GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO P 1878.2A

GSA POLICY AND PROCEDURE

SUBJECT: Conducting Privacy Impact Assessments (PIAs) in GSA

1. Purpose. This directive establishes policy and procedures for addressing privacy issues in GSA Information Technology (IT) systems, online Web sites, and social media venues containing personal information about individuals. This policy and procedure establishes the Privacy Impact Assessment (PIA) as the required tool for conducting privacy evaluations, defines the privacy issues to be addressed, describes the steps for completing a PIA report, and provides the PIA report format. This policy and procedure assigns responsibilities to ensure compliance with applicable laws and regulations governing privacy and GSA policies and procedures for conducting PIAs.

2. Background.

a. Privacy protection is both a personal and fundamental right of individuals (including GSA employees, clients, and members of the public) and the responsibility of GSA when GSA organizations collect, maintain, and use personal information to carry out the agency's mission. GSA must address privacy issues when planning, developing, and implementing automated systems, and GSA must integrate privacy protections into the life cycle of the systems. In addition, GSA organizations must address privacy issues when online Web sites and social media venues collect personal information about individuals.

b. GSA has instituted the PIA as the means for ensuring that GSA's information systems, online Web sites, and social media venues protect the privacy of individuals. GSA has designed the PIA process to assure compliance with applicable laws and regulations governing an individual's privacy and to ensure the confidentiality, integrity, and availability of an individual's personal information at every stage of system development and operation. The PIA incorporates privacy into design and development to system upgrades and improvement.

3. Applicability. This policy applies to GSA Services, Staff Offices in Central Office, and all GSA Regions, including:

a. the IT systems under each jurisdiction;
b. the GSA employees whose duties involve the management, acquisition, maintenance, and use of IT systems;
c. the contractors, subcontractors, and anyone specified in Memorandums of Understanding (MOUs) or other agreement vehicles; and
d. individual corporations and other organizations that process or handle GSA-owned information.

This policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission.

4. Cancellation. CPO 1878.2B, Conducting Privacy Impact Assessments (PIAs) in GSA is cancelled.

5. Revisions. Revisions reflect that the Privacy Office is now within the Office of GSA IT. The Chief Information Officer (CIO) is the Senior Agency Official for Privacy. Also, signatures on the PIAs are now required from the Project Manager, the Information Systems Security Officer (ISSO), and the Privacy Officer.

6. Responsibilities.

a. Program Manager/System Owner. As the official with management responsibility of the program requiring the system, the Program Manager/System Owner is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the system manager, system developer, and others who may have a concern about resolving privacy and security issues; and reviewing and approving the PIA before submission to a higher level of authority.

b. System Manager (also known as the Project Manager). As the official responsible for the management and operation of the system, the system/project manager is responsible for working with the program manager and the system developer on the system's privacy issues; preparing the PIA report; obtaining the program manager's approval of the PIA report; and submitting the PIA report to GSA IT officials for review and approval. The system/project manager also serves as the point of contact for the system. The system/project manager must sign the PIA before the PIA is sent to GSA IT officials.

c. System developer/designer. The system developer/designer is responsible for ensuring that the system design and specifications conform to privacy standards and requirements and that technical controls are in place for safeguarding personal information from unauthorized access.

d. Authorizing Official (AO). Each Service, Staff Office, and Regional AO is responsible for ensuring the security of their organization's IT systems. Additionally, the AOs are responsible for reviewing and approving PIAs for their organizations. The list of AOs can be found at: https://ea.gsa.gov/tip/frameset?__showtitle=false&__svg=false&__reportCompUUID=DD90A2EF-122A-438D-8A6B-E32692A74EA2

e. The Senior Agency Official for Privacy (SAOP). The SAOP is responsible for ensuring that PIAs are reviewed for privacy issues and meet the privacy requirements under the law and GSA policy.

f. GSA Privacy Act Officer. Under the direction of the Senior Agency Official for Privacy (SAOP), the GSA Privacy Act Officer is responsible for evaluating the PIAs for completeness of privacy related information.

g. The Chief Information Security Officer (CISO). The CISO is responsible for ensuring that PIAs meet IT security standards and requirements established by law and GSA policy.

h. The Chief Information Officer (CIO). The CIO is responsible for overall IT security and privacy management in GSA.

i. Heads of Services and Staff Offices (HSSOs) and Regional Administrators (RAs). These leadership heads are responsible for coordinating the efforts of management and technical personnel under their jurisdiction in meeting PIA requirements.

j. Information System Security Officer (ISSO). The ISSO works with the System/Project Manager to complete the PIA. The ISSO must sign the PIA.

7. Signature.

/S/	October 29, 2014
SONNY HASHMI	Date
Senior Agency Official for Privacy (SAOP)	
Office of GSA IT	

CIO P 1878.2A CONDUCTING PRIVACY IMPACT ASSESSMENTS (PIA'S) IN GSA
TABLE OF CONTENTS

Conducting Privacy Impact Assessments (PIAs) in GSA

1. Policy.

a. Evaluating systems for PIA applicability. All GSA IT systems in existence and systems planned or under development must be evaluated to determine if a full PIA must be done under the requirements of the policy. This includes all minor applications such as Salesforce and Google Apps.

b. Completing the PIA Report.

(1) Part I of the PIA report must be completed for all systems. This part identifies the officials with responsibility for the system and provides the qualifying questions that determine whether a full PIA is required. The System/Project Manager and Information System Security Officer (ISSO) both must sign the PIA.

(2) Part II of the PIA report must be completed for systems that meet the full PIA criteria presented below.

c. Systems that require a full PIA (Parts I and II).

(1) All existing GSA systems that contain information in identifiable form about the general public are subject to the full PIA requirement and must complete an initial PIA. A PIA for any new system must be prepared in the fiscal year in which it is proposed.

(2) All GSA systems that contain information in identifiable form on Federal Government employees require a full PIA. A PIA for any new system must be prepared in the fiscal year in which it is proposed.

d. PIA timing.

(1) A PIA should be initiated in the early stages of development of a new system with information in identifiable form when requirements are being analyzed and decisions made about system design and data usage.

(2) A PIA for an existing system must be completed and reviewed annually. Updates to the PIA are done when there are significant changes to the system or a change in the privacy posture.

(3) A PIA must reflect current information collection practices under continuing authorities and business processes, and accurately describe the data, uses, and handling of the information. The PIA must be updated or revised for: any significant change in the collection or flow of data; new uses or disclosure of information; incorporation into the system of additional items of information; and similar changes.

e. Responsibility for completing a PIA.

(1) The system owner or program manager (the program official with jurisdiction over the system); the system or project manager (the person responsible for developing and managing the system); and the system designer/developer should work together to complete the PIA. The PIA should be completed in coordination with the Office of the CISO.

(2) The system owner/program manager and the system/project manager must determine what data is to be used, how the data is to be used, and who will use the data.

(3) The system developer/designer must determine whether the system requirements and specifications present any threat to individuals' privacy or information security and how the data is to be safeguarded technically. This determination should be completed in coordination with the Office of the CISO.

2. The Privacy Impact Assessment (PIA). A PIA must evaluate the applicability of legal and policy requirements and how the risk to privacy might be minimized. The depth and extent of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the system. In conducting the PIA, the information life cycle (collection, use, retention, processing, disclosure, and destruction) must be considered.

a. Preparing the PIA. The PIA must be prepared in the format provided in Appendix A. The PIA consists of two parts:

(1) Part I, PIA Contacts and Qualification Questions. This section collects the names and contact information for the individuals and offices with responsibility for the system, as well as responses to questions that determine whether the system qualifies for a full PIA. If the answer is "NO" to questions 1 and 2, only Part I should be completed. If the answer is "YES" to either question, a full PIA is required.

(2) Part II, System Assessment. The System Assessment contains questions that address privacy and security issues and requirements. A response must be entered for each question unless a question is not applicable, in which case "N/A" may be entered.

b. Coordination, review, and approval process. (See Appendix A for details.)

(1) The Program Manager/Owner and the System/Project Manager, with assistance from developers and technical experts, coordinate the preparation of the PIA. The System/Project Manager and the Information ISSO must both sign the PIA.

(2) The Service, Staff Office, or regional AO reviews and approves the PIA for the organization.

(3) The GSA Privacy Act Officer reviews the PIA for privacy risks and assesses the PIA for conformance with privacy legal and regulatory requirements.

(4) The CISO reviews the PIA for security risks and assesses the PIA for conformance with security legal and regulatory requirements.

3. Applicable legal and regulatory requirements.

a. The Privacy Act of 1974 (5 USC 552a). The Privacy Act, as amended, affords individuals the right to privacy of records that are maintained in systems of records by Federal agencies. (The Act incorporates the Computer Matching and Privacy Protection Act of 1988, Public Law 100-503; and the Computer Matching and Privacy Protection Amendments of 1990, both of which address electronic sharing of information.) The Act specifically states that each agency shall:

(1) Maintain in its records only the information about an individual that is relevant and necessary to accomplish a purpose of the agency as required by statute or executive order of the President;

(2) Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about individuals' rights, benefits, and privileges under Federal programs;

(3) Maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; and

(4) Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained.

(5) To see the entire reference in the Privacy Act go to http://www.gsa.gov/portal/content/104250

b. The Federal Information Security Management Act of 2002 establishes security practices for Federal computer systems and, among its other system security provisions, requires that agencies:

(1) Conduct a periodic assessment of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; and

(2) Address Information security throughout the life cycle of each agency information system.

c. Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources. It requires Federal agencies to:

(1) Implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications; and

(2) Review the security controls in each system at least every three years, or when significant modifications are made to the system.

d. The Paperwork Reduction Act (44 U.S.C. Chapter 35). The Paperwork Reduction Act requires agencies to limit the collection of information from the public to that which is necessary for the proper performance of agency functions.

e. The E-Government Act of 2002, Section 208. This section aims to ensure privacy in the conduct of Federal information activities and requires agencies to conduct PIAs of electronic information systems.

f. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003, provides clarification and additional guidance on the Section 208 privacy provisions of the Act.

g. CIO 2106.1 GSA Social Media Policy, establishes policy for employee use of social media. It applies to all GSA employees and contractors engaged in social media on behalf of GSA as part of their duties.

h. The GSA Social Media Navigator, GSA's guide to official use of social media.

4. Privacy issues to be considered in a PIA.

a. Information sharing. The availability of vast amounts of stored information and the expanded capabilities of information systems to process the information, mandate that the sharing of information must be strictly controlled and shared only for necessary and lawful purposes.

b. Purpose and use of information. Information collected for a specified purpose may not be used for other purposes without the consent of the individuals whose records are in the system unless specifically authorized or mandated by law.

c. Information collection. Individuals must be informed in writing, in the form of a Privacy Act Statement, of the principal purpose and routine uses of the information collected from them.

d. Information sources. The sources of the information in the system are an important privacy consideration. If data come from other than GSA records or from non-GSA sources, the data must be verified to the extent practicable that the information is accurate, current, and complete, particularly if the information will be used to make determinations about individuals.

e. Data attributes. Privacy attributes of the data in the system must be considered when system information requirements are being determined. The privacy attributes are derived from the legal requirements imposed by the Privacy Act. The data must be *relevant* and *necessary* to accomplish the purpose of the system. The data also must be *complete, accurate,* and *timely* to ensure fairness to the individual in making decisions based on the data. These attributes are defined as follows:

(1) Relevance. Data must be limited to only those elements that clearly bear on the determination(s) for which the records are intended.

(2) Necessity. The threshold of the need for an element of information must be greater than mere relevance and utility.

(3) Completeness. All elements necessary for making a determination must be present before such determination is made.

(4) Accuracy. Information must be free of error to the extent that its use assures an equitable determination.

(5) Timeliness. Information must be updated in a timely manner for making determinations.

f. Access to system data. Access to system data (whether individuals, other systems, or other agencies) must be clearly defined and documented:

(1) Individuals. Access to the data may be system users, system administrators, system owners/program managers, system/project managers, agency managers, and developers in limited, clearly defined circumstances. When individuals are granted access, it must be limited to data needed to perform their assigned duties. If individuals are granted access to all the data in the system, procedures must be in place to detect and deter browsing and unauthorized access.

(2) Other systems. It must be determined if there are there any programs or projects that interface with the system and have access to the data. The transferred data must be defined and controls must be in place to assure that only the defined data is transmitted.

(3) Other agencies. Can be international, Federal, state, or local entities that have authorized access to system data.

g. Data retention and disposal. Data disposition procedures must meet statutory and GSA requirements as set forth in OAS P 1821.1 GSA Records Management Program.

h. Intrusion protection. The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to prevent unnecessary and unauthorized intrusion.

i. Maintaining administrative controls. Automation of systems can lead to the consolidation of processes, data, and controls that protect the data. When administrative controls are consolidated or changed due to automation or system upgrades, the automation/upgrades must be evaluated to ensure that necessary controls of data access and use are maintained.

5. Definitions.

a. Individual. A citizen of the United States or a legal resident alien.

b. Information in identifiable form. Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification (from OMB M-03-22). (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). This includes social media venues such as Facebook, Twitter, and YouTube.

c. Privacy Impact Assessment (PIA). An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (from OMB M-03-22). For this report, information systems, online Web sites, and social media venues will be referred to as "systems."

d. System of Records. Any group of records under the control of an agency from which information is retrieved by the name of an individual, by Social Security Number (SSN), or by some other identifying number, symbol, or other unique identifier assigned to that individual. All such “systems of records” are subject to the Privacy Act.

e. Record. Any item, collection, or grouping of information that is maintained by an agency about an individual within a system of records which contains the individual’s name or any other personal identifier such as number or symbol, fingerprint, voiceprint, or photograph. The information may include but not be limited to education, financial transactions, medical conditions, employment, or criminal history collected in connection with an individual’s interaction with GSA.

f. Information technology (IT) system. Also known as electronic information system, the hardware and software used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

g. Social media. “Social media,” also known as “Web 2.0” or “Gov 2.0” in the case of Federal Government use, are Web-based, interactive tools and media, oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online. Their interactions with the information (both collectively and individually) can significantly alter the experience of subsequent users.

Appendix A. Summary of Steps for Completing a PIA

Project Manager/System Manager Developer: Answers the questions in Part I of the PIA. If a full PIA is required, also completes Part II. Signs the PIA. Submits the PIA to the appropriate AO for review and approval.

Information System Security Officer (ISSO): Works with the Project/System Manager to complete the PIA. Signs the PIA.

Service/Staff Office/Region, Authorizing Official: Reviews and approves the PIA. Submits the PIA to the GSA Privacy Act Officer and the Chief Information Security Officer.

GSA Privacy Act Officer: Reviews the PIA for privacy considerations. Obtains clarification as needed. Approves the PIA on privacy issues.

Chief Information Security Officer: Reviews the PIA for security requirements and risks. Approves the PIA on IT Security issues.

Program Managers/System Manager/Developer, Authorizing Official, Privacy Act Officer, and Chief Information Security Officer: If needed, reach agreement on design requirements to resolve all identified risks. If needed, issues will be raised to the Chief Information Officer for resolution.

Program Manager/System Manager/Developer: As needed, incorporates the agreed upon requirements and resolve any identified risks. Submit revised PIA to the Privacy Act Officer and the Chief Information Security Officer for final review.

IT Capital Planning Division, Information Assurance Committee: Acts as liaison with OMB on IT reporting mandates. Coordinates inclusion of PIAs in reports to OMB regarding IT capital planning and investment. Maintains PIA documents.

Program Manager/System Manager/Developer, Authorizing Official, Privacy Act Officer, and Chief Information Security Officer: Participate in subsequent reviews to ensure system continue to comply with privacy and security requirements.

Appendix B. PIA Template

PRIVACY IMPACT ASSESSMENT

PART I. PIA Contacts and Qualification QUESTIONS

A. Contact Information

System Title: *Enter the name of the IT system*
Office of Responsibility: *Enter the Service, Staff Office, or Region*
Program Manager Name and Title: Phone: Email: Organization Title and Correspondence Code: *Enter the information for the Program Manager/System Owner of the system*
System or Project Manager/Project PIA Contact Name and Title: Phone: Email: Organization Title and Correspondence Code: *Enter the information for the point of contact for the PIA* *Signature:*____
AO Name and Title: Phone: Email: Organization Title and Correspondence Code: *Enter the information for the Designated Approving Authority for your Service, Staff Office, or Region*

Note on template formatting: Responses to questions should replace the Explanations/Instructions in the space provided in column two.

Date PIA completed: ____

Information System Security Officer: ____

B. Qualification Questions

Question	Explanation/Instructions
1. Does your system collect any information in identifiable form (personal data) on the general public? (YES or NO) If YES, a PIA is required, starting in FY 2004.	*Information in identifiable form (also known as personal data/information) refers to any data collected about an individual that can be used for identification purposes.* *It includes information that identifies the individual by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, geographic indicator, personal email address, home address, home phone number, health records, Social Security Number (SSN), personal credit card information, and similar personal information. Information permitting the physical or online contacting of a specific individual is considered information in identifiable form.* ***This does not refer to business entities or government agencies, or aggregate data that cannot be traced back to an individual person**.*
2. Does your system collect any information in identifiable form (personal data/information) on government employees? (YES or NO) If YES, a PIA is required, starting in FY 2005.	*Information in identifiable form refers to any data collected about an employee that can be used for identification purposes. It includes information that identifies the employee by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, marital status, home email address, home address, home phone number, health records, SSN, performance appraisals, employment history not related to current job, allegations of misconduct/arrests/complaints/grievances/performance based actions, payroll deductions, personal credit card information, and similar personal information.*
3. Has a PIA been done before for the system? (YES or NO)	*If Yes, enter the date of the last PIA.*

***(Please Note: If you answered "No" to Question #1 or Question #2, Part II is not required. Part II is for systems that answered "Yes" to either question.* A PIA for an existing system must be completed and reviewed annually. Updates to the PIA are done when there are significant changes to the system or a change in the privacy posture.)**

PART II. SYSTEM ASSESSMENT

A. Data in the System

Question	**Explanation/Instructions**
What is the specific purpose of the agency's use of the information and how does that use fit with the agency's broader mission?	*Agency should use plain language to disclose the purpose(s) of its use of the information. Agency's description should provide enough detail to allow the reader to gain full understanding of the purpose(s).*
1. Describe all information to be included in the system, including personal data.	*a. Briefly describe the purpose of the system and the data that will be in the system, including that of any subsystems.* *b. Provide the specific privacy data elements that will be maintained in the system.*
1. a. What stage of the life cycle is the system currently in?	*Select: Design/Planning; Development/Implementation; Operation/Maintenance; or Disposal.*
2. a. What are the sources of the information in the system?	*Describe where the system data originates, whether the privacy information is provided by the user or entered on behalf of the user and by whom, or if it comes programmatically from another system.*
2. b. What GSA files and databases are used?	*Identify any GSA files and databases that may be used as a source of the information.*
2. c. What Federal agencies are providing data for use in the system?	*List Federal agencies that are providing the information for use by the system. Specify data provided by each. If none, enter* ***None****.*
2. d. What State and local agencies are providing data for use in the system?	*List any State and local agencies that are providing data for use in this system. Specify the data provided by each. If none, enter* ***None.***
2. e. From what other third party sources will the data be collected?	*List any other sources of data in the system and the data provided. If none, enter* ***None.***
2. f. What information will be collected from the individual whose record is in the system?	*List the data that will be collected from the individual.*
3. a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	*The accuracy of personal information is very important. Indicate the steps that will be taken to ensure that the data is accurate and the integrity of the data remains intact.*
3. b. How will data be checked for completeness?	*Missing information can be as damaging as incorrect information. Indicate the steps that will be taken to ensure that all of the data is complete.*

3.c. Is the data current? How do you know?	*Indicate the process that will be used to ensure that the data is relevant and up-to-date.*
4. Are the data elements described in detail and documented? If yes, what is the name of the document?	*Each of the data elements must be defined and described. Descriptions should include the name, data type, and purpose for collection.*

B. Access to the Data

Question	**Explanation/Instructions**
1. a. Who will have access to the data in the system?	*Provide a list of users or groups of users of the entire system (i.e., government agencies, public access, etc.) and a separate list of people who will have access to privacy data.*
1. b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.	*If so, reference the specific exemption under the FOIA (5 U.S.C. Section (b)(1) through (9)) to support your rationale.* *Dept. of Justice guidance on exemptions:* *http://www.usdoj.gov/oip/foi-act.htm* *FOIA text:* *http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm,*
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	*List any policies or procedures used to implement access to the system and privacy data. If there are supporting documents such as technical and operational manuals or a system security plan, list them here.*
3. Will users have access to all data in the system or will the users' access be restricted? Explain.	*Specify to what degree users can access their own privacy data after it has been entered. If there are any restrictions on access to this data, identify the restrictions.*
4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?	*Reference technical, managerial, administrative, and operational controls in place supporting management of the data.*
5. a. Do other systems share data or have access to data in this system? If yes, explain.	*List any systems that will either send or receive data in this system. Explain the purpose of the connection and the methods used to ensure integrity and security of the data being exchanged.*

5. b. Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface?	*List the title and office of the person(s) responsible to ensure that the privacy data is being handled properly. Typically, this should be the System Manager.*
6. a. Will other agencies share data or have access to data in this system (International, Federal, State, local, other)?	*List any entities that may access the data in this system and specify which data. If there are none, enter **None**.*
6. b. How will the data be used by the agency?	*Describe in detail how each piece of data will be used, including programmatic functions, indexing, aggregation, reporting, etc.*
6. c. Who is responsible for assuring proper use of the data?	*This should typically be the same person(s) listed for question 5.b.*
6. d. How will the system ensure that agencies only get the information to which they are entitled?	*List the controls and security mechanisms in place to ensure that exchange of data is appropriate.*
7. What is the life expectancy of the data?	*Indicate whether the data will be collected and used for a one-time process or whether the data will be maintained in a database. Indicate how long the one-time process typically takes or how long data will be maintained. If shared with other systems, provide indication on life expectancy from those systems as well. Use GSA Handbook CIO P 1820.1, GSA Records Maintenance and Disposition System, as a guide for determining the disposition requirements.*
8. How will the data be disposed of when it is no longer needed?	*Provide explanation of data disposal process. Indicate methods for disposing of data from operational databases as well as for archiving systems.*

C. Attributes of the Data

Question	**Explanation/Instructions**
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	*List each data element and the relevance to the system.*
2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	*Yes or No. If yes, provide details on the derivation of the data. An example would be to create a credit risk rating based on credit history.*
2. b. Will the new data be placed in the individual's record (client or employee)?	*Yes or No.*
2. c. Can the system make determinations about individuals that would not be possible without the new data?	*Yes or No. Explain why or why not.*
2. d. How will the new data be verified for relevance and accuracy?	*Since this is privacy data about an individual that was not provided by the individual, the relevance and accuracy are very important. Provide details on processes used to verify this information.*
3. a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	*Enter* ***N/A*** *if the data is not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.*
3. b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	*Enter* ***N/A*** *if the processes are not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.*
4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	*Explain all processes for retrieving the data. If personal identifiers (i.e., name, SSN, employee number, etc.) are used, list the identifiers.*

5. What are the potential effects on the privacy rights of individuals of: a. Consolidation and linkage of files and systems; b. Derivation of data; c. Accelerated information processing and decision-making; and d. Use of new technologies. How are the effects to be mitigated?	*Explain how the privacy rights of the individual may be protected or jeopardized based on a, b, c, and d. List all mitigation strategies used to ensure that the rights of the individuals are not compromised.*

D. Maintenance of Administrative Controls

Question	**Explanation/Instructions**
1. a. Explain how the system and its use will ensure equitable treatment of individuals.	*Describe the processes in place to ensure fair and equitable treatment of individuals and their privacy data. If judgments are to be made based on the privacy data, indicate the rationale to be used to make the judgments and how the judgments will be kept fair and equitable.*
1. b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	*Describe technical, managerial, and operational controls in place to ensure that data integrity and protection is maintained across sites. Also, describe how data will be kept current and consistent between locations.*
1. c. Explain any possibility of disparate treatment of individuals or groups.	*Describe any potential situation where data could be evaluated differently. List the data elements that may impact disparate treatment (i.e., race, gender, etc.).*
2. a. What are the retention periods of data in this system?	*How long will data be kept (years, months, days, hours)? Use GSA records disposition schedules to determine requirements.*
2. b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	*Provide detailed explanation of the data disposal process. Indicate methods for disposing of data from operational databases as well as archiving procedures. List documents supporting these procedures and the locations of these documents.*
2. c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	*Describe data management procedures and updating requirement.*
3. a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g., Caller-ID)?	*Yes or No. If yes, describe any technologies that may be used to collect or display privacy data.*
3. b. How does the use of this technology affect individuals' privacy?	*Is the data more vulnerable to inadvertent or unintentional display? Does it improve the protection of the privacy data?*
4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	*Describe the rationale and processes for identifying, locating, and monitoring individuals. This can include street address, email, cell phone, as well as GPS data.*

4. b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	*Describe the rationale and processes for identifying, locating, and monitoring groups of individuals. This can include street address, email, cell phone, as well as GPS data.*
4. c. What controls will be used to prevent unauthorized monitoring?	*Describe managerial, technical, and operational controls used to manage monitoring activities.*
5. a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.	*List the Privacy Act Systems of Records Notice name and number here. Contact the* GSA Privacy Act Officer for *guidance.*
5. b. If the system is being modified, will the SOR require amendment or revision? Explain.	*If any of the information in the SOR is altered, such as acquisition of new privacy information, new implementations, etc., explain how or why the SOR should be amended. Coordinate preparation of a revised SOR with the GSA Privacy Act Officer.*