Information System PIA Template Guidance

The following section provides a walk through to aid PIA Authors and Reviewers in completing the HHS PIA template for information systems. It is important to note that the PIA template is built to be user-friendly. As the PIA Author completes the form, some questions may be omitted depending upon answers to previous questions. For convenience, questions that do not require an answer are automatically hidden from view. The following tutorial provides guidance for all of the PIA questions on the template, though it is possible that not all of the PIA questions will appear to the PIA author.

A.1 PIA Template for Information Systems

Question 1. OpDiv.

Answer Format	The HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST SP 800-37, NIST SP 800-122.
Appendix J Control Reference	AR-2; SE-1

Question Guidance: The answer will be pre-populated and assigned by the HSDW and based on the OpDiv who maintains responsibility for the system as identified in the HHS Enterprise Architecture.

Administration for Community Living

Question 2. PIA Unique Identifier.

Answer Format	The HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Publication 199; NIST Special Publications 800-37, NIST SP 800-122.
Appendix J Control Reference	AR-2; SE-1

Question Guidance: The answer to this question will be pre-populated and assigned by the HSDW.

Question 2.a. Name.

Answer Format	HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.

Applicable Reference	HHS Enterprise Performance Life Cycle (EPLC)
Appendix J Control Reference	N/A

Question Guidance: This field is pre-populated by the HSDW. When the PIA correlates to IT systems established through the HHS Enterprise Architecture Repository (HEAR), the system name will be based on the official name. For information collections, TPWAs, or very new systems that are not yet entered into HEAR, OpDiv SOPs will need to create a new PIA in the HSDW (see Appendix D) prior to completing the PIA. Once the system is entered, a PIA will be generated based on the new inventory item and the HSDW will pre-populate this field based on the generated inventory item (e.g., TPWA).

Question 3. The subject of this PIA is which of the following?

Answer Format	Select the radio button that corresponds to the correct answer.
Applicable Reference	OMB Circular A-130, Appendix III; NIST SP 800-37; Paperwork Reduction Act of 1995
Appendix J Control Reference	AR-2; SE-1

This question must be answered by identifying the type of information system. The provided choices are the following:

General Support System (GSS): OMB Circular A-130, Appendix III, defines general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Major Application: OMB Circular A-130, Appendix III, defines major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Minor Application (stand-alone): NIST SP 800-37, Revision 1, defines a minor application as an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Minor Application (child): Minor applications that are considered 'children' are typically included as part of a general support system but require attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Electronic Information Collection: Though typically based within a system, an electronic information collection can be an isolated collection of information (such as a survey) set apart

from normal system operations. The collection of information must have a PIA performed to determine the risks associated with the collection of the information. Electronic information collection is discussed as part of the PRA.

Unknown: If the PIA is being conducted on anything outside of these options, please describe the subject of the PIA.

Electronic Information Collection

Question 3.a. Identify the Enterprise Performance Lifecycle phase of the system.

Answer Format	Enter text in the text field.
Applicable Reference	HHS OCIO IT Policy for Enterprise Architecture; OMB Circular A-130, OMB M-05-23; HHS Enterprise Performance Lifecycle, July 18, 2012.
Appendix J Control Reference	AP-2; AR-1

Question guidance: The drop-down menu provides a list of each phase of the HHS EPLC. A PIA must be conducted before developing or procuring information technology that collects, maintains, or disseminates personal information in identifiable form. For additional information regarding the HHS EPLC, please see http://www.hhs.gov/ocio/eplc-lifecycle-framework.pdf. Section two also includes a discussion of the intersection between the HHS EPLC and the PIA process.

Planning Phase. The need for the information collection has been documented and is required under the Older American Act (OAA). The project charter (i.e., formal authorization of the project, and describes the business need for the project and the product to be created by the project) was approved as part of the FY 2014 Concept paper for ACL's Office of Performance and Evaluation. Approval of the Concept Paper "formally approved and funded the project". The acquisition process included ensuring that the contractor has a Risk Management Plan.

Question 3.b. Is this a FISMA reportable system?

Answer Format	Select the radio button that corresponds to the correct answer.
Applicable Reference	E-Government Act of 2002; OMB Circular A-130, Paperwork Reduction Act of 1995; Clinger-Cohen Act of 1996
Appendix J Control Reference	AR-2; SE-1

Question guidance: FISMA requires that all agencies maintain a system inventory, which is assessed and protected. OMB requires quarterly and annual reporting on the PIA status of the HHS system inventory as reported under FISMA. Many OpDivs have IT system inventories that reflect their FISMA-reported system inventory. However, because some OpDivs do not have matches and Departmental policy requires a PIA for all systems (whether FISMA-reportable or not), some systems will not be FISMA-reportable. Business and system owners should

collaborate with OpDiv SOPs and the CISO to validate this answer is correct. It is important this answer is correct to allow for accurate reporting of metrics to OMB.

No, this is not a FISMA reportable system.

Question 4. Does the system include a Website or online application available to and for the use of the general public?

Answer Format	Select the radio button that corresponds to the correct answer.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	TR-3; UL-2

Question Guidance: The answer to this question should be "Yes" for a system that hosts a website or an online application that provides readability and interaction with the general public and does not meet the exceptions listed in OMB M-03-22. If the system does not host a website or if it does host a website and meets the exceptions/exclusions listed from OMB M-03-22, then indicate a "No" response. For a list of exceptions/exclusions, see http://www.whitehouse.gov/omb/memoranda_m03-22/, Section III, Part C. If PII is collected through a website, several federal requirements must be met as found in OMB M-10-22 and OMB M-10-23.

Note: Intranet sites and sites for grantees should select "no."

No. There will be no website associated with this data set.

Question 5. Identify the operator.

Answer Format	The HSDW will pre-populate this field if known. If an answer is not provided, please provide an appropriate response.
Applicable Reference	HHS Information Security and Privacy Policy; E-Government Act of 2002; OMB M-03-22
Appendix J Control Reference	AR-2; SE-1

Question guidance: The operator of the system must either be an agency of HHS or a contractor point of contact. The operator is defined as when the Department or contractor uses the system to perform a Department function and/or maintains and upgrades the infrastructure of the system. For FISMA-reportable systems, the HSDW maintains this information and will pre-populate the answer.

The contractor collecting the consumer-level data is Westat. They will collect and store the data, including PII during the development of the system. They will remove PII once the system is complete and before submitting it to ACL at the end of their contract period in September 2017. While in their possession, Westat is committed to protecting the security of all study data and, in particular, the protection of personally identifiable information (PII) that respondents provide. They will assure respondents that their identities and the data they provide will be kept private as allowable under the law, will be used only for the purposes explained to them, and will not be linked to other data, except for research purposes. Westat will take the following precautions to ensure the privacy and anonymity of all data collected:

- *All Westat project staff, including recruitment specialists, telephone interviewers, research analysts, and systems analysts, will be instructed in the privacy requirements of the survey and will be required to sign statements affirming their obligation to maintain privacy;*
- *Only Westat staff who are authorized to work on the NFCSP Caregiver Outcome Evaluation have access to client contact information, completed survey instruments, and data files.*
- *Data files that are delivered to ACL will contain no personal identifiers for survey respondents; and*
- *Analysis and publication of survey findings will be in terms of aggregated statistics only.*

Question 6. Point of Contact

Answer Format	Enter text into the text fields. All text fields must be addressed for the answer to be complete.
Applicable Reference	E-Government Act of 2002; OMB M-03-22
Appendix J Control Reference	AR-2; SE-1

Question guidance: The operator POC is the person to who questions about the system and the responses to this PIA may be addressed. A complete answer must include the POC title, name, organization, e-mail, and phone number.

The point of contact is Susan Jenkins, Social Science Analyst with the US Department of Health and Human Services (HHS), Administration for Community Living (ACL), Center for Policy and Evaluation, Office of Performance and Evaluation. She can be contacted at: Susan.Jenkins@ACL.HHS.Gov or 202.795.7369.

Question 7. Is this a new or existing system?

Answer Format	The HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.
Applicable Reference	E-Government Act of 2002; OMB M-03-22

Appendix J Control Reference	AR-2; SE-1

Question guidance: The HSDW will pre-populate this information. If the system is a new system, the PIA Author should work within the EPLC process to develop the document during the initiation phase of the system. The PIA may indicate that a SORN is required as well. If the system is an existing system, subsequent questions within the PIA will ask the reason for reviewing and updating the PIA.

This is a new system. A SORN is not required because data will not be retrievable by or retrieved by PII.

Question 8. Does the system have Security Authorization (SA)?

Answer Format	The HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.
Applicable Reference	FIPS Publication 199; NIST SP 800-37, NIST SP 800-39, NIST SP 800-53A, NIST SP 800-115, NIST SP 800-137; E-Government Act of 2002; OMB M-03-22
Appendix J Control Reference	AR-2; SE-1

Question guidance: A security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls. For most IT systems, particularly those that are FISMA-reportable, the HSDW should provide the appropriate answer.

No, this is not a FISMA reportable system.

Question 8.a. Date of Authorization.

Answer Format	The HSDW will pre-populate this field. If an answer is not provided, please provide an appropriate response.
Applicable Reference	FIPS Publication 199; NIST SP 800-37, NIST SP 800-39, NIST SP 800-53A, NIST SP 800-115, NIST SP 800-137; E-Government Act of 2002; OMB M-03-22
Appendix J Control Reference	AR-2; SE-1

Question guidance: If the answer to Question 8 is 'Yes,' then Question 8.a. will ask for the PIA Author to indicate the date of the SA&A. If the answer to Question 8 is "No," then Question 8.a. will ask the PIA Author to indicate the planned date that the information system will receive authorization. For most IT systems, particularly those that are FISMA-reportable, the HSDW should provide the appropriate answer.

Question 9. Indicate the following reason(s) for updating this PIA. Choose from the following options.

Answer Format	Select the box that corresponds to the correct answer(s). If 'Other' is indicated then enter text into the text field to describe what the additional reason(s) for updating the PIA.
Applicable Reference	E-Government Act of 2002; OMB M-03-22, OMB M-05-08, OMB M-10-23
Appendix J Control Reference	AR-2; AR-6; AR-7; DI-1; SE-1

Question guidance: Department PIAs must be reviewed annually. OMB M-03-22 provides common examples of major changes that require an updated PIA. It is important to note that the major changes identified in OMB M-03-22 are not an exhaustive list. Changes to the way in which PII is generally collected, maintained, used, and shared may require that the system PIA be updated to determine new risks associated with PII in the system.

Not applicable this is a new PIA

Question 10. Describe in further detail any changes to the system that have occurred since the last PIA.

Answer Format	Enter text into the text field.
Applicable Reference	E-Government Act of 2002; OMB M-03-22, OMB M-05-08, OMB M-10-23
Appendix J Control Reference	AR-2; AR-6; AR-7; DI-1; SE-1

Question guidance: Changes, even if not considered major, occur all the time to systems. The answer should provide a detail of changes whether it relates to business partners, types of PII collected, and administration of the system.

Not applicable this is a new PIA

Question 11. Describe the purpose of the system.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-05-08, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; AR-7; DM-2, TR-1

Question guidance: The description of the purpose of the system is one of the most important sections of the PIA. A thorough and clear description of the purpose of the system gives the reader the appropriate context to understand the responses to the remaining questions asked in the PIA. Is this a human resources system? Is this a system to disperse benefits? This should be

described in clear, simple prose. Often budget documents, such as Exhibit 300s, provide effective overviews of the system.

This system is a data collection by the Administration for Community Living's (ACL) contractor under a contract to conduct an outcome evaluation of the Title III-E National Family Caregiver Support Program (NFCSP) (contract # HHSP23320095655WC_HHSP23337027T). The Older Americans Act (OAA) Title III-E National Family Caregiver Support Program (statutory authority is contained in Title II section 205(a)(2)(A), and Title III sections 373 of the Older Americans Act (OAA) (42U.S.C. 3032), as amended by the Older Americans Act Amendments of 2006, P.L. 109-365) is part of comprehensive home-and community-based services. Older Americans Act Title III, Part E provides grants to States and Territories under approved State Plans for the establishment and operation of the Program. Section 373 authorizes grants to provide a multifaceted system of support services to family caregivers and grandparents or older family members caring for related children. Supportive services include five core services for family caregivers, including:

- *Information to caregivers about available services;*
- *Assistance to caregivers in accessing supportive services;*
- *Individual counseling, support groups, and caregiver education/training* to assist caregivers in making decisions and solving problems relating to their caregiving roles;*
- *Respite care* to temporarily relieve caregivers from their caregiving responsibilities; and*
- *Supplemental services, on a limited basis, to complement the care provided by caregivers.*

** The outcome evaluation described here will focus on these services.*

The authorizing legislation for the data collection is found in Title II of the OAA. The requirements stipulated under section 206(a, c) directs ACL to "…measure and evaluate the impact of all programs authorized by this Act…" This evaluation will be used by ACL to assess program effectiveness, as measured by the program's effects on a variety of important outcomes, including caregiver financial, emotional, and physical stress, and, ultimately, helping elderly people avoid institutionalization. The data collected during the evaluation is essential to ACL for meeting the needs of a rigorous evaluation of the impact of the Title III-E Program. There is currently no other national effort that addresses the research objectives of the proposed study. The resulting information will be critical to federal policymakers and will assist all levels of the aging network as ACL attempts to maximize efficiency and service. Data will be used by ACL staff to improve program operations, provide improved technical assistance and guidance to grantees and service providers, and to support mandated agency reporting to congress and through annual reports.

More specifically, the outcome evaluation aims to assess a series of target outcomes by comparing NFCSP participants and their care recipients to non-participants and their care recipients. It will ascertain the impact of services on the ability of caregivers to continue to provide caregiving as needed, and include, for example, an examination of the relationship between the self-reported measures of physical and mental well-being of program participants and the amount of caregiver services received.

Question 12. Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; DM-2, TR-1

Question Guidance: Identify and list the type of information that is collected and stored in the system. As the parenthetical indicates, this answer is not meant to get into detail about the PII, but to provide a general context for additional information. Exhibit 300s often provides a good overview of the type of information collections applicable to the system.

The data will be collected through telephone during an initial contact with two follow ups 6 months apart. The surveys used to collect the individual-level data can be viewed at http://www.aoa.gov/Program_Results/Outcome_Evaluation_Survey.aspx

Question 13. Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; AR-7; DM-2, TR-1

Question Guidance: Identify and list the type of information that is collected and stored in the system. While subsequent PIA questions will get into the specific data fields, if there is PII, but this question should provide an indication of the kinds of information and with some specificity. For example, this would be the appropriate question to describe the information that the system maintains, such as human resource data used to process salary and employment benefits. Later questions will address whether this is PII and the specific data elements. Exhibit 300s often provides a good overview of the type of information collections applicable to the system.

The data will be collected through telephone during an initial contact with two follow ups 6 months apart. The surveys used to collect the individual-level data can be viewed at http://www.aoa.gov/Program_Results/Outcome_Evaluation_Survey.aspx

Question 14. Does the system collect, maintain, use, or share PII?

Answer Format	Select the radio button that corresponds to the correct answer.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; DM-2, TR-1

Question guidance: The answer to this question should identify whether PII is collected, maintained, used, or shared within the system. OMB M-07-16 defines PII as information that can be used to distinguish or trace an individual's identity such as their name, SSN, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Please refer to section 1.3 for a complete discussion of the definition of PII.

This is the crucial question of the PIA and the PIA Author and Reviewer must first accurately determine if PII is present before determining whether PII handling and PII security practices are appropriate. PIA authors often feel hesitant about identifying that their system maintains PII out of fears that maintaining PII necessarily requires very strong (expensive) security controls. However, this is not always the case, and there are opportunities throughout the PIA to clearly convey the low confidentiality if necessary.

Through a contractor, the system collects PII in order to link records across the three data collections and to contact respondents. Name, address including zipcode, and telephone number will be collected for service recipients and members of the matched comparison group and used to contact respondents for collection and to send their gifts for participation. Once contacted, participants' name, address, and telephone number will be deleted from the system. Once the data set is complete zipcode is the only PII that will remain in the system.

Question 15. Indicate the type of PII that the system will collect or maintain.

Answer Format	Select the box that corresponds to the correct answer(s). If 'Other' is indicated then enter text into the text field to describe what the additional reason(s) for updating the PIA.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; DM-2, TR-1

Question guidance: Please indicate the category of PII shared or disclosed. If the category of personal information is not listed, please check 'Other' and identify the category in the text field.

The system will collect the following PII:

- *Full name*
- *Mailing Address including zipcode*
- *Telephone number*

Zipcode is the only PII that will be maintained in the system

Question 16. Indicate the categories of individuals about whom PII is collected, maintained, or shared.

Answer Format	Select the box that corresponds to the correct answer(s). If 'Other' is indicated then enter text into the text field to describe what the additional reason(s) for updating the PIA.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; DM-2, TR-1

Question Guidance: Please indicate the individuals about whom PII is collected, maintained within the system, and whom the information is shared with. HHS considers grantees and principal investigators to be business partners.

Zipcode, name, address and telephone number will be collected from service recipients and their care recipients and members of the matched comparison group and their care recipients.

Question 17. How many individuals' PII is in the system?

Answer Format	Select the appropriate size from the drop-down menu.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M 03-22; OMB Circular A-130, FIPS Publication 199; NIST SP 800-37, NIST SP 800-122
Appendix J Control Reference	DM-1; SE-1

Question guidance: This question seeks to define the number of individuals for which PII is collected and maintained in the system. Understanding the number of individuals within the system is critical to determining the privacy protections that must be implemented for the system. In addition, understanding the number of individuals within the system can assist with determining the degree of breach response should the system experience a loss or exposure of PII.

The goal for the evaluation is to collect consumer level data from a total of 2,500 caregivers and 2500 care recipients from whom zipcode, name, address, and telephone number will be collected The final data set will only contain zip code for these 5,000 people.

Question 18. For what primary purpose is the PII used?

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control	AP-2; AR-2; AR-4; AR-7; DM-2, TR-1

Reference	

Question guidance: Please indicate the reason the system collects, maintains, and shares PII. The purpose should be consistent with the legal authority stated within the SORN (if the Privacy Act of 1974 is applicable), which refers to the notice that describes the purpose of the system, the legal authority to collect information, the categories of information collected, maintained, retrieved, and used within a set of records, the categories of individuals for whom the information is collected, to whom the information can be disclosed, etc.

This could include, but is not limited to: name, date of birth, mailing address, telephone number, SSN, e-mail address, zip code, facsimile number, mother's maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/ license number, vehicle identifier including license plate, marriage record, civil or criminal history information, device identifiers and serial numbers, uniform resource locators (URLs), education record, internet protocol addresses, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic. If the system creates information (for example, a score, analysis, or report), please list the information that the system creates. If the system receives information from another system, such as a response to a background check, describe what information is returned. This answer should be as specific as possible.

System Purpose- This integrated evaluation of the Title III-E program includes two major research components: (1) a process study to examine strategies and activities at all levels of the Aging Network—(State Units on Aging (SUAs), Area Agencies on Aging (AAAs), and Local Service Providers (LSPs)); (2) a client outcomes study with an assessment of caregiver stress, well-being, and ability to continue providing care. The data collected during the evaluation is essential to ACL for meeting the needs of a rigorous evaluation of the impact of the Title III-E Program. There is currently no other national effort that addresses the research objectives of the proposed study. The resulting information will be critical to federal policymakers and will assist all levels of the aging network as ACL attempts to maximize efficiency and service. It is the data related to goal two that will reside in this system, but the other goals are presented here for context in understanding how the individual-level data fits into the larger research project. The outcome evaluation will be analyzed to determine the extent to which NFCSP clients as compared with non-clients are able to continue providing care in the community.

The study aims to assess a series of target outcomes by comparing NFCSP participants to non-participants. It will ascertain the impact of services on the ability of caregivers to continue to provide caregiving as needed, and include, for example, an examination of the relationship between the self-reported measures of physical and mental well-being of program participants and the amount of caregiver services received.

The data from both parts of the research will be combined to answer questions about which types of structures and approached are correlated with the most positive client-level outcomes. This information will allow ACL to provide improved guidance to grantees and service providers to help them improve their operations and, ultimately, improve the health and well-being of older Americans.

The specific purpose of the PII is described below:

- *Contact information (e.g., name, address and telephone number, zipcode) will be used to contact respondents. Once the final contact is made at the 12 month follow up, this information, with the exception of zipcode, will be removed from the system.*

Categories of information collected: The following categories of data will be collected from caregivers:

A. *Service receipt*
B. *Caregiving tasks, frequency, and intensity*
C. *Knowledge and use of formal services available*
D. *Caregiving satisfaction and other aspects*
E. *Impact of caregiving (health, social, and financial)*
F. *Delayed institutionalization and continued caregiving*
G. *Caregiver and household demographics*
H. *Caregiver health status and healthcare utilization*
I. *Caregiver support of recipient's demographics, health, and function*

Data about quality of life and quality of caregiving will be collected from care recipients.

The surveys used to collect the individual-level data can be viewed at http://www.aoa.gov/Program_Results/Outcome_Evaluation_Survey.aspx

Categories of individuals from whom the information is collected: Information will be collected from a random sample of individuals at selected AAAs who receive either respite care or individual counseling, support groups, and caregiver education/training during the data collection period. Data will also be collected from a matched set of individuals who did not receive either service. This group will be identified through contacting other OAA service recipients and requesting permission to contact their caregivers. In addition, caregivers will be asked for permission to contact their care recipients.

To whom the information can be disclosed The PII will only be disclosed to the research team.

Question 19. Describe the secondary uses for which the PII will be used (e.g., testing, training, or research).

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-2; AR-2; AR-4; AR-7; DM-2, TR-1

Question guidance: Please indicate any secondary uses of the information that is collected, maintained, or shared by the system. The secondary purposes could include data for research purposes, statistical analysis, or information that is used to compare within another system.

There is no secondary function for the PII.

Question 20. Describe the function of the SSN.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-aDM-2, TR-1

Question guidance: If an SSN is collected within the system, please describe the way in which the SSN is used. The answer should clearly indicate the use of the SSN through all procedures and processes for which it is involved.

Not applicable. SSN will not be collected.

Question 20.a. Cite the legal authority to use the SSN.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-aDM-2, TR-1

Question guidance: OMB M-07-16 requires agencies to review and eliminate (where applicable) uses of SSNs. The OMB guidance came about as a result of the President's Identity Theft Task Force, which found that the ubiquitous nature of SSN use, and the fact that it is a key component of credit applications, made it a common target of identity thieves. Generally speaking, unless the SSN is required under a legal authority, the system should take steps to remove the SSN. Budget documentation often provides useful references to legal authorities establishing the program or system.

Not applicable. SSN will not be collected.

Question 21. Identify legal authorities governing information use and disclosure specific to the system and program.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-1; DM-2, TR-1

Question guidance: Please indicate the legal authority for the system that provides for the use and disclosure of the PII within the system.

If the SSN is used and a legal authority is cited, it may be an appropriate legal authority for a larger set of PII. Budget documentation often provides useful references to legal authorities establishing the program or system. These same legal authorities may also address appropriate or necessary information for meeting the business function set forth in the legal authority.

Note: the Privacy Act of 1974 is not a legal authority for collecting information. If a system is subject to the Privacy Act of 1974 because it retrieves records by a personal identifier, then certainly the Privacy Act of 1974 governs the handling of the information. The Act provides certain standards and codifies certain acceptable information practices, but it does not grant any system specific authority to collect information.

Is this 'not applicable' because the final system will not contain PII. But, the authority to collect PII and use it in the development of the system is provide through the Older Americans Act (OAA).

Statutory authority is contained in Title II section 205(a)(2)(A), and Title III sections 373 of the Older Americans Act (OAA) (42U.S.C. 3032), as amended by the Older Americans Act Amendments of 2006, P.L. 109-365) is part of comprehensive home-and community-based services. Title III, Part E provides grants to States and Territories under approved State Plans authorizes grants to provide a multifaceted system of support services to family caregivers and grandparents or older family members caring for related children. The authorizing legislation for the data collection is found in Title II of the OAA. The requirements stipulated under section 206(a, c) directs ACL to "…measure and evaluate the impact of all programs authorized by this Act, their effectiveness in achieving stated goals in general, and in relation to their cost, their impact on related programs, their effectiveness in targeting for services under this Act unserved older individuals with greatest economic need (including low-income minority individuals and older individuals residing in rural areas) and unserved older individuals with greatest social need (including low-income minority individuals and older individuals residing in rural areas), and their structure and mechanisms for delivery of services, including, where appropriate, comparisons with appropriate control groups composed of persons who have not participated in such programs. Evaluations shall be conducted by persons not immediately involved in the administration of the program or project evaluated."

Question 22. Are records on the system retrieved by one or more PII data elements?

Answer Format	Select the radio button that corresponds to the correct answer.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-1; DM-2, TR-1

Question guidance: In addition to providing insights into the functionality of a system, this question verifies the applicability of the Privacy Act of 1974. If a personal identifier such as a name or SSN retrieves information, the system is likely subject to the Privacy Act of 1974 and a SORN will be required. System owners are strongly encouraged to contact their Privacy Act of 1974 contacts to validate the applicability and status of any relevant SORNs.

No, once completed, the system will not contain PII.

Question 22.a. Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-1; DM-2, TR-1

Question guidance: If the system includes a group of records containing PII designed to be retrieved by a name or other identifier, the Privacy Act of 1974 applies to the information collection. If the Privacy Act of 1974 applies, the system requires the completion of the full PIA (all tabs must be completed) and a SORN must be cited. In the case of records pertaining to government employees and their work information, OMB M-03-22 indicates that information in identifiable form (PII) about government personnel generally is protected. In addition, NIST SP 800-53, Revision 4, Appendix J states; "Often statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations verify, in consultation with the SAOP/CPO and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes are identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIA, SORNs, and Privacy Act statements on forms organizations use to collect PII. Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII and on the contents of the notice."

No, not applicable

Question 23. Identify the sources of PII in the system.

Answer Format	Select the box(es) that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23
Appendix J Control Reference	AP-1; AP-2; AR-2; AR-4; AR-7; DM-1; DM-2, TR-1

Question guidance: Responses must be sufficiently specific to describe only those individuals whose information is collected. Individuals may, for example, be limited to recipients of specific

benefits or services, individuals requesting further information concerning a particular government function or service, or individuals subject to particular laws or regulations.

PII in the system will come directly from AAA's that provide NFCSP services, randomly selected recipients of Title III-E NFCSP services, as well as selected individuals receiving other OAA Title III services in order to construct a comparison group.

Question 23.a. Identify the OMB information collection approval number and expiration date.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; Paperwork Reduction Act of 1995; OMB M-03-22, OMB 07-16, OMB
Appendix J Control Reference	AP-1; AR-2; AR-4; DM-1; DM-2

Question guidance: The PRA focuses on increasing the efficiency of the federal government's information collection practices. The PRA specifies that CIOs shall improve protection for the privacy and security of information under their agency's control. The PRA also created the Office of Information and Regulatory Affairs (OIRA) within OMB to provide central oversight of information management activities across the federal government. Furthermore, the PRA requires agencies to receive an OMB information collection approval number (also known as an "OMB control number") for an information system, prior to using that system to collect information from any person. For more information on federal collection of information please see the Federal Collection of Information on the OMB website at www.whitehouse.gov/omb/inforeg_infocoll.

OMB PRA clearance is in process.

Question 24. Is the PII shared with other organizations?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB
Appendix J Control Reference	AP-1; AR-2; AR-4; DM-1; DM-2

Question guidance: This question seeks to determine whether PII is shared from the system to other systems or applications.

Not applicable. The PII will not be shared with other organizations.

Question 24.a. Identify with whom the PII is shared or disclosed and for what purpose.

Answer Format	Select the box that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22,

	OMB 07-16, OMB
Appendix J Control Reference	AP-1; AR-2; AR-4; AR-8; DM-1; DM-2

Question guidance: Please identify who information is shared with and provide an affirmative explanation why the information is shared, regardless of whether disclosure is on paper, electronic, or oral.

PII will not be shared outside of the research team.

Question 24.b. Describe any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; Paperwork Reduction Act of 1995; OMB-01-05; OMB M-03-22, OMB 07-16
Appendix J Control Reference	AR-7; AR-8; UL-2

Question guidance: No record contained within a SOR can be disclosed to an agency or non-federal agency for use in a computer-matching program except pursuant to a written agreement stating the security and privacy controls between the source agency and the recipient agency. For more information on the requirements of a computer data matching agreement, see OMB M-01-05.

Not applicable. The information will not be shared.

Question 24.c. Describe the procedures for accounting for disclosures.

Answer Format	Enter text into the text field.
Applicable Reference	The Privacy Act of 1974; E-Government Act 2002
Appendix J Control Reference	AR-7; AR-8

Question guidance: Describe how disclosures of PII are recorded and documented. The process of documenting disclosures can be a manual process. The specific requirements are that if you maintain PII, particularly within a Privacy Act SOR, though the Health Information Portability and Accountability Act (HIPAA) and other privacy laws require this as well, that the system maintain a record or accounting of each time it discloses information and that the individuals should be able to make a request for these records. The question seeks to find out how the system and the relevant business owners maintain this accounting. For more information see NIST 800-53, Revision 4, Appendix J, Controls AR-7 & AR-8.

As an Operating Division of HHS, Administration for Community Living (ACL), follows established HHS policies for IT Security and Privacy, including:

HHS Policy for Privacy Impact Assessments (PIA) (2009-0002.001 2/9/2009)

HHS Policy for Responding to Breaches of Personally Identifiable Information (PII), (2008-0001.003 2/09/2009)

HHS Policy for IT Security and Privacy Incident Reporting and Response (2010-0004 4/05/2010)

A comprehensive list is found at http://www.hhs.gov/ocio/policy/#Security.

Question 25. Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; OMB Circular A-130; E-Government Act of 2002; OMB M-03-22; OMB M-07-16
Appendix J Control Reference	AP-1; AP-2; AR-7; TR-1; TR-2

Question guidance: For systems that are subject to the Privacy Act of 1974 and collect information from members of the public, System Owners/Managers must post a Privacy Act notification statement at the point at which personal information is provided, or requested by the OpDiv, such as on a manual or electronic form, or on a website.

A Privacy Act notification statement should address the following criteria:

- What is the Government Authorization (Public Law, Statute, Executive Order, etc.) authorizing the information collection?
- What information is collected?
- What is the purpose of the information collection?
- What are the routine uses for disclosure of the information to others?
- Can the information be provided on a voluntary basis, or is it mandatory?
- If mandatory, what effect, if any, will there be if the information is not provided?

At the start of the survey process individuals will be read the following consent statement: In the beginning of each survey, Westat reads to respondent: "We will not report responses from a specific individual. In addition, we will not provide information that identifies individuals to anyone outside the study team, except as required by law."

As an Operating Division of HHS, Administration for Community Living (ACL), follows established HHS policies for IT Security and Privacy, including:

HHS Policy for Privacy Impact Assessments (PIA) (2009-0002.001 2/9/2009)

HHS Policy for Responding to Breaches of Personally Identifiable Information (PII), (2008-0001.003 2/09/2009)

HHS Policy for IT Security and Privacy Incident Reporting and Response (2010-0004 4/05/2010)

A comprehensive list is found at http://www.hhs.gov/ocio/policy/#Security.

Question 26. Is the submission of PII by individuals voluntary or mandatory?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; OMB Circular A-130
Appendix J Control Reference	TR-2

Question guidance: Please indicate whether the PII collected is voluntary or mandatory. Generally, speaking, a core privacy principle is that individuals should have a choice about what information they provide. Wherever possible, HHS should make the collection of the PII voluntary. However, there will be many cases where information is mandatory such as to verify identity or to grant benefits correctly. Generally speaking PII is mandatory if the individual must provide the PII to receive the services the system is designed to provide.

PII collected from individuals is voluntary. There will be no negative consequences for individuals who decline to prove any of the requested data.

Question 27. Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22
Appendix J Control Reference	IP-1

Question guidance: NIST SP 800-53, Revision 4, Appendix J, states "Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the collection or use of such PII. For example, the Federal Trade Commission's (FTC) Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and

subsequent uses of that PII. Organizational consent mechanisms include a discussion of the consequences to individuals for failure to provide PII."

To opt out respondents may verbally decline to provide their information.

Question 28. Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22
Appendix J Control Reference	IP-1; IP-2; IP-4

Question guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

PII will only be in the system for a limited amount of time. This is a onetime research project with no anticipated changes to the system during the period in which it contains PII. If such a change does occur, the research team will send a letter to respondents using the contact information collected to conduct the survey.

Question 29. Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; OMB Circular A-130; OMB M-07-16, OMB M-08-09
Appendix J Control Reference	IP-1; IP-2; IP-4

Question guidance: NIST SP 800-53, Revision 4, Appendix J, states "Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the SAOP/CPO or other official designated to receive complaints), and are easy

to use. Organizational complaint management processes include tracking mechanisms to review all complaints received and appropriately addressed in a timely manner."

As an Operating Division of HHS, Administration for Community Living (ACL), follows established HHS policies for IT Security and Privacy, including:

HHS Policy for Privacy Impact Assessments (PIA) (2009-0002.001 2/9/2009)

HHS Policy for Responding to Breaches of Personally Identifiable Information (PII), (2008-0001.003 2/09/2009)

HHS Policy for IT Security and Privacy Incident Reporting and Response (2010-0004 4/05/2010)

A comprehensive list is found at http://www.hhs.gov/ocio/policy/#Security.

Question 30. Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16
Appendix J Control Reference	AR-7; DM-1

Question guidance: OpDivs should have a system for periodic management review of the PII housed in our IT Systems. An internal system audit is an example of a process for reviewing the integrity and accuracy of data. OMB M-07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Reductions in organizational holdings of PII are consistent with the National Archives and Records Administration (NARA) retention schedules.

There is no process in place because PII will only remain in the system during the data collection phase of the evaluation. Once data collection is complete PII will be removed.

Question 31. Identify who will have access to the PII in the system and the reason why they require access.

Answer Format	Select the box that corresponds to the correct answer(s). Insert text into the corresponding box that is selected.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16

Appendix J Control Reference	AR-4

Question guidance: Please indicate the roles that have access to PII in the system along with the reason why each role needs the access to PII.

Selected members of the research team will have access to the PII or the purposed of contacting respondents for data collection. Each person will have signed a data security agreement per the requirements of the evaluation contract. In this agreement project staff pledge to maintain the protection of all information collected from the respondents and will not disclose it to anyone other than authorized representatives of the evaluation, except where otherwise required by law. Issues of data security are discussed during interviewer training.

Question 32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16
Appendix J Control Reference	AR-4

Question guidance: All Department systems should have roles and responsibilities established for each user role associated with the system. Pursuant to FISMA, all major systems, GSS, and other applications that contain sensitive data must have a SA&A completed on them. As part of the SA&A package, the System Security Plan (SSP) contains a description of user privileges that should also include a governance strategy to determine access to PII in the system.

Access to PII is based solely on position requirements. Interviewers will need respondent contact information.

Question 33. Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16
Appendix J Control Reference	AR-4

Question guidance: The Department must monitor and audit privacy controls and internal privacy policies. One aspect of monitoring and audit controls is to verify that collected PII is only provided to a user on a need-to-know basis. Reviewing the roles and responsibilities for gaining access to PII will require that individuals are authorized to access PII within the system.

While in their possession, the contractor guarantees data security. Westat is committed to protecting the security of all study data and, in particular, the security of personally identifiable information (PII) that respondents provide. They will be able to assure respondents that their identities and the data they provide will be kept in the strictest confidence, will be used only for the purposes explained to them, and will not be linked to other data, except for research purposes.

Westat, the contractor administering the survey instrument and collecting the data, has extensive experience in protecting and maintaining the privacy of respondent data collected from surveys. To ensure privacy, Westat has drawn from its experience in designing the data collection procedures incorporated in this program. In addition to the corporate Assurance of Data Security Agreement, Westat has implemented several other procedures to protect privacy of survey participants.

1. *Data is saved on secure network folders only accessible to authorized users. No data is ever stored on laptop computers. At the end of the survey, all private data is permanently deleted.*

2. *For the 11th National Survey of Older Americans Act Participants (from which the sample of NFCSP caregivers will be drawn) and for the NFCSP Outcome Evaluation, AAAs will be instructed to submit private personally identifiable client data to Westat via electronic files using the secure survey web site. This web site is written in Active Server Pages (ASP), HTML, and JavaScript and uses the industry-standard SSL (Secure Socket Layer) encryption for secure File Transport Protocol (FTP) data submissions. Agencies will receive usernames and passwords that enable their staff to sign on to the file upload utility on the web site. The passwords are created by a password generator which creates random passwords that are highly secure due to a combination of lower and upper case letters, numbers and punctuation symbols. The database containing the client survey data is not accessible via the Internet; it resides on a server inside the Westat firewall. Only Westat Data Collection Program staff members have access to the master survey database.*

3. *For AAAs that may experience problems with the survey website and wish to send client data electronically by email, we instruct the AAAs to password protect the file containing the data. Password protection of client data sent electronically by email is required not only for transmission between the AAA and Westat, but even internally within Westat. Additionally, we provide the AAAs with an email address to a secure dedicated project email box (aoasurvey@westat.com) which cannot be accessed remotely.*

4. *For the small number of AAAs which are not able to generate client records by service electronically, they can submit client information in a hard copy format (fax, FedEx, U.S. Postal Service). Hard copies of client information are stored in locked filing cabinets*

within a locked room. At the conclusion of the survey, all hard copies of client data are shredded.

5. *A secure fax machine dedicated solely to this survey is used to receive faxes from AAAs that choose to transmit their data by fax. The fax machine is located within a locked project room. AAAs that need to transmit their data by fax are asked to call to Westat staff to alert them to watch for and intercept an incoming fax. If the fax machine is busy, it does not roll over to any other fax machine.*

All respondents in this data collection effort are assured of the privacy of their answers. Respondent data are aggregated and estimates are produced and published at the both at the national level and at the geographic regional or demographic sub-group level. No individual-level data are published, nor are they accessible or provided to anyone outside the Westat Data Collection Program staff.

Question 34. Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16
Appendix J Control Reference	AR-1; AR-5

Question guidance: Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as PIA or SORN for a program or information system.

ACL staff have annual training about security and privacy. Westat, the contractor collecting these data, has significant experience recruiting and training staff to collect valid and reliable survey data. They are national leaders in the collection of sensitive data, with established procedures and processes to train and monitor staff to safeguard the respectful conduct of data collection and the security of data. Interview staff, who will collect the PII will undergo training which includes information about privacy and data security, prior to starting to collect data.

Question 35. Describe training system users receive (above and beyond general security and privacy awareness training).

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-07-16
Appendix J Control Reference	AR-1; AR-5

Question guidance: Federal guidance and Departmental policy requires annual privacy awareness training. For systems with PII, particularly systems covered by the Privacy Act of 1974, employees must receive system-specific training. Individuals must be educated about their responsibilities, such as when to encrypt and with whom and by what methods to share information. This question should address the type, frequency, and content of the training. Specific training methods may include: (i) classroom or web-based training; (ii) internal privacy program Websites; (iii) manuals, guides, and handbooks; (iv) slide presentations; (v) events (e.g., privacy awareness week, privacy clean-up day); (vi) posters and brochures; and (vii) e-mail messages to system staff.

Once the data are finalized in the system PII will be removed. Therefore there is no special training for system users related to privacy-see previous responses

Question 36. Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974, OMB Circular A-130, Federal Acquisition Regulation
Appendix J Control Reference	AR-1; AR-3; AR-4; AR-5

Question guidance: The Federal Acquisition Regulations (FAR) subpart 24.1, "Protection of Individual Privacy," states the following requirements: (a) The Act requires that when an agency contracts for the design, development, or operation of a system of records on individuals on behalf of the agency to accomplish an agency function the agency must apply the requirements of the Privacy Act of 1974 to the contractor and its employees working on the contract. (b) An agency officer or employee may be criminally liable for violations of the Privacy Act of 1974. When the contract provides for operation of a system of records on individuals, contractors and their employees are considered employees of the agency for purposes of the criminal penalties of the Privacy Act of 1974. (c) If a contract specifically provides for the design, development, or operation of a system of records on individuals on behalf of an agency to accomplish an agency function, the agency must apply the requirements of the Act to the contractor and its employees working on the contract. The system of records operated under the contract maintained by the agency and is subject to the Privacy Act of 1974. (d) Agencies, which within the limits of their authorities, fail to require that systems of records on individuals operated on their behalf under contracts be operated in conformance with the Act may be civilly liable to individuals injured as

a consequence of any subsequent failure to maintain records in conformance with the Privacy Act of 1974."

The contracting officer shall review requirements to determine whether the contract will involve the design, development, or operation of a system of records on individuals to accomplish agency functions. The contracting officer shall require that the contract work statement specifically identifies the system of records on individuals and the design, development, or operation work to be performed; and make available, in accordance with agency procedures, agency rules and regulation implementing the Privacy Act of 1974.

The contract under which these data will be collected includes the following clauses:

- *HHSAR 352.239-70 STANDARD FOR SECURITY CONFIGURATIONS*
- *HHSAR 352.239-71 STANDARD FOR ENCRYPTION LANGUAGE*
- *HHSAR 352.239-72 SECURITY REQUIREMENTS FOR FEDERAL INFORMATION*
- *TECHNOLOGY RESOURCES*

Question 37. Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-07-16; OMB Circular A-130; NIST SP 800-88
Appendix J Control Reference	AR-1; DM-1; DM-2; IP-1;

Question guidance: NARA provides retention schedules that govern the disposition of federal records containing PII. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper.

Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete SSNs if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated SORN) to inform the public of any changes in holdings of PII.

Once data collection is complete and the data are finalized, the Westat data systems will not contain PII. PII is necessary for the construction of the system and will be deleted once the system is complete. Therefore, there are no retentions schedules. As an Operating Division of HHS, Administration for Community Living (ACL), follows established HHS policies for IT Security and Privacy, including:

HHS Policy for Privacy Impact Assessments (PIA) (2009-0002.001 2/9/2009)

HHS Policy for Responding to Breaches of Personally Identifiable Information (PII), (2008-0001.003 2/09/2009)

HHS Policy for IT Security and Privacy Incident Reporting and Response (2010-0004 4/05/2010)

A comprehensive list is found at http://www.hhs.gov/ocio/policy/#Security.

Question 38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-07-16; OMB Circular A-130; NIST SP 800-88
Appendix J Control Reference	SE-1; SE-2

Question guidance: NIST SP 800-53, Revision 4, Appendix J, contains a family of controls titled, "Security." This family supplements the security controls found in the security control families within the SP to validate administrative, technical, and physical safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act of 1974, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

During the system development the following controls will be used:

- ***Data on Central Office Computers.*** *Standard backup procedures will be implemented for the central office computer system to protect project data from user error system failure. Backups and inactive files will be maintained on tape or compact disks. The system servers will be maintained inside a secure locked area accessible only to authorized systems personnel. Files will be accessible only by authorized personnel who have been provided project logons and passwords. Access to any of the study files (active, backup, or inactive) on any network multi-user system will be under the central control of the database manager who will ensure that the appropriate network partitions used in the study are appropriately protected (by password access, decryption, or protected or hidden directory partitioning) from access by unauthorized users.*
- ***Documents Received in Central Office.*** *Once in the central office, documents containing respondent information are kept in locked filing cabinets. At the close of the study, such documents are shredded.*
- ***Personally Identifiable Information.*** *Any respondent-identifying information will be contained only in a master list to be created and protected in secure storage, to which*

only a limited number of project staff pledged to maintain data security will have access.

Question 39. Identify the publicly-available URL:

Answer Format	Enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: Identify the URL that is hosted by the system, if applicable.

Not applicable

Question 40. Does the website have a posted privacy notice?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: According to OMB M-03-22 and Title II and III of the E-Government Act of 2002, each website must post clear privacy policies on top-level/principal websites, including major on-line public resource sites and any other known major public entry points and any webpage that collects or posts personal information. Privacy policy links must be clearly labeled and easily accessed by all visitors to a website. If the privacy statement is combined with other mandated or recommended website statements or information, the link should be labeled accordingly, (e.g., Privacy Act notification statement). Accordingly, NIST SP 800-53, Revision 4, Appendix J, states "A privacy notice provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII for the purpose of having it amended or corrected, where appropriate; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in activities that impact privacy, before or as soon as practicable after the change."

Not applicable

Question 40.a. Is the Privacy Policy available in a machine-readable format?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: Per the E-Government Act and OMB M-10-23, all agency websites should have machine-readable privacy policies. System Owners/Managers should consult with the OpDiv SOP and the ISSOs to ensure that their websites are Platform for Privacy Preferences (P3P) compliant. For more information about Machine-Readable Privacy Policy and Platform for Privacy Preferences, refer to the following link for a list of frequently asked questions: http://www.hhs.gov/ocio/policy/hhs-ocio2010_0001_policy_for_machinereadable_privacy_policies.html.

Not applicable.

Question 41. Does the Website use web measurement and customization technology?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: Web measurement and customization technologies, commonly referred to as "Cookies," track computer use. "Session cookies" track the user's activities through a single website and are an approved use of cookies by HHS. "Persistent cookies" track the activities of users over time and across different websites. Federal policy states that federal agencies and their contractors may not use persistent cookies on federal websites unless a number of conditions are met. If a justification exists for a particular system, the OpDiv must submit a written request to the OpDiv SOP, who, in turn, must request approval from HHS before the persistent tracking technology can be installed and used. Agencies may use web measurement and customization technologies for the purpose of improving federal services online through conducting measurement and analysis of usage or through customization of the user's experience. Under no circumstances may agencies use such technologies to track user individual-level activity on the Internet outside of the website or application from which the technology originates; to share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies; to cross-reference, without the user's explicit consent, any data gathered from web measurement and customization technologies against PII to determine individual-level online activity; to collect PII without the user's explicit consent in any fashion; or for any like usages so designated by OMB.

Not applicable

Question 41.a. Select the type of Website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply).

Answer Format	Select the box and the radio button that corresponds to the correct answer(s). If 'Other' is selected enter text into the text field.
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: Indicate the type of Website measurement and customization technologies in use:

Web beacons: Digital objects that are embedded in a web page or e-mail that allows the tracking or checking that a user has viewed the page or e-mail.

Web bugs: Used in combination with cookies, this is often a transparent graphic image that is placed on a Website or in an e-mail that is used to monitor the behavior of the user visiting the Website.

Session cookies: Session cookies track the user's activities through a single website and are an approved use of cookies by HHS.

Persistent cookies: Persistent cookies track the activities of users over time and across different websites. OMB M-02-22 and M-10-23 state that federal agencies and their contractors may not use persistent cookies on federal Websites unless numerous conditions are met. If a justification exists for a particular system, the System Manager or System Owner must submit a written request to the HHS SAOP for approval before the persistent tracking technology can be installed and used.

Not applicable

Question 42. Does the Website have any information or pages directed at children under the age of thirteen?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; Children's Online Privacy Protection Act (COPPA); OMB M-00-13; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: COPPA applies to private sector websites that collect personal information online from children under the age of thirteen. OMB M-00-13, "Privacy Policies and Data Collection on Federal Web Sites" extended the provisions of COPPA to federal websites. COPPA identifies content that a website operator must include in a Privacy Policy, outlines when and how to seek verifiable consent from a parent, and specifies the responsibilities an operator has for protecting children's privacy and safety online.

Not applicable

Question 42.a. Is there a unique Privacy Policy for the Website and does the unique Privacy Policy address the process for obtaining parental consent if any information is collected?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; COPPA; OMB M-00-13; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: If the website collects information from children under the age of thirteen, please describe the process for parents to provide consent for collecting PII.

Not applicable

Question 43. Does the Website contain links to non-federal government Websites external to HHS?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; COPPA; OMB M-00-13; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: "Link" refers to a "hyperlink"—a text, graphic, or other feature on a website —that, when the user clicks on it with a mouse or cursor, automatically directs the viewer to another web page or site. If the site contains links that take the user to a website that is not owned and/or operated by the Department, a link must be provided to a disclaimer stating that the information the user is about to view is not under the control of the Department.

Not applicable

Question 43.a. Is a disclaimer notice provided to users that follow external links to Websites not owned or operated by HHS?

Answer Format	Select the radio button that corresponds to the correct answer(s).
Applicable Reference	Privacy Act of 1974; E-Government Act of 2002; COPPA; OMB

	M-00-13; OMB M-03-22, OMB M-10-22, OMB M-10-23
Appendix J Control Reference	AP-2; DM-1; IP-1; TR-1; TR-3; UL-2

Question guidance: Please indicate whether a disclaimer notice is provided to users. The disclaimer notice must clearly state that an external link will take the user to Websites that are not owned and operated by HHS.

Not applicable