APPENDIX D.1 INDUSTRY EXPERT INTERVIEW PROTOCOL

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-XXXX. 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.

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]:

   a. ***Personnel Policies and Procedures:*** approaches used 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
   b. ***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
   c. ***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

5. 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?
   a. Age of the data systems
   b. Use of security services from vendor companies
   c. Lack of alignment with other State social service agencies (or other types of Federal and State Agencies) that have more advanced safeguards
   d. 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)
   e. Focus on other work that has a higher priority
   f. Unclear or inadequate Federal requirements and/or guidance

g. 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]:
   a. Age of the data systems
   b. Use of security services from vendor companies
   c. Lack of alignment with other State social service agencies (or other types of Federal and State Agencies)that have more advanced safeguards
   d. 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)
   e. Focus on other work that has a higher priority
   f. Unclear or inadequate federal requirements and/or guidance
   g. 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?
   a. Personnel security (restricting access to approved personnel)
   b. Information collection
   c. Information processing (both automated and manual)
   d. Information transmission and dissemination
   e. Information storage
   f. 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]:

    a. Personnel policies and procedures
    b. Security policies and procedures
    c. Program operations
    d. 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?
    a. Information Technology and SNAP
    b. SNAP data collection and management
    c. Privacy protection legislation
    d. Preventing employee fraud
    e. Program integrity
    f. Privacy or security training for program or IT staff

15. Would you like to share any other pertinent information or additional thoughts?