.5%	5.0%	47.5%	10.0%
NIST Guide to Protecting Confidentiality of PII	42	21.4%	2.4%	69.0%	7.1%

Notes: Number of responses for each guidance varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.3.

Table A.9 Time Since SA's Last Security System Plan Update

Time Since Last Security System Plan Update	
Average number (in months)	11.5
Median number (in months)	7
Minimum number (in months)	1
Maximum number (in months)	48
Total number of respondents	**27**

Notes: Number of responses for time since last update is 27, Don't know/ Unsure = 13. it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.4.

Table A.10 Familiarity of Agency's Security Professionals with FNS Guidance on Protecting PII

Guidance	Frequency	Percentage
Staff from the State's Office of Information Technology	32	74.4%
SNAP IT staff or SNAP applications development staff	31	72.1%
SNAP policy staff	30	69.8%
SNAP Director	26	60.5%
The State's CISO or their staff	24	55.8%
The State's CIO or their staff	22	51.2%
Other SNAP program staff	17	39.5%
EBT contractors	16	37.2%
Contractors/vendors	13	30.2%
Staff from other agencies in the State (e.g., internal auditing staff; state enterprise office)	7	16.3%
Staff from county offices administering SNAP	3	7.0%
Not applicable. My SA has not updated the security plan for protecting SNAP PII	1	2.3%
Total number of respondents	**43**	**100.0%**

Notes: Findings about staff providing input on or are involved in updating the security plan are based on the responses from 43 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100. 7 respondents selected the "Staff from other agencies in the State" option, they provided the following other procedures: internal auditing staff; state enterprise office; the Department's Deputy Information Security Officer and Eligibility System's IT Manager; Agency ISO,Agency Compliance Office, RAPIDS contract staff; DHSS/DMS/IRM/ISO staff; etc.
Source: SNAP PII State Agency Survey, question 2.6.

Table A.11 Use of Plan of Action and Milestones (POA&M) by SAs

Plan of Action and Milestones	Frequency	Percentage
Yes, use a Plan of Action and Milestones (POA&M) or another similar risk planning tool	40	93.0%
No, do not use a Plan of Action and Milestones (POA&M) or another similar risk planning tool	1	2.3%
Don't know/unsure	2	4.7%
Total number of respondents	**43**	**100.0%**

Notes: Findings about if SA using a Plan of Action and Milestones (POA&M) or another similar risk planning tool are based on the responses from 43 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.7.

Table A.12 Challenges Faces by SAs in Understanding, Complying with, Testing or Validating or Updating its System Security Plan

Challenges	Number of Response	Extent			
		To a Great Extent	Somewhat	Very Little	Not at All
Understanding the system security plan	42	11.9%	14.3%	40.5%	33.3%
Complying with the system security plan	42	11.9%	19.0%	35.7%	33.3%
Testing or validating the system security plan	42	14.3%	19.0%	33.3%	33.3%
Updating the system security plan	41	12.2%	14.6%	43.9%	29.3%
Other	4	0.0%	0.0%	0.0%	100.0%

Notes: Number of responses for each challenge varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 2.8.

Section 3: Personnel Policies and Procedures

Table A.13 Methods Used by Agencies for Contractors

Methods	Frequency	Percentage
PII trainings	31	68.9%
Contractual agreements (such as a Memorandum of Understanding [MOU] or a Data Use Agreement [DUA]) that meet specific security standards	42	93.3%
Other (e.g., Business Use and Confidentiality Agreement and Information Security Requirements Contract Exhibit, and the DHHS Confidentiality Policy)	6	13.3%
Total number of respondents	**45**	**100.0%**

Notes: Findings about methods using to establish PII safeguarding requirements are based on the responses from 45 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 3.4.

Section 4: Security Policies and Procedures

Table A.14 Information Captured by SA's Audit Trails

Information	Frequency	Percentage
Successful and unsuccessful login attempts	45	100.0%
Timing of system startup and shutdown	42	93.3%
Date and time of any security events	42	93.3%
User actions to access files or applications	41	91.1%
Attempts to access data for which a worker does not have access/permissions	39	86.7%
The activities of system administrators and systems security staff	38	84.4%
Type of security event experienced and its success or failure	37	82.2%
Names of files or applications accessed during a security event	35	77.8%
Other (e.g., log in attempts and activities of system administrators)	3	6.7%
Total number of respondents	**45**	**100.0%**

Notes: Findings about information being captured within audit trails are based on the responses from 45 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 4.2.

Table A.15 Firewall Safeguards, Policies and Procedures Implemented by SAs

Firewall safeguards, policies, and procedures	Number of Respondents	Yes/No		
		Yes	No	Don't Know/Unsure
Use of a hardware-based firewall	44	97.7%	2.3%	0.0%
Use of a software-based firewall	44	90.9%	6.8%	2.3%
Maintaining audit records of all security-related events	44	95.5%	0.0%	4.5%
Limiting firewall access to network security analysts or other approved users	44	97.7%	0.0%	2.3%
Regularly reviewing the list of approved users with access to the firewall	44	84.1%	0.0%	15.9%
Timely installation of security-related updates, fixes, or modifications that have been tested and approved	44	93.2%	0.0%	6.8%
Other firewall safeguards, policies, and procedures	38	73.7%	0.0%	26.3%

Notes: Number of responses for each row varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 4.3.

Table A.16 Parties Used by SAs to Conduct Penetration Testing

Parties	Frequency	Percentage
A contractor or vendor	19	41.3%
SA's IT or security team	18	39.1%
Another agency in the State (e.g., Dept. of Enterprise Technology; the Office of Management and Enterprise Services)	9	19.6%
Not currently performed on systems containing the PII of SNAP applicants and participants	4	8.7%
Don't know/unsure	9	19.6%
Total number of respondents	**46**	**100.0%**

Notes: Findings about parties that being used to conduct penetration testing are based on the responses from 46 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100. Nine respondents selected the "Another agency in the State" option, they provided the following other procedures: Dept. of Enterprise Technology; the Office of Management and Enterprise Services; Governor's Office of Information Technology; EOTSS; Office of Information Technology; the Indiana Office of Technology.
Source: SNAP PII State Agency Survey, question 4.6.

Table A.17 Components Present Within SA's Disaster Recovery Plan to Protect PII During Disasters or Other Emergency Situation

Components	Number of Respondents	Yes/No		
		Yes	No	Don't Know/Unsure
It effectively details how the SA will recover and restore the system to normal operations	42	88.1%	7.1%	4.8%
It specifies a process for protecting PII from internal and external threats until the system is restored to normal operations	42	73.8%	9.5%	16.7%
It is effectively integrated into the SA's security plan	42	78.6%	11.9%	9.5%
It provides a process for training staff in their specific response to a disaster according to their roles	43	69.8%	14.0%	16.3%
It specifies a process for maintaining Local Area and Wide Area Networks	42	71.4%	16.7%	11.9%
It specifies a process for maintaining desktops and personal computers	42	69.0%	16.7%	14.3%
It specifies a process for maintaining SA websites	42	66.7%	9.5%	23.8%
It specifies a process for maintaining distributed and mainframe systems	42	83.3%	4.8%	11.9%
It specifies alternative physical locations for operations in the event that original facilities are unavailable	43	76.7%	4.7%	18.6%
It can be activated on its own and does not require that other contingency plans be activated first	42	54.8%	14.3%	31.0%

Notes: Number of responses for each row varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 4.7.

Section 5: SNAP Application and Recertification Processes

Table A.18 Methods Used by SA to Receive SNAP Applications and Recertifications

Methods	Number of Respondents	Yes	No
Interview with SNAP staff (either in person or on the phone)	46	97.8%	2.2%
Mailing or faxing physical applications to the SA	46	97.8%	2.2%
Interviews with non-SNAP staff who do eligibility determinations for multiple public assistance programs, such as SNAP, TANF, WIC, public housing assistance, child care, and employment training programs	45	48.9%	51.1%
Online initial application	46	89.1%	10.9%
Online recertifications	46	73.9%	26.1%
Mobile apps – initial application	45	26.7%	73.3%
Mobile apps – recertifications	45	17.8%	82.2%
Other (e.g., in person)	9	44.4%	55.6%

Notes: Number of responses for each method varies, it is reported in the table; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. Nine respondents selected the "Other" option, they provided the following other methods: in-person; the "mobile app" above is based on our mobile-browser compliant website - not a standalone app; Interim Reporting Forms (6 month reporting form) can be submitted online, telephone, or via mobile; Inner office mail, email, phone via outreach partner.
Source: SNAP PII State Agency Survey, question 5.1.

Table A.19 Methods Used by SAs to Conduct Interviews for SNAP Applications and Recertifications

Methods	Number of Respondents	Yes/No		
		Yes	No	Don't Know/Unsure
Telephone interviews with local office	23	100.0%	0.0%	0.0%
Face-to-face interviews	23	95.7%	4.3%	0.0%
Other (e.g., On-Demand telephone interviews; Telephone Interviews through Virtual Interview Center)	3	66.7%	33.3%	0.0%
Telephone interviews with call center	23	52.2%	47.8%	0.0%
Telephone interviews with interactive voice response	23	8.7%	87.0%	4.3%

Notes: Number of responses for each method varies, it is reported in the table; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. Three respondents selected the "Other" option, they provided the following other procedures: On-Demand telephone interviews; Telephone Interviews through Virtual Interview Center (VIC); SNAP Outreach providers.
Source: SNAP PII State Agency Survey, question 5.2.

Table A.20 Cases or Applications Uniquely Identified in the Eligibility System

Cases or applications	Frequency	Percentage
Assigned case numbers (i.e., a client ID number or another unique number)	43	93.5%
Social Security Number	29	63.0%
Head of household's name	28	60.9%
Head of household's date of birth	19	41.3%
Other (e.g., Program Case Number; Person number)	7	15.2%
Total number of respondents	**46**	**100.0%**

Notes: Findings about cases or applications uniquely identified are based on the responses from 46 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 5.3.

Table A.21 Methods Used to Safeguard PII Submitted by SNAP Applicants or Participants via Online Forms

Methods	Frequency	Percentage
Applicants/participants must enter a system- or user-generated password to access their accounts	38	90.5%
Warnings are displayed regarding the need for applicants/participants to protect their PII	24	57.1%
Time-out functions are used to automatically log out applicants/participants due to inactivity	37	88.1%
Applications and other forms are encrypted	18	42.9%
Other (e.g., No online forms; data is encrypted when stored)	5	11.9%
Total number of respondents	**42**	**100.0%**

Notes: Findings about methods using to safeguard PII are based on the responses from 42 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 5.5.

Table A.22 Handling of Denied Applications

Methods	Frequency	Percentage
Scanned to a document imaging system and then destroyed	30	65.2%
Kept for a specified period before destruction	6	13.0%
Other (e.g., destroy the application after 7 years)	6	13.0%
Don't know/unsure	3	6.5%
Never destroyed/stored securely	1	2.2%
Destroyed upon denial	0	0.0%
Total number of respondents	**46**	**100.0%**

Notes: Findings about ways to handle denied applications are based on the responses from 46 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket.
Source: SNAP PII State Agency Survey, question 5.8.

Table A.23 Methods Used by SNAP Staff to Determine Eligibility for SNAP Applications and Recertifications

Methods	Number of Respondents	Yes/No		
		Yes	No	Don't Know/Unsure
Client provides paper documents	46	97.8%	2.2%	0.0%
Client provides documents via email/fax	45	97.8%	2.2%	0.0%
Client uploads scanned documents to a secure portal	46	82.6%	17.4%	0.0%
Client uploads documents via mobile application	46	41.3%	56.5%	2.2%
Worker requests data files from commercial/State/federal databases	45	88.9%	11.1%	0.0%
Worker directly queries commercial/State/federal databases in real time	46	87.0%	13.0%	0.0%

Notes: Number of responses for each method varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 5.9.

Table A.23 Methods Used by SNAP Staff to Determine Eligibility for SNAP Applications and Recertifications

Methods	Number of Respondents	Yes/No		
		Yes	No	Don't Know/Unsure
Client provides paper documents	46	97.8%	2.2%	0.0%
Client provides documents via email/fax	45	97.8%	2.2%	0.0%
Client uploads scanned documents to a secure portal	46	82.6%	17.4%	0.0%
Client uploads documents via mobile application	46	41.3%	56.5%	2.2%
Worker requests data files from commercial/State/federal databases	45	88.9%	11.1%	0.0%
Worker directly queries commercial/State/federal databases in real time	46	87.0%	13.0%	0.0%

Notes: Number of responses for each method varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 5.9.

Table A.24 Methods Used by SAs to Conduct Interviews for SNAP Applications and Recertifications

Methods	Frequency	Percentage
Secure File Transfer Protocol (SFTP) sites	39	90.7%
Use of encryption	35	81.4%
Direct email	11	25.6%
Telephone	11	25.6%
Fax	9	20.9%
Face-to-face	6	14.0%
Other (e.g., a multifactor authentication (MFA) virtual private network)	4	9.3%
Mailed physical storage devices (CDs, USB drives, etc.) with requested information	3	7.0%
Don't know/unsure	3	7.0%
Total number of respondents	**43**	**100.0%**

Notes: Findings about methods being used during requested transmission of data are based on the responses from 43 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 5.10.

Table A.25 Frequency of Security Incidents

Years	Frequency	Percentage
2013	1	12.5%
2014	2	25.0%
2015	1	12.5%
2016	1	12.5%
2019	1	12.5%
2020	2	25.0%
Total number of respondents	**8**	**100.0%**

Notes: Findings about year that incidents occur are based on the responses from 8 SAs; total sample size = 47.
Source: SNAP PII State Agency Survey, question 5.16.

Table A.26 Stakeholders Notified of Security Incidents

Stakeholders	Number of Respondents	Yes	No
Affected SNAP recipients	8	100.0%	0.0%
Other	2	100.0%	0.0%
Affected SNAP applicants	7	85.7%	14.3%
FNS	6	83.3%	16.7%
U.S. Department of Homeland Security	5	40.0%	60.0%
General public	5	40.0%	60.0%

Notes: Number of responses for each stakeholder varies, it is reported in the table; total sample size = 47.
Source: SNAP PII State Agency Survey, question 5.18.

Table A.27 Methods Used by SAs to Handle Data files

Methods	Frequency	Percentage
The file is kept for a specific amount of time before being destroyed	30	68.2%
The file is destroyed immediately after the match is completed	4	9.1%
The file is never destroyed	1	2.3%
Other (e.g., depends on the terms of the data-sharing agreement)	3	6.8%
Don't know/unsure	6	13.6%
Total number of respondents	**44**	**100.0%**

Notes: Findings about what SA do with the created data file(s) are based on the responses from 44 SAs; total sample size = 47. Additional measures were specified in an open-text response, one or two open-text responses were listed in the bracket.
Source: SNAP PII State Agency Survey, question 7.3.

Section 8: Opportunities and Challenges

Table A.28 Possible Gaps in the Approach to Safeguarding PIIs

Possible Gaps	Frequency	Percentage
Need for various systems upgrades in order to adopt up-to-date security practices	19	43.2%
Auditing requirements of different agencies that either conflict or are burdensome to implement	16	36.4%
Difficulty of hiring staff with cybersecurity backgrounds	15	34.1%
Lack of resources for SNAP administration overall	13	29.5%
Non-regular or infrequent use of penetration testing	10	22.7%
Difficulties in monitoring system access	7	15.9%
Not applicable. There are no gaps in our SA's approach	7	15.9%
Lack of or inadequate training on PII	4	9.1%
Don't know/unsure	4	9.1%
Other	0	0.0%
Total number of respondents	**44**	**100.0%**

Notes: Findings about methods being used during requested transmission of data are based on the responses from 44 SAs; total sample size = 47. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 8.2.

Table A.29 Additional Safeguarding Practices

	Number of Respondents	Percentage
SA planning to adapt the State Bureau of Information Technology (BIT) Security Plans.	2	16.7%
SA needs to implement stringent requirements to ensure compliance and hence do not use additional programs.	4	33.3%
None	6	50.0%

Notes: Discussion on other procedures to safeguard SNAP PII are based on the responses of 11 SAs; total sample size = 47. Each respondent can choose multiple options.
Source: SNAP PII State Agency Survey, question 8.3.

Table A.30 Discussion on Other Safeguarding Practices

Other Safeguarding Practices	Frequency	Percentage
Upgrading/ transitioning eligibility legacy system	2	20.0%
Do not have a formal Disaster Recovery plan, but have robust compensating controls and policies proven by zero downtime	1	10.0%
Follow NIST, HIPPA, and IRS 1075 that cover and exceed SNAP requirements.	1	10.0%
None	6	60.0%

Notes: Findings about methods being used during requested transmission of data are based on the responses from 44 SAs; total sample size = 47. This survey question allowed the respondent to select all options that applied; percentages will not sum to 100.
Source: SNAP PII State Agency Survey, question 8.4.

APPENDIX D: SURVEY OF SNAP STATE AGENCIES (PAPER VERSION)

Thank you for participating in the survey contracted from the U.S Department of Agriculture (USDA) Food and Nutrition Service (FNS) to gain a better understanding of how States safeguard personally identifiable information (PII) of participants in the Supplemental Nutrition and Assistance Program (SNAP). The survey and other data collection efforts will document practices in SNAP State agencies (SAs) located in all 50 States, the District of Columbia, Guam, and the U.S. Virgin Islands. The ultimate purpose of the project is to identify best practices for safeguarding PII that can be shared among SNAP SAs.

This survey includes the following eight sections as they pertain to safeguarding PII:

1) SA Systems Context
2) System Security Plan Information
3) Personnel Policies and Procedures
4) Security Policies and Procedures
5) SNAP Application and Recertification Processes
6) Maintenance and Storage of PII
7) Data Sharing and Transfer of PII
8) Opportunities and Challenges

[*Branching Language Displayed for County-Administered States*: Within county-administered systems, the SNAP SAs are responsible for establishing statewide safeguarding requirements in accordance with federal policies, while county-level agencies are given discretion in how to best meet or exceed the requirements set by the SNAP SA. Accordingly, this survey is primarily focused on the statewide safeguarding requirements established by your SA as opposed to the individual requirements established by county-level agencies.]

Please answer as openly and honestly as possible. Your answers will be kept private; answers will not be associated with individual names, and only aggregated results will be published in any reports. More specifically, while we will report findings across States, there is still a risk that information about specific States could be inferred. We will employ disclosure avoidance methods to de-identify data in order to reduce the likelihood of identifying individual States. Your participation in this survey will not affect your employment or your State's SNAP funding. We encourage you to work with other staff if you do not have answers to all questions; share the survey link with staff who will be responding to specific questions. Please see the Frequently Asked Questions at the top of the survey page for more information on types of staff who may be most appropriate to answer each module.

The survey is designed to be completed in approximately 60 minutes. Please complete the survey by January 14, 2022. As you respond to survey questions, please note the following:

- Hovering your cursor over text in blue will show more information about the term.
- Please respond to all questions to the best of your ability and use the survey link to share sections with other staff who may have more technical knowledge.
- Unless you see the words "SELECT ALL THAT APPLY" after a question, please select only one response for each question.
- You may move forward through the questions by clicking on the **Next** button, and you may always go back and change an answer by clicking on the **Back** button.
- To skip through sections, click the **Table of Contents** button at the top of the survey window. Clicking a section in the Table of Contents will take you to the beginning of that section.
- Your answers will automatically be saved (but can still be edited) when you click **Next**.
- If you would like to exit the survey and finish it at a later time, click on the "X" at the top right corner.
- You can return to the survey by using the same link.

If you have any questions or concerns about completing the survey, please do not hesitate to contact the help desk at SNAPPII@2mresearch.com or call toll free at 1-877-230-3035. Thank you for your participation in this important survey.

According to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0584-0666. The time required to complete this information collection is estimated to average 60 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Section 1. SA Systems Context Suggested respondents for this section include: SA Director or Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person].

This section asks about your SA's systems and organizational structure to provide context for the questions on security planning and approaches to protecting SNAP participants' PII. For this survey, we define "systems" as general purpose information systems and the individual devices that connect to these systems (NIST SP 800-171r1[67]).

Questions about your SA's organizational structure include the degree to which SNAP systems are administered at the State or county level and the integration of SNAP systems with systems from other State programs (including those required to share or receive data from SNAP).

The context for implementation includes questions regarding the numbers and positions of staff responsible for SNAP participant PII security, the age and history of the SA's data systems, and the infrastructure available for establishing data use agreements.

1.1. How has your agency structured its approach for using systems security professionals[68] dedicated to protecting SNAP PII?

- System security professionals are located within the agency that administers the SNAP program (often along with other programs)
- Systems security professionals are located within another state agency (such as a Department of Technology Services or an Office of the Chief Information Officer)
- Our agency utilizes a combination of system security professionals located within our agency and systems security professionals located within another state agency
- Other. Please specify:_____

1.2. What staff member(s) in or outside of your SA are responsible for protecting SNAP PII? SELECT ALL THAT APPLY.

- ☐ SNAP IT Director
- ☐ Lead Applications Developer
- ☐ Systems cybersecurity specialists within the agency that administers the SNAP program (often along with other programs)
- ☐ Data analysts
- ☐ IT Contractor staff

[67] Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016). P*rotecting controlled unclassified information in nonfederal systems and organizations* (NIST Special Publication 800-171 R.1). Retrieved from U.S. Department of Commerce, *National Institute of Standards and Technology* Website: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[68] Hover to read the following definition: "Staff whose primary job duties are focused on activities to mitigate potential and existing vulnerabilities and threats, including but not limited to preventing cyber-attacks and leveraging their expertise and knowledge of databases, networks, hardware, and firewalls and encryption."

- ☐ Staff from a central state agency (such as the State CIO or CISO[69] Office)
- ☐ Other. Please specify:_____

1.3 In what time period was the main SNAP eligibility system implemented?

- Before 1990
- 1990–1999
- 2000–2009
- 2010–2019
- 2020–2021

1.4. Do you consider your main SNAP eligibility system to be a legacy system?[70]

- Yes
- No

1.5 Is your SNAP eligibility system integrated with eligibility systems of the following programs? SELECT ALL THAT APPLY.

- Temporary Assistance for Needy Families (TANF)
- Medicaid
- Women, Infants, and Children (WIC)
- Low Income Home Energy Assistance Program (LIHEAP)
- The state's child care program
- The state's child welfare system
- Other. Please specify:_____

Data Matching. SAs are required by law and federal regulations to match or exchange data including PII with other State and federal agencies, as well as institutions such as school districts and law enforcement agencies. The next set of questions asks about your SA's data-matching activities.

1.6. Against which data sources does your SA match SNAP applicant and recipient data? SELECT ALL THAT APPLY.

National Data Sources

- ☐ Prisoner Verification System
- ☐ Social Security Administration Death Master File
- ☐ National Directory of New Hires (NDNH)

[69] Hover to read the following definition: "Chief Information Officers (CIOs) or Chief Information Security Officers (CISOs) are typically senior officials who have executive-level and statewide responsibility for developing and overseeing policies and programs to ensure that government information is protected."
[70] Hover to read the following definition: "A current information system that uses a computing infrastructure several generations old."

- ☐ Internal Revenue Service
- ☐ Veterans Administration
- ☐ Electronic Disqualified Recipient System (eDRS)
- ☐ State Data Exchange (SDX)
- ☐ Beneficiary Data Exchange (BENDEX)
- ☐ Income and Eligibility Verification System (IEVS)
- ☐ Public Assistance Reporting Information System (PARIS)
- ☐ Other. Please specify:_____

State Data Sources

- State death records
- State birth record directory
- State new hire directory
- State or local prison listings
- State warrant management directory
- State parole directory
- State lottery information
- State Department of Motor Vehicles
- State workforce data – unemployment insurance/state quarterly wage information/State employee information
- State child support payments
- State educational agencies
- State law enforcement agencies
- Other. Please specify:_____

1.7. Do you have data-sharing agreements with each of the agencies your SA shares data with?

- ○ Yes
- ○ No (go to Q1.9)
- ○ Don't know/unsure (*go to Q1.9*)

1.8. How often are data-sharing agreements updated? SELECT ALL THAT APPLY.

- ☐ Every 6 months
- ☐ Once a year
- ☐ When the data-sharing agreement is renewed or there is a change in the data sharing processes used by one of the agencies
- ☐ Other. Please specify: _____
- ☐ Don't know/unsure

1.9. When a data match is requested, what type of applicant/recipient data are commonly used to perform the match? SELECT ALL THAT APPLY.

- ☐ Social Security Number
- ☐ Applicant/recipient name
- ☐ Applicant/recipient date of birth
- ☐ Case number
- ☐ Another unique identifier used by your SA or other agencies in the State. Please specify:_____
- ☐ Other data to facilitate "probabilistic/fuzzy matching"[71] using a combination of variables. Please specify:___
- ☐ Don't know/unsure

Branched Question for County-Administered States (This question will only be displayed to the 10 states with county-administered SNAP systems)

1.10. To what extent have county offices developed their own SNAP-eligibility systems to interact with your SA's statewide SNAP eligibility system?

- ○ None of the county offices
- ○ A minority of county offices
- ○ A majority of county offices
- ○ All county offices

Section 2. System Security Plan Information: Creation, Updates, Adherence, Vulnerabilities, and Threats. Suggested respondents for this section include: Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person]and SA Director).

In this section, we ask questions that help us understand your SA's system security plan for safeguarding PII of SNAP applicants and participants.

[*Branching Language Displayed for County-Administered States*: In this section, we ask questions that help us understand your SA's **statewide** system security plan for safeguarding PII of SNAP applicants and participants.]

2.1. Which of the following sources is your SA's system security plan for protecting PII based on? SELECT ALL THAT APPLY.

- ▪ Standards from central State Information Security (IS)/IT agency
- ▪ Standards from systems contractor
- ▪ Other. Please specify:_____

2.2. Is the SA's policy based on one or more of the following? SELECT ALL THAT APPLY.

[71] Hover to read the following definition: "A matching technique that is typically applied to records that cannot be exactly matched using unique identifiers. This approach compares several variable values between two records and then assigns a weighted probability on the likelihood of a match."

- ☐ FISMA[72]
- ☐ NIST[73] Guidelines
- ☐ HIPAA[74]
- ☐ Federal SNAP Regulations
- ☐ State SNAP Laws or Regulations
- ☐ Other. Please specify:_____

2.3. Are you or your agency's systems security professionals familiar with the following guidance that FNS has provided to SAs on methods for protecting PII? SELECT ONE RESPONSE PER ROW.

	Very Familiar	Somewhat Familiar	Not Really Familiar	Not Aware of this Resource
Privacy Act of 1974 (5 U.S.C. § 552a)	○	○	○	○
FNS Handbook 901: The Advance Planning Document Process	○	○	○	○
7 CFR 274.5 – Record retention and forms security	○	○	○	○
7 CFR 274.8 – Functional and technical EBT system requirements	○	○	○	○
Other guidance provided by USDA, FNS State Systems Office	○	○	○	○
NIST[6] Guide to Protecting Confidentiality of PII	○	○	○	○

2.4. How long has it been since your SA's system security plan for safeguarding PII of SNAP applicants and participants was last updated?

_____ (enter number of months)

- ☐ Don't know/unsure

2.5. If not already in place, in which of the following domains is your SA ***likely to undertake efforts*** to upgrade its formal safeguarding policies and procedures within the next 2 years? SELECT ONE RESPONSE PER ROW.

[72] Hover to read the following definition: "The Federal Information Security Management Act (FISMA) is federal legislation that provides a comprehensive framework for protecting government information, operations, and assets against man-made and natural threats."
[73] Hover to read the following definition: "The National Institute of Standards and Technology (NIST) is responsible for developing information technology (IT) security standards and guidelines for the Federal Government. Pertinent examples include the Guide to Protecting Confidentiality of PII and the minimum security requirements for federal information and information systems."
[74] Hover to read the following definition: "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal legislation that provides data privacy and security provisions for safeguarding medical information."

	Very Likely	Somewhat Likely	Unlikely	Very Unlikely	Already in Place	Don't Know/Unsure
Personnel Policies and Procedures: Ensuring that staff working with PII have met the requisite security requirements and are approved to access data						
Using Role-Based Security Levels[75] to provide data access	○	○	○	○	○	○
Delivering regular security training and education	○	○	○	○	○	○
Other personnel policies and procedures (Specify) _____	○	○	○	○	○	○
Security Policies and Procedures: Approaches for implementing a robust security plan						
Securing PII across hardware systems	○	○	○	○	○	○
Securing PII across software systems	○	○	○	○	○	○
Securing PII across network systems	○	○	○	○	○	○
Regularly assessing risk and vulnerabilities	○	○	○	○	○	○
Regularly performing security testing	○	○	○	○	○	○
Developing emergency preparedness and contingency plans	○	○	○	○	○	○
Other security policies and procedures (Specify)_____	○	○	○	○	○	○
Program Operations: Safeguards associated with administering SNAP						
Masking PII[76]	○	○	○	○	○	○
Implementing time-out features on computer screens	○	○	○	○	○	○
Safeguarding PII during delivery of SNAP benefits via EBT	○	○	○	○	○	○
Matching PII to other data sources for eligibility determination	○	○	○	○	○	○
Matching PII to other data sources for program integrity purposes	○	○	○	○	○	○
Securely destroying PII data that are no longer used	○	○	○	○	○	○
Other program operations (Specify) _____	○	○	○	○	○	○

[75] Hover to read the following definition: "Role-based security levels are used to allow system access only to authorized users. Under this approach, employees are only allowed to access the information necessary to effectively perform their job duties."

[76] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

2.6. In addition to your SA's system security professional(s), which of the following staff provide input on or are involved in updating the security plan for protecting SNAP PII as security requirements and guidelines change? SELECT ALL THAT APPLY.

- ☐ SNAP Director
- ☐ SNAP IT staff or SNAP applications development staff
- ☐ SNAP policy staff
- ☐ EBT contractors
- ☐ Other SNAP program staff
- ☐ Staff from the State's Office of Information Technology
- ☐ The State's CIO or their staff
- ☐ The State's CISO or their staff
- ☐ Staff from other agencies in the State. Please specify:_____
- ☐ Staff from county offices administering SNAP
- ☐ Contractors/vendors
- ☐ Not applicable. My SA has not updated the security plan for protecting SNAP PII.

2.7. After identifying a security gap or a necessary update to the security plan, does your SA use a Plan of Action and Milestones (POA&M)[77] or another similar risk planning tool to identify tasks that need to be accomplished?

- ○ Yes
- ○ No
- ○ Don't know/unsure

2.8. To what extent has your SA faced challenges with understanding, complying with, testing or validating, or updating its system security plan for safeguarding PII of SNAP applicants and participants? SELECT ONE RESPONSE PER ROW

	To a Great Extent	Somewhat	Very Little	Not at All
Understanding the system security plan	○	○	○	○
Complying with the system security plan	○	○	○	○
Testing or validating the system security plan	○	○	○	○
Updating the system security plan	○	○	○	○
Other (Please specify) _____	○	○	○	○

Section 3. Personnel Policies and Procedures. Suggested respondents for this section include: SA Director and Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person]

[77] Hover to read the following definition: "A key document that facilitates a structured approach to tracking risk mitigation strategies."

This section includes questions about restrictions on personnel access to data that include PII, procedures for authorizing and monitoring access, and frequency and content of staff training regarding cybersecurity and processes for safeguarding PII.

[*Branching Language Displayed for County-Administered States*: This section includes questions about the **statewide procedures** that your SA has established regarding restrictions on personnel access to data that include PII, procedures for authorizing and monitoring access, and frequency and content of staff training regarding cybersecurity and processes for safeguarding PII.]

Staffing and Training

3.1. In addition to staff who determine eligibility and their managers, who has direct access to SNAP PII? SELECT ALL THAT APPLY.

- ☐ Clerical/administrative workers
- ☐ Program integrity/quality control staff
- ☐ SNAP data analysts
- ☐ Staff from another SA (such as Medicaid, TANF, Low Income Home Energy Assistance Program)
- ☐ Other. Please specify:_____
- ☐ Don't know/unsure

3.2. How are role-based security levels[78] established to limit staff access to PII data? SELECT ALL THAT APPLY.

- ☐ Staff need approval to view participant data.
- ☐ Staff need approval to modify or edit participant data.
- ☐ Staff have access to participant data on an "as needed" basis, with supervisor approval.
- ☐ Other. Please specify:_____

3.3. Which staff receive training on PII? SELECT ALL THAT APPLY.

- ☐ IT/IS professionals
- ☐ Line staff who process applications or recertifications in person, online, or as part of a telephone center
- ☐ Managers
- ☐ Members of the Incident Response Team
- ☐ Staff of EBT contractors
- ☐ Other staff. Please specify:_____

[78] Hover to read the following definition: "Role-based security levels are used to allow system access only to authorized users. Under this approach, employees are only allowed to access the information necessary to effectively perform their job duties."

3.4. What methods does your agency use to establish PII safeguarding requirements for contractors (such as an EBT contractor or a call center)? SELECT ALL THAT APPLY.

- ☐ PII trainings
- ☐ Contractual agreements (such as a Memorandum of Understanding [MOU] or a Data Use Agreement [DUA]) that meet specific security standards.
- ☐ Other. Please specify:_____
- ☐ Don't know/unsure

3.5. In general, how often are the majority of staff with access to PII trained on its protection? SELECT ALL THAT APPLY.

- ☐ On hire
- ☐ Annually
- ☐ Whenever major systems changes are implemented
- ☐ Other. Please specify:_____

3.6. Who provides the PII training for your SNAP SA? SELECT ALL THAT APPLY.

- ☐ SNAP SA
- ☐ Other agency in the State (such as CIO)
- ☐ Contractor for eligibility system. Please specify:_____
- ☐ Commercial "off the shelf" training provider. Please specify:_____
- ☐ Other. Please specify:_____

3.7. How are PII trainings provided? SELECT ALL THAT APPLY.

- ☐ Online training in a group setting
- ☐ In-person training in a group setting
- ☐ Webinar
- ☐ Self-paced online trainings
- ☐ Other. Please specify:_____

3.8. What are major components of the training? SELECT ALL THAT APPLY.

- ☐ What is PII, and why does it need to be protected?
- ☐ Protecting accidental disclosure of PII on screens or papers in SNAP office
- ☐ Limits on use of mobile devices to safely access PII (if safeguarding procedures exist)
- ☐ Protection of PII during data analysis, transmission, and storage
- ☐ Protection of PII used to issue EBT cards
- ☐ Using matched data and resolving any issues with matching results
- ☐ Procedures when PII has been inappropriately disclosed
- ☐ Procedures for reporting violations to management
- ☐ Updates on efforts to protect PII

- ☐ Penalties for not protecting PII
- ☐ Other. Please specify:_____

3.9. To what extent does your SA's security plan meet and/or exceed the safeguarding requirements for personnel that are in FNS Handbook 901 and associated FNS regulations? Please give us your best assessment of the following: SELECT ONE RESPONSE PER ROW.

	Meeting Requirements, with Room for Improvement	Meeting Requirements	Especially Successful at Meeting Requirements
Ensuring that staff working with PII have met the requisite security requirements and are approved to access data	○	○	○
Conducting personnel background checks	○	○	○
Using role-based security levels to provide data access	○	○	○
Delivering regular IT security training and education	○	○	○

Section 4. Security Policies and Procedures. Suggested respondents for this section include: Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person].

This section asks about the use of various security features that are not client-facing, including firewalls, limits on remote access, third-party testing, and emergency preparedness.

[*Branching Language Displayed for County-Administered States*: This section includes asks about the **statewide procedures** that your SA has established for the use of various security features that are not client-facing, including firewalls, limits on remote access, third-party testing, and emergency preparedness.]

4.1. An SA's ability to effectively safeguard SNAP PII may be hindered by a combination of internal vulnerabilities and internal and external threats. To what extent has your SA encountered the following vulnerabilities and threats to SNAP PII? SELECT ONE RESPONSE PER ROW.

	Never	Rarely	Sometimes	Often	Very Often	Don't Know/Unsure
Internal Vulnerabilities						
Improper storage or disposal of physical materials that contain PII (such as printouts or other paper documents)	○	○	○	○	○	○
Improperly secured systems with access to PII	○	○	○	○	○	○
Improperly secured mobile devices with access to PII	○	○	○	○	○	○

	Never	Rarely	Sometimes	Often	Very Often	Don't Know/Unsure
Unauthorized use of system resources by SA employees to access PII or unauthorized manipulation of PII data by SA employees	○	○	○	○	○	○
Unauthorized disclosure of PII data by SA employees or a trusted partner	○	○	○	○	○	○
Macro-level system failures (Specify)	○	○	○	○	○	○
Failures or decreases in the reliability of hardware	○	○	○	○	○	○
Failures or decreases in the reliability of software	○	○	○	○	○	○
Other vulnerabilities (Specify)	○	○	○	○	○	○
External Threats						
Denial of service attacks[79]	○	○	○	○	○	○
Phishing, spoofing, or pharming[80]	○	○	○	○	○	○
Introduction of malicious code (such as viruses, spyware, or malware)	○	○	○	○	○	○

Branched Question for County-Administered States (This version of the question will only be displayed to the 10 states with county-administered SNAP systems)

4.1. An SA's ability to effectively safeguard SNAP PII may be hindered by a combination of internal vulnerabilities and internal and external threats. To what extent has your SA encountered the following vulnerabilities and threats to SNAP PII? SELECT ONE RESPONSE PER ROW.

	Never	Rarely	Sometimes	Often	Very Often	Don't Know/Unsure
Internal Vulnerabilities						
Improper storage or disposal of physical materials that contain PII (such as printouts or other paper documents)	○	○	○	○	○	○
Improperly secured systems with access to PII	○	○	○	○	○	○
Improperly secured mobile devices with access to PII	○	○	○	○	○	○
Unauthorized use of system resources by SA or county employees to access PII or unauthorized manipulation of PII data by SA employees	○	○	○	○	○	○
Unauthorized disclosure of PII data by SA or county employees or a trusted partner	○	○	○	○	○	○

[79] Hover to read the following definition: "An external attack that attempts to make computer resources, such as a website or web service, unavailable to users."
[80] Hover to read the following definition: "Methods commonly used by cyber criminals to exploit individuals and gain access to private information. These methods consist of sending a malicious email that is disguised as an email from a legitimate, trustworthy source (i.e., phishing); impersonating another individual or organization (i.e., spoofing); or creating a malicious website that resembles a legitimate website (i.e., pharming)."

	Never	Rarely	Sometimes	Often	Very Often	Don't Know/Unsure
Macro-level system failures (Specify)	○	○	○	○	○	○
Failures or decreases in the reliability of hardware	○	○	○	○	○	○
Failures or decreases in the reliability of software	○	○	○	○	○	○
Other vulnerabilities (Specify)	○	○	○	○	○	○
External Threats						
Denial of service attacks[81]	○	○	○	○	○	○
Phishing, spoofing, or pharming[82]	○	○	○	○	○	○
Introduction of malicious code (such as viruses, spyware, or malware)	○	○	○	○	○	○

4.2. Audit trails[83] support several security objectives. Which of the following information is captured within your SA's audit trails? SELECT ALL THAT APPLY.

- ☐ Timing of system startup and shutdown
- ☐ Successful and unsuccessful login attempts
- ☐ User actions to access files or applications
- ☐ Attempts to access data for which a worker does not have access/permissions
- ☐ The activities of system administrators and systems security staff
- ☐ Date and time of any security events[84]
- ☐ Type of security event experienced and its success or failure
- ☐ Names of files or applications accessed during a security event
- ☐ Other. Please specify:_____
- ☐ Not applicable. Our SA does not use audit trails.

4.3. Has your SA implemented the following firewall[85] safeguards, policies, and procedures?

	Yes	No	Don't Know/Unsure
Use of a hardware-based firewall	○	○	○
Use of a software-based firewall	○	○	○
Maintaining audit records of all security-related events	○	○	○

[81] Hover to read the following definition: "An external attack that attempts to make computer resources, such as a website or web service, unavailable to users."
[82] Hover to read the following definition: "Methods commonly used by cyber criminals to exploit individuals and gain access to private information. These methods consist of sending a malicious email that is disguised as an email from a legitimate, trustworthy source (i.e., phishing); impersonating another individual or organization (i.e., spoofing); or creating a malicious website that resembles a legitimate website (i.e., pharming)."
[83] Hover to read the following definition: "A record of user activity within a system that supports several security objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification."
[84] Hover to read the following definition: "A security event is any occurrence during which data or records may have been exposed. In contrast, **security incidents** are less common occurrences in which data or records have been breached."
[85] Hover to read the following definition: "Firewalls are employed to prevent unauthorized users or illicit software from gaining access to private networks connected to the internet."

	Yes	No	Don't Know/Unsure
Limiting firewall access to network security analysts or other approved users	○	○	○
Regularly reviewing the list of approved users with access to the firewall	○	○	○
Timely installation of security-related updates, fixes, or modifications that have been tested and approved	○	○	○
Other firewall safeguards, policies, and procedures	○	○	○

4.4. Does your SA allow employees remote access (such as a VPN connection) to systems containing the PII of SNAP applicants and participants?

- ○ Yes, employees can use remote access but only when using authorized agency equipment.
- ○ Yes, employees can use remote access when using authorized agency equipment or personal devices.
- ○ No (go to Q4.6)
- ○ Don't know/unsure

Branched Question for County-Administered States (This version of the question will only be displayed to the 10 states with county-administered SNAP systems)

4.4. Does your SA allow state or county employees remote access (such as a VPN connection) to systems containing the PII of SNAP applicants and participants?

- ○ Yes, employees can use remote access but only when using authorized agency equipment.
- ○ Yes, employees can use remote access when using authorized agency equipment or personal devices.
- ○ No (go to Q4.6)
- ○ Don't know/unsure

4.5. Which of the following procedures has your SA implemented for providing employees remote access to PII? SELECT ALL THAT APPLY.

- ☐ Establishing policies on usage restrictions, user application and approval, and implementation guidance for each approved method of remote access
- ☐ Regularly reviewing the list of approved users with remote access and monitoring for unauthorized remote access
- ☐ Enforcing technical requirements for remote access prior to authorizing connections
- ☐ Other. Please specify:_____
- ☐ Don't know/unsure

Branched Question for County-Administered States (This version of the question will only be displayed to the 10 states with county-administered SNAP systems)

4.5. Which of the following procedures has your SA implemented for providing state or county employees with remote access to PII? SELECT ALL THAT APPLY.

- ▪ Establishing policies on usage restrictions, user application and approval, and implementation guidance for each approved method of remote access
- ▪ Regularly reviewing the list of approved users with remote access and monitoring for unauthorized remote access
- ▪ Enforcing technical requirements for remote access prior to authorizing connections
- ▪ Other. Please specify:_____
- ○ Don't know/unsure

4.6. Which of the following parties, if any, does your SA use to conduct penetration testing[86]? SELECT ALL THAT APPLY.

- ☐ A contractor or vendor. Please specify:_____
- ☐ SA's IT or security team
- ☐ Another agency in the State. Please specify:_____
- ○ Not currently performed on systems containing the PII of SNAP applicants and participants
- ○ Don't know/unsure

4.7. Disasters and other emergencies pose a formidable challenge to safeguarding the PII of SNAP applicants and participants. In your opinion, are the following components present within your SA's disaster recovery plan to protect PII during disasters or other emergency situations? SELECT ONE RESPONSE PER ROW.

	Yes	No	Don't Know/Unsure
It effectively details how the SA will recover and restore the system to normal operations.	○	○	○
It specifies a process for protecting PII from internal and external threats until the system is restored to normal operations.	○	○	○
It is effectively integrated into the SA's security plan.	○	○	○
It provides a process for training staff in their specific response to a disaster according to their roles.	○	○	○
It specifies a process for maintaining Local Area and Wide Area Networks.	○	○	○
It specifies a process for maintaining desktops and personal computers.	○	○	○
It specifies a process for maintaining SA websites.	○	○	○
It specifies a process for maintaining distributed and mainframe systems.	○	○	○
It specifies alternative physical locations for operations in the event that original facilities are unavailable.	○	○	○

[86] Hover to read the following definition: "A controlled, real-world hacking process that is used to evaluate the security of systems in real-time, identify vulnerabilities, and determine mitigation strategies."

	Yes	No	Don't Know/Unsure
It can be activated on its own and does not require that other contingency plans be activated first.	○	○	○

4.8. To what extent does your SA's security plan meet and/or exceed the safeguarding requirements that are in FNS Handbook 901 and associated FNS regulations? Please give us your best assessment of how your SA's security plan meets or exceeds FNS requirements for security policies and procedures used to safeguard PII. SELECT ONE RESPONSE PER ROW.

	Meeting Requirements, with Room for Improvement	Meeting Requirements	Especially Successful at Meeting Requirements
Hardware-specific controls[87]	○	○	○
Software-specific controls[88]	○	○	○
Network-specific controls[89]	○	○	○
Regularly assessing risk and vulnerabilities	○	○	○
Regularly performing security testing	○	○	○
Developing emergency preparedness and contingency plans	○	○	○

Section 5. SNAP Application and Recertification Processes. Suggested respondents for this section include: SA Director and Data Analyst

This section asks about your SA's procedures that involve safeguarding PII throughout the SNAP application and recertification processes.

5.1. Does your SA receive SNAP applications and recertifications in the following ways?

	Yes	No
Interview with SNAP staff (either in person or on the phone)	○	○
Mailing or faxing physical applications to the SA	○	○
Interviews with non-SNAP staff who do eligibility determinations for multiple public assistance programs, such as SNAP, TANF, WIC, public housing assistance, child care, and employment training programs	○	○
Online initial application	○	○
Online recertifications	○	○
Mobile apps – initial application	○	○
Mobile apps – recertifications	○	○

[87] Hover to read the following definition: "Hardware-specific controls include servers, firewalls, wireless access points, cameras, keycard readers, biometric devices, etc."
[88] Hover to read the following definition: "Software-specific controls include antivirus, access control, audit logging, Secure File Transfer Protocol (SFTP) software, VPN clients, etc."
[89] Hover to read the following definition: "Network-specific controls include IP filtering, MAC address filtering, etc."

	Yes	No
Other (Specify) _____	○	○

(*If no to Q5.1(a) or Q5.1(c), go to Q5.3*)

5.2. Does your SA conduct interviews for SNAP applications and recertifications via the following methods? SELECT ONE RESPONSE PER ROW.

	Yes	No	Don't Know/Unsure
Face-to-face interviews	○	○	○
Telephone interviews with local office	○	○	○
Telephone interviews with call center	○	○	○
Telephone interviews with interactive voice response	○	○	○
Other (Specify) _____	○	○	○

5.3. How are cases or applications uniquely identified in your eligibility system? SELECT ALL THAT APPLY.

- ☐ Social Security Number
- ☐ Assigned case numbers (i.e., a client ID number or another unique number)
- ☐ Head of household's name
- ☐ Head of household's date of birth
- ☐ Other. Please specify:_____
- ☐ Don't know/unsure

5.4. Does your eligibility system mask[90] Social Security numbers during data entry?

- ○ Yes
- ○ No
- ○ Don't know/unsure

5.5. What methods does your SA use to safeguard PII that is submitted by SNAP applicants or participants via online forms? SELECT ALL THAT APPLY.

- ☐ Applicants/participants must enter a system- or user-generated password to access their accounts.
- ☐ Warnings are displayed regarding the need for applicants/participants to protect their PII.
- ☐ Time-out functions are used to automatically log out applicants/participants due to inactivity.
- ☐ Applications and other forms are encrypted.
- ☐ Other. Please specify: _____

[90] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

☐ Don't know/unsure

Data Entry and Storage

5.6. How does your SA enter paper SNAP applications into your eligibility system? SELECT ALL THAT APPLY.

☐ Office staff manually enter paper applications into eligibility system.
☐ Office staff scan and upload paper applications into eligibility system.
☐ Our SA does not accept paper applications. (*go to Q5.8*)
☐ Don't know/unsure

5.7. How are paper SNAP applications and recertification documents (or online versions that are later printed out) stored by local agencies or call centers while the applications are pending or in process? SELECT ALL THAT APPLY.

☐ In a file cabinet in a locked room
☐ In Caseworker's/Eligibility Counselor's locked drawer in the desk
☐ On Caseworker's/Eligibility Counselor's desk
☐ In buckets/baskets in an open office behind a restricted area
☐ Located with a designated staff member. Please specify:_____
☐ Other. Please specify: _____
☐ Don't know/unsure

5.8. How are denied applications handled?

o Destroyed upon denial
o Kept for a specified period before destruction
o Scanned to a document imaging system and then destroyed
o Never destroyed/stored securely
o Other. Please specify:_____
o Don't know/unsure

Verification of Applications/Recertifications

5.9. Do SNAP staff who determine eligibility gather verification data for SNAP applications and recertifications use the following methods? SELECT ONE RESPONSE PER ROW.

Client provides paper documents.	O	O	O
Client provides documents via email/fax.	O	O	O
Client uploads scanned documents to a secure portal.	O	O	O
Client uploads documents via mobile application.	O	O	O
Worker requests data files from commercial/State/federal databases.	O	O	O
Worker directly queries commercial/State/federal databases in real time.	O	O	O

5.10. What methods are used in safeguarding PII during requested transmission of data from commercial/State/federal databases for eligibility determination or program integrity assessments? SELECT ALL THAT APPLY.

- ☐ Use of encryption
- ☐ Secure File Transfer Protocol (SFTP) sites
- ☐ Direct email
- ☐ Fax
- ☐ Telephone
- ☐ Face-to-face
- ☐ Mailed physical storage devices (CDs, USB drives, etc.) with requested information
- ☐ Other. Please specify: _____
- ☐ Don't know/unsure

Time-Out Functions

5.11. Is there a time-out function used on caseworker eligibility system screens that contain PII?

- o Yes
- o No (go to Q5.13)
- o Don't know/unsure (*go to Q5.13*)

5.12. What is the time limit for the time-out? Please enter number of minutes.

_____ Minutes

- o Don't know/unsure

Security Incidents

As a reminder, **your answers to this survey will be kept private**; answers will not be associated with individual names, and only aggregated results will be published in any reports.

5.13. Does your SA's security plan have a specific policy for responding to security incidents?

- o Yes
- o No
- o Don't know/unsure (*go to Q5.19*)

5.14. Does your plan include required steps for incident response, including required reports to FNS and other agencies?

- Yes
- No
- Don't know/unsure (*go to Q5.19*)

5.15. To your knowledge, has your SA's SNAP eligibility system or application website ever had a security incident where PII was compromised that was created by internal users or external entities?

- Yes
- No (go to Q5.19)
- Don't know/unsure (*go to Q5.19*)

5.16. In what year did the Incident occur? Please describe the incident in the box below.

_____ (enter year of Incident)

[Please describe the incident.]

5.17. How many SNAP cases/applications were affected? Please enter an estimated number.

_____(number box)

- Don't know/unsure

5.18. Outside of your SA, which stakeholders were notified of the Incident?

Entity	Yes	No
FNS	○	○
U.S. Department of Homeland Security	○	○
General public	○	○
Affected SNAP applicants	○	○
Affected SNAP recipients	○	○
Other (Specify)	○	○

5.19. We are interested in understanding the extent to which your SA's application and recertification procedures meet the safeguarding requirements specified in FNS Handbook 901 and FNS regulations and policy memos. Please give us your best assessment of whether your SA's security plan incorporates safeguards associated with administering SNAP. SELECT ONE RESPONSE PER ROW.

Safeguards	Meeting Requirements, with Room for Improvement	Meeting Requirements	Especially Successful at Meeting Requirements
Masking[91] PII during data entry	○	○	○
Implementing time-out features on eligibility system screens containing PII	○	○	○
Secure delivery of SNAP benefits via EBT	○	○	○
Matching PII to other data sources for eligibility determination	○	○	○
Matching PII to other data sources for program integrity purposes	○	○	○

Branched Section for County-Administered States (This section will only be displayed to the 10 states with county-administered SNAP systems).

Section 5. SNAP Application and Recertification Processes. Suggested respondents for this section include: SA Director and Data Analyst .

This section asks about your SA's establishment of statewide procedures for county agencies to safeguard PII throughout the SNAP application and recertification processes.

5.1. Do county agencies receive SNAP applications and recertifications in the following ways?

	Yes	No
Interview with SNAP staff (either in person or on the phone)	○	○
Mailing or faxing physical applications to the county agency	○	○
Interviews with non-SNAP staff who do eligibility determinations for multiple public assistance programs, such as SNAP, TANF, WIC, public housing assistance, child care, and employment training programs	○	○
Online initial application	○	○
Online recertifications	○	○
Mobile apps – initial application	○	○
Mobile apps – recertifications	○	○
Other (Specify) _____	○	○

(*If no to Q5.1(a) or Q5.1(c), go to Q5.3*)

5.2. Do county agencies conduct interviews for SNAP applications and recertifications via the following methods? SELECT ONE RESPONSE PER ROW.

[91] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

	Yes	No	Don't Know/Unsure
Face-to-face interviews	○	○	○
Telephone interviews with county agency	○	○	○
Telephone interviews with call center	○	○	○
Telephone interviews with interactive voice response	○	○	○
Other (Specify) _____	○	○	○

5.3. How are cases/applications uniquely identified in your statewide SNAP eligibility system? SELECT ALL THAT APPLY.

- ☐ Social Security Number
- ☐ Assigned case numbers (i.e., a client ID number or another unique number)
- ☐ Head of household's name
- ☐ Head of household's date of birth
- ☐ Other. Please specify:_____
- ☐ Don't know/unsure

5.4. Does your statewide SNAP eligibility system mask[92] Social Security numbers during data entry?

- ○ Yes
- ○ No
- ○ Don't know/unsure

5.5. What methods does your SA require county agencies to use to safeguard PII that is submitted by SNAP applicants or participants via online forms? SELECT ALL THAT APPLY.

- ☐ Applicants/participants must enter a system- or user-generated password to access their accounts.
- ☐ Warnings are displayed regarding the need for applicants/participants to protect their PII.
- ☐ Time-out functions are used to automatically log out applicants/participants due to inactivity.
- ☐ Applications and other forms are encrypted.
- ☐ Other. Please specify: _____
- ☐ Don't know/unsure

Data Entry and Storage

[92] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

5.6. How do county agencies enter paper SNAP applications into your statewide SNAP eligibility system? SELECT ALL THAT APPLY.

- ☐ County staff manually enter paper applications into eligibility system.
- ☐ County staff scan and upload paper applications into eligibility system.
- ☐ County agencies do not accept paper applications. (*go to Q5.8*)
- ☐ Don't know/unsure

5.7. How are paper SNAP applications and recertification documents (or online versions that are later printed out) stored by county agencies or call centers while the applications are pending or in process? SELECT ALL THAT APPLY.

- ☐ In a file cabinet in a locked room
- ☐ In Caseworker's/Eligibility Counselor's locked drawer in the desk
- ☐ On Caseworker's/Eligibility Counselor's desk
- ☐ In buckets/baskets in an open office behind a restricted area
- ☐ Located with a designated staff member. Please specify:_____
- ☐ Other. Please specify: _____
- ☐ Don't know/unsure

5.8. How does your SA require county agencies to handle denied applications?

- ○ Destroyed upon denial
- ○ Kept for a specified period before destruction
- ○ Scanned to a document imaging system and then destroyed
- ○ Never destroyed/stored securely
- ○ Other. Please specify:_____
- ○ Don't know/unsure

Verification of Applications/Recertifications

5.9. Do county SNAP staff who determine eligibility gather verification data for SNAP applications and recertifications use the following methods? SELECT ONE RESPONSE PER ROW

Method of Receipt			
Client provides paper documents.	○	○	○
Client provides documents via email/fax.	○	○	○
Client uploads scanned documents to a secure portal.	○	○	○
Client uploads documents via mobile application.	○	○	○
Worker requests data files from commercial/State/federal databases.	○	○	○
Worker directly queries commercial/State/federal databases in real time.	○	○	○

5.10. What methods in your statewide SNAP eligibility system are used to safeguard PII during requested transmission of data from commercial/State/federal databases for eligibility determination or program integrity assessments? SELECT ALL THAT APPLY.

- ☐ Use of encryption
- ☐ Secure File Transfer Protocol (SFTP) sites
- ☐ Direct email
- ☐ Fax
- ☐ Telephone
- ☐ Face-to-face
- ☐ Mailed physical storage devices (CDs, USB drives, etc.) with requested information
- ☐ Other. Please specify: _____
- ☐ Don't know/unsure

Time-Out Functions

5.11. Does your SA require county agencies to use a time-out function on caseworker eligibility system screens that contain PII?

- o Yes
- o No (go to Q5.13)
- o Don't know/unsure (*go to Q5.13*)

5.12. What is the time limit for the time-out? Please enter number of minutes.

_____ Minutes

- o Don't know/unsure

Security Incidents

As a reminder, your **answers to this survey will be kept private**; answers will not be associated with individual names, and only aggregated results will be published in any reports.

5.13. Does your SA's security plan for its state SNAP eligibility system have a specific policy for responding to security Incidents?

- o Yes
- o No
- o Don't know/unsure (*go to Q6.1*)

5.14. Does your statewide plan include required steps for incident response, including required reports to FNS and other agencies?

- o Yes

- No
- Don't know/unsure (*go to Q6.1*)

5.15. To your knowledge, has your SA's statewide SNAP eligibility system or application website ever had a security incident where PII was compromised that was created by internal users or external entities?

- Yes
- No (go to Q5.19)
- Don't know/unsure (*go to Q5.19*)

5.16. In what year did the Incident occur? Please describe the incident in the box below.

_____ (enter year of Incident)

[Enter description of incident here.]

5.17. How many SNAP cases/applications were affected? Please enter an estimated number.

_____(number box)

- Don't know/unsure

5.18. Outside of your SA, which stakeholders were notified of the Incident?

Entity	Yes	No
FNS	O	O
U.S. Department of Homeland Security	O	O
County agencies	O	O
General public	O	O
Affected SNAP applicants	O	O
Affected SNAP recipients	O	O
Other (Specify)	O	O

5.19. We are interested in understanding the extent to which your SA's application and recertification procedures meet the safeguarding requirements specified in FNS Handbook 901 and FNS regulations and policy memos. Please give us your best assessment of whether your SA's statewide security plan incorporates safeguards associated with administering SNAP. SELECT ONE RESPONSE PER ROW.

Safeguards	Meeting Requirements, with Room for Improvement	Meeting Requirements	Especially Successful at Meeting Requirements
Masking[93] PII during data entry	○	○	○
Implementing time-out features on eligibility system screens containing PII	○	○	○
Secure delivery of SNAP benefits via EBT	○	○	○
Matching PII to other data sources for eligibility determination	○	○	○
Matching PII to other data sources for program integrity purposes	○	○	○

Section 6. Maintenance and Storage of PII. Suggested respondents for this section include: Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person].

Questions in this section are about your SA's operations associated with the maintenance and storage of PII, including questions about the safeguards your SA has implemented to prevent unauthorized physical access and the encryption methods used to safeguard PII when it is stored.

[*Branching Language Displayed for County-Administered States*: Questions in this section are about your SA's statewide requirements associated with the maintenance and storage of PII, including questions about the safeguards your SA has implemented to prevent unauthorized physical access and the encryption methods used to safeguard PII when it is stored.]

6.1 Which of the following safeguards has your SA implemented to prevent unauthorized physical access to stored SNAP PII? SELECT ALL THAT APPLY.

- ☐ Conducting regular risk assessments of a facility's physical resources
- ☐ Identifying critical areas within a facility for implementing physical safeguards (such as areas containing system hardware or software)
- ☐ Assessing risk among supporting services (e.g., electrical power); backup media; and other elements required for system operations
- ☐ Conducting regular onsite and offsite backups of stored data
- ☐ Securely disposing of data after established archiving or retention periods have passed
- ☐ Implementing facility-wide security measures on the basis of the level of risk to physical resources

[93] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

- ☐ Regularly reviewing the list of persons with physical access to SNAP PII
- ☐ Periodically reviewing physical safeguards for effectiveness
- ☐ Periodically reviewing reports and documents that can be printed with PII
- ☐ Other. Please specify: ____
- ☐ Don't know/unsure

6.2. Which encryption methods are used by your SA to safeguard data when they are stored or when the data are "at rest"? SELECT ALL THAT APPLY.

- ☐ Software-based encryption
- ☐ Hardware-based encryption
- ☐ SA uses another encryption method to safeguard data when they are stored or at rest. Please specify:_____
- ☐ SA does not currently use encryption methods for data that are stored or at rest
- ☐ Don't know/unsure

Section 7. Data Sharing and Transfer of PII. Suggested respondents for this section include: Data Analyst

Questions in this section ask about your SA's operations associated with sharing and transferring PII. The following questions ask about the entities that PII is shared with and the processes your SA uses to facilitate data sharing.

7.1. Does your SA share or transfer data that includes PII to the following entities?

Entities	Yes	No	Don't Know/ Unsure
EBT contractors	○	○	○
State education agencies or school districts	○	○	○
Other agencies in the State, such as those administering Medicaid, TANF, WIC, child care, and child support programs	○	○	○
Federal entities, such as Social Security Administration databases, National Directory of New Hires	○	○	○
Law enforcement agencies	○	○	○
Research entities (universities, government contractors, etc.)	○	○	○
Other entities (Specify)_____	○	○	○

7.2. How are data files or information containing SNAP PII transferred to requesting agencies? SELECT ALL THAT APPLY.

- ☐ Direct access to the SNAP system (such as application-to-application access) for approved users
- ☐ Password encrypted files
- ☐ Direct email
- ☐ Fax
- ☐ SFTP sites
- ☐ Physical storage devices (CDs, USB drives, etc.) with requested information

- ☐ Other. Please specify:____
- ☐ Don't know/unsure

7.3. Once the data file(s) created by your SA are sent to the requesting agency, what does your SA do with the created data file(s)?

- o The file is destroyed immediately after the match is completed.
- o The file is kept for a specific amount of time before being destroyed.
- o The file is never destroyed.
- o Other. Please specify:_____
- o Don't know/unsure

7.4. Which encryption methods are used by your SA to transmit PII data? SELECT ALL THAT APPLY.

- ☐ Software-based encryption
- ☐ Hardware-based encryption
- ☐ My SA does not currently use encryption methods when transmitting PII data.
- ☐ Don't know/unsure

7.5. On occasion, SAs may need to share SNAP PII with law enforcement agencies. How does your SA respond to law enforcement requests for PII?

- o SNAP PII is shared after law enforcement agencies provide the name of a SNAP recipient.
- o SNAP PII must be shared with law enforcement agencies if the recipient is a fleeing felon and the law enforcement agency provides a written request and the name of the SNAP recipient.
- o SNAP PII is shared after law enforcement agencies provide other information. Please specify: _____
- o We do not share data with law enforcement (unless directed to do so via a court order)
- o Don't know/unsure

Section 8. Opportunities and Challenges Suggested respondents for this section include: SA Director, Chief Information Security Officer from your agency or another central state agency [or an individual designated by that person]and Data Analyst.

Questions in this final section ask about your SA's opportunities and challenges for safeguarding PII. The following questions ask about your level of satisfaction with your SA's approach to safeguarding PII, possible gaps in its approach, and safeguarding practices at another agency or an external organization that you think would have value for other SAs.

8.1. How would you rate your level of satisfaction with your SA's approach to the following domains for safeguarding PII? SELECT ONE RESPONSE PER ROW.

Safeguarding Domains	Very Satisfied	Satisfied	Neither Satisfied nor Dissatisfied	Dissatisfied	Very Dissatisfied	Don't Know/Unsure
Personnel Policies and Procedures: Approaches used to ensure that staff working with PII have met the requisite requirements to access data at approved security levels and receive regular security training and education	○	○	○	○	○	○
Security Policies and Procedures: Approaches for implementing a robust security plan; securing PII across hardware, software, and systems; and regularly assessing risk and vulnerabilities and performing security testing	○	○	○	○	○	○
Program Operations: Safeguards associated with administering SNAP such as masking[94] or time-out features, using secure data systems to process information, secure delivery of SNAP benefits via EBT, and protected matching of PII to other data sources for eligibility determination or program integrity purposes	○	○	○	○	○	○

[94] Hover to read the following definition: "Masking is the process of hiding sensitive data with modified content (i.e., characters or other data). For instance, Social Security Numbers may be masked by replacing the first five digits with an asterisk and only showing the last four digits."

8.2. Which of the following, if any, would your SA consider as possible gaps in its approach to safeguarding PII? SELECT ALL THAT APPLY.

- ☐ Lack of resources for SNAP administration overall
- ☐ Difficulty of hiring staff with cybersecurity backgrounds
- ☐ Lack of or inadequate training on PII
- ☐ Difficulties in monitoring system access
- ☐ Non-regular or infrequent use of penetration testing
- ☐ Auditing requirements of different agencies that either conflict or are burdensome to implement
- ☐ Need for various systems upgrades in order to adopt up-to-date security practices
- ☐ Other. Please specify:_____
- ☐ Not applicable. There are no gaps in our SA's approach.
- ☐ Don't know/unsure

8.3. Are there any safeguarding practices not yet discussed, at another agency or an external organization, that you think would have value for some or all SAs, including your own? If so, please identify the State using the practice, the programs involved (if other than SNAP), and the reason you would recommend it.

[Enter open-ended text here.]

8.4. Is there anything else you would like to share regarding safeguarding of SNAP participant PII?

[Enter open-ended text here.]

APPENDIX E: INDUSTRY EXPERT INTERVIEW PROTOCOL

The U.S. Department of Agriculture Food and Nutrition Service (FNS) has hired our firm, 2M Research (2M), to conduct a study of how States are currently protecting the personally identifiable information (PII) of individuals applying to and participating in the Supplemental Nutrition Assistance Program (SNAP). The goal of the study is to gain an improved understanding of the policies and practices that SNAP State Agencies have implemented to safeguard PII included in SNAP applications or maintained in SNAP caseload files and to identify associated best practices.

As part of this study, 2M is conducting interviews with industry experts who work closely with SNAP State Agencies regarding the protection of PII and private industry and public sector benchmarks for information security. You were recommended by the project's subject matter experts and other stakeholders as a technical expert who could provide valuable insight into the safeguards that SNAP State Agencies have implemented to safeguard PII. The interview is scheduled to last 1 hour and is composed of four sections: (1) gaps in knowledge and implementation, (2) barriers to compliance, (3) industry best practices, and (4) important supports for maintaining PII security.

Do you have any questions about the study?

Permission to Record

For this interview, we will take notes during the discussion. We would like to record the conversation so that we can ensure that our notes are accurate. The recording will only be used for research purposes, and only members of the 2M team will have access to the materials. The information that you provide will be analyzed as part of all information gathered from the industry experts participating in these interviews. In the study's final report, we will formulate general lessons and present specific insights shared by the industry experts who participated in the interviews. We will not identify you or any other industry experts by name in the final report. Do we have your permission to take notes and record this interview?

If interviewee agrees to be recorded:

> Thanks—let's get started. Now, we are going to turn on the recorder (TURN ON RECORDER). Can you please confirm that you have agreed to be recorded?

If interviewee declines:

Okay, that is not a problem. Please bear with us as we take detailed notes.

1. Our records list your title as [interviewee's title] within [interviewee's organization]. Can you please confirm this information and describe your roles and responsibilities within your organization?

2. Can you please tell us a little about your experience in working with State and/or county human services agencies to safeguard SNAP PII?

Probe: In particular, which States or counties have you worked with?

Topic 1. Gaps in Knowledge and Implementation

3. Drawing on your experience working with State and county human services agencies, what vulnerabilities and threats to PII do SNAP State Agencies most commonly encounter?

Probe: In your view, are internal or external threats a bigger issue to safeguarding PII? Why?

4. SNAP State Agencies are required to adopt a variety of safeguards to ensure PII security throughout all phases of the data lifecycle, including when data are in use, in transit, or at rest (that is—filed or archived). In your view, in what areas do SNAP State Agencies have the most difficulties in implementing the following safeguards?

[Interviewer to read each domain, pause and await response, before reading the next domain]:

Personnel Policies and Procedures: approaches used to ensure that staff working with PII have met the security requirements to access`s data at approved security levels and have received regular security training and education

Security Policies and Procedures: approaches for implementing a robust security plan; securing PII across hardware, software, and systems; and for regularly assessing risks and vulnerabilities and performing security testing

Program Operations: safeguards used in administering the SNAP program, such as masking or timeout features, using secure data systems to process information, protecting delivery of SNAP benefits via Electronic Benefits Transfer (EBT), and matching PII to other data sources

Considering the answers you just provided, in which areas are the safeguarding practices of SNAP State Agencies ***most*** in need of improvement?

Topic 2. Barriers to Compliance

6. The contexts in which SNAP State Agencies operate may contribute to inadequate levels of PII security. In your view, can you describe the degree to which the following factors affect the ability of SNAP State Agencies to safeguard PII?

- Age of the data systems
- Use of security services from vendor companies
- Lack of alignment with other State social service agencies (or other types of Federal and State Agencies) that have more advanced safeguards
- Limits to resources for IT system security development, security staff training, and/or implementing security protocols (such as those related to threat detection, incident response, and testing)
- Focus on other work that has a higher priority
- Unclear or inadequate Federal requirements and/or guidance
- Specific features of the SNAP system that involve PII, such as benefit delivery through EBT; data sharing with other Federal and State Agencies to prevent fraud and abuse; and data sharing with State education agencies to ensure that children receiving SNAP benefits receive free or reduced-price school meals.

7. Among the contextual factors we have discussed, which factor do you think poses the most significant barrier to safeguarding PII?

Probe: [*In the event that respondent is having trouble recalling the contextual factors discussed above, re-read the list of factors*]:

- Age of the data systems
- Use of security services from vendor companies
- Lack of alignment with other State social service agencies (or other types of Federal and State Agencies) that have more advanced safeguards
- Limits to resources for IT system security development, security staff training, and/or implementing security protocols (such as those related to threat detection, incident response, testing)
- Focus on other work that has a higher priority
- Unclear or inadequate federal requirements and/or guidance
- Specific features of the SNAP system that involve PII, such as benefit delivery through EBT; data sharing with other Federal and State Agencies to prevent fraud and abuse; and data sharing with State education agencies to ensure that children receiving SNAP benefits receive free or reduced-price school meals.

Topic 3. Industry Best Practices

8. To what extent do the safeguards and security benchmarks used by SNAP State Agencies differ from those used in private industry?

Probe: Are there particular safeguards practiced by SNAP State Agencies that could be improved if they were more in line with industry best practices?

Probe: Does your organization have a set of national best practices that it follows and would recommend to SNAP State Agencies?

9. The information systems containing SNAP PII data may be guided by an array of security requirements established by Federal agencies (such as FNS Handbook 901, NIST guidelines, HIPAA, CMS MARS-E). In addition to these requirements, are there industry best practices that SNAP State Agencies should consider implementing for the following processes?

- Personnel security (restricting access to approved personnel)
- Information collection
- Information processing (both automated and manual)
- Information transmission and dissemination
- Information storage
- Information destruction (after an established period of time)

10. SNAP State Agencies typically operate under considerable resource constraints. Given the need to consider associated costs and feasibility of implementation, are there critical industry best practices that you would recommend SNAP State Agencies consider implementing?

Probe: If funding and implementation constraints didn't exist, what would be the "ideal" set of safeguards that SNAP State Agencies should pursue?

Probe: Are there safeguarding practices implemented by States that have limited utility and could be dropped or removed in consideration of resource constraints?

Topic 4. Important Supports for Maintaining PII Security

11. Based on your experience, what safeguarding best practices that are currently in use by the private and/or public sectors that could be valuable to SNAP State Agencies?

[*Interviewer to read each response option, pause and await response, before reading the next response option*]:

- Personnel policies and procedures
- Security policies and procedures
- Program operations
- Other safeguarding practices not previously mentioned

12. For each of the domains mentioned above, what other supports or resources would you deem critical for SNAP State Agencies in maintaining PII security?

13. Are there SNAP State Agencies that you would deem as leaders in safeguarding PII? If so, which ones?

Probe: What would you consider to be the primary reasons for identifying these SNAP State Agencies as leaders?

14. We will be conducting additional interviews with industry experts. Are there particular experts in the following areas whom you would recommend we contact for an interview?

- Information Technology and SNAP
- SNAP data collection and management
- Privacy protection legislation
- Preventing employee fraud
- Program integrity
- Privacy or security training for program or IT staff

15. Would you like to share any other pertinent information or additional thoughts?

Web Survey_FINAL_Revised.docx

APPENDIX F: SNAP STATE AGENCY LEADERS IN SAFEGUARDING PII: INTERVIEW PROTOCOL

The U.S. Department of Agriculture Food and Nutrition Service (FNS) has hired our firm, 2M Research (2M), to conduct a study to examine how States are currently protecting the personally identifiable information (PII) of individuals applying to and participating in the Supplemental Nutrition Assistance Program (SNAP). The goal of the study is to gain an improved understanding of the policies and practices that SNAP State Agencies have implemented to safeguard PII included in SNAP applications or maintained in SNAP caseload files and to identify associated best practices.

As part of this study, 2M is conducting telephone interviews with SNAP State Agencies that have been identified as leaders in safeguarding PII. We greatly appreciate your responses to the web survey of all SNAP State Agencies, which helped inform the selection of your agency for participation in this interview. The interview is scheduled to last 1 hour and is composed of three sections: (1) experiences in protecting PII, (2) lessons learned, and (3) on-the-ground insights for improving PII practices.

Do you have any questions about the study?

Permission to Record

For this interview, we will take notes during the discussion. We would like to record the conversation so that we can ensure that our notes are accurate. The recording will only be used for research purposes, and only members of the 2M team will have access to the materials. The information your agency provides will be analyzed as part of all information gathered from the SNAP State Agencies participating in these interviews. In the study's final report, we will formulate general lessons and present specific examples of experiences, lessons learned, and insights from each SNAP State Agency that participated in the interviews. We will not identify your agency or any other SNAP State Agencies by name in the final report. Do we have your permission to take notes and record this interview?

If interviewee agrees to be recorded:

> Thanks—let's get started. Now, we are going to turn on the recorder (TURN ON RECORDER). Can you please confirm that you have agreed to be recorded?

If interviewee declines:

Okay, that is not a problem. Please bear with us as we take detailed notes.

[*Interviewer to read the following statement for county-administered States*: Within county-administered systems, the SNAP SAs are responsible for establishing statewide safeguarding requirements in accordance with federal policies, while county-level agencies are given discretion in how to best meet or exceed the requirements set by the SNAP SA. Accordingly, this interview is primarily focused on the statewide safeguarding requirements established by your SA as opposed to the individual requirements established by county-level agencies.]

1. Our records list your title(s) as [interviewee's title] within [interviewee's agency]. Can you please confirm this information and describe your roles and responsibilities within your agency?

Probe: How long have you been in your current position?

2. We noted in our previous emails that it would be helpful for your agency to review applicable State legislation and regulations that govern the handling of PII. Can you please briefly describe the State legislation and regulations that govern your agency's handling of PII?

Topic 1. Experiences in Protecting PII

3. SNAP State Agencies, via FNS regulations and FNS Handbook 901 (*The Advance Planning Document Process*), are required to adopt a variety of safeguards to ensure adequate security of PII data throughout all phases of the data lifecycle, including when data are in use, in transit, or residing at rest. Can you please provide an overview of your agency's approach to the following safeguards?

[*Interviewer to read each domain, pause and await response, before reading the next domain*]:

> **Personnel Policies and Procedures**: approaches used to ensure that staff working with PII have met security requirements to access data at approved security levels and to receive regular security training and education
>
> **Security Policies and Procedures**: approaches for implementing a robust security plan; for securing PII across hardware, software, and systems; and for regularly assessing risks and vulnerabilities and performing security testing
>
> **Program Operations**: safeguards used in administering SNAP, such as masking or timeout features, using secure data systems to process information, protecting delivery of SNAP benefits via Electronic Benefits Transfer (EBT), and matching PII to other data sources for eligibility determination or program integrity purposes

Probe: As far as you know, how does your agency's approach to protecting PII differ from SNAP State Agencies in other States? In what ways is your agency's approach similar?

4. Are there safeguarding practices used by your agency that you would deem unique or innovative?

Probe: What makes these practices unique or innovative?

5. The contexts in which SNAP State Agencies must operate may contribute to the adequacy of PII security. To what extent has your agency encountered any of the following challenges to safeguarding PII?

- Age of the associated data systems
- Use of vendor company security services that are inadequate or outdated
- Inadequate alignment with other State social service agencies (or other types of State Agencies) that have more advanced and effective safeguards
- Limits to resources for IT system security development, security staff training, and/or implementing security protocols (such as those related to threat detection, incident response, testing, etc.)
- Focus on other work that has higher and more immediate priority
- Unclear or inadequate Federal requirements and guidance
- Specific features of the SNAP system that involve PII, such as benefit delivery via EBT; systematic data sharing with other Federal and State Agencies as required to prevent fraud and abuse; access to SNAP data by outside entities such as the Fresh EBT app; and ensuring that children receiving SNAP benefits also receive school nutrition benefits

Probe: How did your agency work to overcome these challenges?

6. In your view, are internal or external threats (coming from inside the agency versus coming from malicious actors residing outside of the agency) a bigger issue for the security of your agency's PII data? Why?

7. A recent report noted that shortfalls in resources, including inadequate budgets and lack of available cybersecurity talent, are the primary barriers to protecting PII for many State social services agencies.1 To what extent has your agency encountered these types of barriers, and has it been able to overcome them?

Probe: In the same report, outsourcing was identified as an effective solution to overcoming resource issues. To what extent has your agency used outsourcing?

Probe: In your view, has outsourcing been an effective approach to addressing resource issues?

Probe: In your view, are there any particular challenges related to outsourcing?

8. [*If State Agency oversees or has policy responsibility for a county-administered SNAP program*] How has operating a county-administered SNAP affected your agency's safeguarding practices?

Probe: Have the safeguarding processes and procedures used by county IT or county security offices produced challenges in safeguarding PII across the State? Conversely, have these processes and procedures provided ideas for Statewide improvements?

Probe: To what extent have county agencies elected to develop their own data systems? What has been the associated impact of these external systems for safeguarding PII?

9. In the first phase of this study, the 2M team conducted exploratory discussions with FNS staff and several SNAP State Agencies. These discussions identified a preliminary set of safeguarding best practices. Your agency's survey answers noted that your agency had adopted the following safeguarding practices [*Interviewer to read the affirmative responses from the survey and ask the respondent to confirm. In the event that respondents provide a short response, the interviewer will ask the respondent to provide additional contextual information*]:

- Third-party security or vulnerability testing
- Monitoring email communications among staff
- Resting encryption
- Patch management
- Multifactor authentication
- National Institute of Standards and Technology (NIST) cybersecurity framework

Probe: [*Interviewer to list the practices that the respondent stated were not currently in use*]: Is your agency planning to adopt any of these practices within the next 5 years?

Topic 2. Lessons Learned

10. [*Remind respondent that the interview is confidential and that individual agencies will not be named in the final report*] What internal and external security threats has your agency faced related to SNAP PII data? Has your agency experienced any data breaches?

Probe: If so, can you summarize the nature of the threats or breaches and your agency's response?

11. Development of a comprehensive security plan is a central component of State efforts to protect PII. However, subject matter experts have suggested that SNAP State Agencies may find it challenging to keep their security plans up to date. To what extent has your agency struggled with updating, understanding, and/or complying with its security plan?

Probe: How did your agency work to overcome these challenges?

12. What are the key lessons that your agency has learned in regard to safeguarding PII? What has worked well, and what hasn't worked well?

13. From a national perspective, in which areas are the PII safeguarding practices of SNAP State Agencies most in need of improvement?

Probe: What suggestions would you have for FNS and other SNAP State Agencies on improving safeguarding practices?

Topic 3. On-the-Ground Insights for Improving PII Practices

14. As we noted earlier, your agency was identified by other stakeholders as a leader in safeguarding SNAP PII. In your view, what was the process, including the key steps, for your agency to achieve a high level of success in safeguarding PII?

15. Given the need to consider associated costs and feasibility of implementation, what are the critical best practices that you would recommend SNAP State Agencies implement?

Probe: If funding and implementation constraints didn't exist, what would be the "ideal" set of safeguards that SNAP State Agencies should pursue?

Probe: Are there safeguarding practices implemented by your SNAP State Agency that have limited utility and could be dropped or removed in consideration of resource constraints?

16. Are there any safeguarding practices not yet discussed, which are used at another agency or an external organization, that you think would have value for SNAP State Agencies, including your own? If so, please identify.

Probe: Who are the agency or organizational contacts who could provide information about these practices?

17. Are there SNAP State Agencies in other States that you would consider leaders in safeguarding PII? If so, which ones?

Probe: Why would you consider these other SNAP State Agencies to be leaders?

18. Is there any other information that you'd like to share?