APPENDIX B.1 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 [DATE]. 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.

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[1]).

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**[2] dedicated to protecting SNAP PII?

- o System security professionals are located within the agency that administers the SNAP program (often along with other programs)
- o Systems security professionals are located within another state agency (such as a Department of Technology Services or an Office of the Chief Information Officer)
- o Our agency utilizes a combination of system security professionals located within our agency and systems security professionals located within another state agency
- o 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
- Staff from a central state agency (such as the State **CIO** or **CISO**[3] Office)
- Other. Please specify:_____

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

[1] 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

[2] 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."

[3] 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."

- o Before 1990
- o 1990–1999
- o 2000–2009
- o 2010–2014
- o 2015–2019

1.4. Do you consider your main SNAP eligibility system to be a **legacy system?**[4]

- o Yes
- o 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
- o 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.

[4] Hover to read the following definition: "A current information system that uses a computing infrastructure several generations old."

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)
- 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?

- o Yes
- o No *(go to Q1.9)*
- o 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: _____
- o 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**"[5] using a combination of variables. Please specify:_____

o 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?

o None of the county offices
o A minority of county offices
o A majority of county offices
o 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: _____

[5] 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."

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

- **FISMA**[6]
- **NIST**[7] **Guidelines**
- **HIPAA**[8]
- 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)	o	o	o	o
FNS Handbook 901: The Advance Planning Document Process	o	o	o	o
7 CFR 274.5 – Record retention and forms security	o	o	o	o
7 CFR 274.8 – Functional and technical EBT system requirements	o	o	o	o
Other guidance provided by USDA, FNS State Systems Office	o	o	o	o
NIST[6] Guide to Protecting Confidentiality of PII	o	o	o	o

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

[6] 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."

[7] 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."

[8] 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."

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.

	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[9] to provide data access	o	o	o	o	o	o
Delivering regular security training and education	o	o	o	o	o	o
Other personnel policies and procedures (Specify)	o	o	o	o	o	o
Security Policies and Procedures: Approaches for implementing a robust security plan						
Securing PII across hardware systems	o	o	o	o	o	o
Securing PII across software systems	o	o	o	o	o	o
Securing PII across network systems	o	o	o	o	o	o
Regularly assessing risk and vulnerabilities	o	o	o	o	o	o
Regularly performing security testing	o	o	o	o	o	o
Developing emergency preparedness and contingency plans	o	o	o	o	o	o
Other security policies and procedures (Specify)_____	o	o	o	o	o	o
Program Operations: Safeguards associated with administering SNAP						
Masking PII[10]	o	o	o	o	o	o
Implementing time-out features on computer screens	o	o	o	o	o	o
Safeguarding PII during delivery of SNAP benefits via EBT	o	o	o	o	o	o
Matching PII to other data sources for eligibility determination	o	o	o	o	o	o
Matching PII to other data sources for program integrity purposes	o	o	o	o	o	o
Securely destroying PII data that are no longer used	o	o	o	o	o	o
Other program operations (Specify) _____	o	o	o	o	o	o

[9] 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."

[10] 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

o 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)**[11] or another similar risk planning tool to identify tasks that need to be accomplished?

o Yes
o No
o 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	o	o	o	o
Complying with the system security plan	o	o	o	o
Testing or validating the system security plan	o	o	o	o
Updating the system security plan	o	o	o	o
Other (Please specify) _____	o	o	o	o

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

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]

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:_____
- o Don't know/unsure

3.2. How are **role-based security levels**[12] 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:_____

[12] 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	o	o	o
Conducting personnel background checks	o	o	o
Using role-based security levels to provide data access	o	o	o
Delivering regular IT security training and education	o	o	o

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)	o	o	o	o	o	o
Improperly secured systems with access to PII	o	o	o	o	o	o
Improperly secured mobile devices with access to PII	o	o	o	o	o	o
Unauthorized use of system resources by SA employees to access PII or unauthorized manipulation of PII data by SA employees	o	o	o	o	o	o
Unauthorized disclosure of PII data by SA employees or a trusted partner	o	o	o	o	o	o
Macro-level system failures (Specify)	o	o	o	o	o	o
Failures or decreases in the reliability of hardware	o	o	o	o	o	o
Failures or decreases in the reliability of software	o	o	o	o	o	o
Other vulnerabilities (Specify)	o	o	o	o	o	o
External Threats						
Denial of service attacks[13]	o	o	o	o	o	o
Phishing, spoofing, or pharming[14]	o	o	o	o	o	o
Introduction of malicious code (such as viruses, spyware, or malware)	o	o	o	o	o	o

[13] 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."

[14] 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)."

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)	o	o	o	o	o	o
Improperly secured systems with access to PII	o	o	o	o	o	o
Improperly secured mobile devices with access to PII	o	o	o	o	o	o
Unauthorized use of system resources by SA or county employees to access PII or unauthorized manipulation of PII data by SA employees	o	o	o	o	o	o
Unauthorized disclosure of PII data by SA or county employees or a trusted partner	o	o	o	o	o	o
Macro-level system failures (Specify)	o	o	o	o	o	o
Failures or decreases in the reliability of hardware	o	o	o	o	o	o
Failures or decreases in the reliability of software	o	o	o	o	o	o
Other vulnerabilities (Specify)	o	o	o	o	o	o
External Threats						
Denial of service attacks[15]	o	o	o	o	o	o
Phishing, spoofing, or pharming[16]	o	o	o	o	o	o
Introduction of malicious code (such as viruses, spyware, or malware)	o	o	o	o	o	o

[15] 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."

[16] 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)."

4.2. **Audit trails**[17] 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**[18]
- Type of security event experienced and its success or failure
- Names of files or applications accessed during a security event
- Other. Please specify:_____
- o Not applicable. Our SA does not use audit trails.

4.3. Has your SA implemented the following **firewall**[19] safeguards, policies, and procedures?

	Yes	No	Don't Know/Unsure
Use of a hardware-based firewall	o	o	o
Use of a software-based firewall	o	o	o
Maintaining audit records of all security-related events	o	o	o
Limiting firewall access to network security analysts or other approved users	o	o	o
Regularly reviewing the list of approved users with access to the firewall	o	o	o
Timely installation of security-related updates, fixes, or modifications that have been tested and approved	o	o	o
Other firewall safeguards, policies, and procedures	o	o	o

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

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

[17] 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."

[18] 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."

[19] 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."

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?

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

4.6. Which of the following parties, if any, does your SA use to conduct **penetration testing**[20]? SELECT ALL THAT APPLY.

- A contractor or vendor. Please specify:_____
- SA's IT or security team
- Another agency in the State. Please specify:_____
- o Not currently performed on systems containing the PII of SNAP applicants and participants
- o 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.	o	o	o
It specifies a process for protecting PII from internal and external threats until the system is restored to normal operations.	o	o	o
It is effectively integrated into the SA's security plan.	o	o	o
It provides a process for training staff in their specific response to a disaster according to their roles.	o	o	o
It specifies a process for maintaining Local Area and Wide Area Networks.	o	o	o
It specifies a process for maintaining desktops and personal computers.	o	o	o
It specifies a process for maintaining SA websites.	o	o	o
It specifies a process for maintaining distributed and mainframe systems.	o	o	o
It specifies alternative physical locations for operations in the event that original facilities are unavailable.	o	o	o
It can be activated on its own and does not require that other contingency plans be activated first.	o	o	o

[20] 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."

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[21]	o	o	o
Software-specific controls[22]	o	o	o
Network-specific controls[23]	o	o	o
Regularly assessing risk and vulnerabilities	o	o	o
Regularly performing security testing	o	o	o
Developing emergency preparedness and contingency plans	o	o	o

[21] Hover to read the following definition: "Hardware-specific controls include servers, firewalls, wireless access points, cameras, keycard readers, biometric devices, etc."

[22] Hover to read the following definition: "Software-specific controls include antivirus, access control, audit logging, Secure File Transfer Protocol (SFTP) software, VPN clients, etc."

[23] Hover to read the following definition: "Network-specific controls include IP filtering, MAC address filtering, etc."

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)	o	o
Mailing or faxing physical applications to the SA	o	o
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	o	o
Online initial application	o	o
Online recertifications	o	o
Mobile apps – initial application	o	o
Mobile apps – recertifications	o	o
Other (Specify) _____	o	o

(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	o	o	o
Telephone interviews with local office	o	o	o
Telephone interviews with call center	o	o	o
Telephone interviews with interactive voice response	o	o	o
Other (Specify) _____	o	o	o

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:_____

o Don't know/unsure

5.4. Does your eligibility system **mask**[24] Social Security numbers during data entry?

o Yes
o No

[24] 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."

- o 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: _____
- o 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)
- o 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: _____
- o 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

Method of Receipt	Yes	No	Don't Know/Unsure
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: _____
- o 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?

- o Yes
- o No
- o 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?

- o Yes
- *o* No (*go to Q5.19)*
- *o* 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)

- o 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
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 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[25] PII during data entry	o	o	o
Implementing time-out features on eligibility system screens containing PII	o	o	o
Secure delivery of SNAP benefits via EBT	o	o	o
Matching PII to other data sources for eligibility determination	o	o	o
Matching PII to other data sources for program integrity purposes	o	o	o

[25] 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."

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)	o	o
Mailing or faxing physical applications to the county agency	o	o
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	o	o
Online initial application	o	o
Online recertifications	o	o
Mobile apps – initial application	o	o
Mobile apps – recertifications	o	o
Other (Specify) _____	o	o

(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.

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

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:_____

o Don't know/unsure

5.4. Does your statewide SNAP eligibility system **mask**[26] Social Security numbers during data entry?

- o Yes
- o No
- o 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: _____
- o Don't know/unsure

Data Entry and Storage

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)
- o 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: _____
- o Don't know/unsure

[26] 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."

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

- 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 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	Yes	No	Don't Know/Unsure
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 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: _____
- o 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
- o No
- o 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?

- o Yes
- *o* No (*go to Q5.19)*
- *o* 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)

- o 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[27] PII during data entry	o	o	o
Implementing time-out features on eligibility system screens containing PII	o	o	o
Secure delivery of SNAP benefits via EBT	o	o	o
Matching PII to other data sources for eligibility determination	o	o	o
Matching PII to other data sources for program integrity purposes	o	o	o

[27] 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."

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
- 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: ____
- o 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
- o 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	o	o	o
State education agencies or school districts	o	o	o
Other agencies in the State, such as those administering Medicaid, TANF, WIC, child care, and child support programs	o	o	o
Federal entities, such as Social Security Administration databases, National Directory of New Hires	o	o	o
Law enforcement agencies	o	o	o
Research entities (universities, government contractors, etc.)	o	o	o
Other entities (Specify)_____	o	o	o

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:____
  - o 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?

- SNAP PII is shared after law enforcement agencies provide the name of a SNAP recipient.
- 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.
- SNAP PII is shared after law enforcement agencies provide other information. Please specify: _____
- We do not share data with law enforcement (unless directed to do so via a court order)
- 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	o	o	o	o	o	o
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	o	o	o	o	o	o
Program Operations: Safeguards associated with administering SNAP such as masking[28] 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	o	o	o	o	o	o

[28] 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.]