U.S. Securities and Exchange Commission
Office of Information Technology
Alexandria, VA

PRIVACY IMPACT ASSESSMENT (PIA) GUIDE

Revised January 2007

Privacy Office
Office of Information Technology

PRIVACY IMPACT ASSESSMENT GUIDE

Introduction

The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections[1]. The assessment is a practical method of evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The process is designed to guide SEC system owners and developers in assessing privacy during the early stages of development and throughout the System Development Life Cycle (SDLC), to determine how their project will affect the privacy of individuals and whether the project objectives can be met while also protecting privacy.

This guide provides a framework for conducting privacy impact assessments and a methodology for assessing how personally identifiable information is to be managed in information systems within the SEC.

PIA Overview

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the SEC's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the SEC's electronic information systems and collections handle personally identifiable information (PII). The objective of the PIA is to systematically identify the risks and potential effects of collecting, maintaining, and disseminating PII and to examine and evaluate alternative processes for handling information to mitigate potential privacy risks.

Personally Identifiable Information (PII)

PII is information in an IT system or online collection that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) In addition, PII may be comprised of information by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may also include gender, race, birth date, geographic indicator and other descriptors.

PII should not be confused with "private" information. Private information is information that an individual prefers not to make publicly known, e.g., because of the information's sensitive nature. Personally identifiable information is much broader in scope and includes all information that can be used to directly or indirectly identify individuals. PIAs require analysis of broader PII issues, not just the narrower "private" aspects.

[1] See OMB Memorandum (M-03-22) Guidance for Implementing the Privacy Provisions of The E-Government Act of 2002.

PIA Requirements

A PIA should be completed when any of the following activities occur:

1. Developing, or procuring any new technologies or systems that handle or collect personal information.
    - A PIA is required for all Exhibit 300 submissions, which serve as budget justification and reporting requirements for major information technology investments.[2] The PIA should show that privacy was considered from the beginning stage of system development. If a program is beginning with a pilot, a PIA is required prior to the commencement of the pilot test.
2. Developing system revisions.
    - If an existing system is modified, a PIA may be required. (See Appendix A for activities that may trigger the need for a PIA)
3. Initiating a new electronic collection of information in identifiable form for 10 or more persons, consistent with the Paperwork Reduction Act (PRA).
    - This requirement includes any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. For additional information, contact the SEC's PRA liaison located in the Office of Information Technology, Information Resources Management Branch.
4. Issuing a new or updated rulemaking that affects personal information.
    - A PIA is required for collections of new information or update to existing collections as part of a rulemaking. The PIA should discuss how the management of these new collections ensures conformity with privacy laws. Even if a program has specific authority to collect certain information, a PIA is required.
5. Categorizing System Security Controls as "High-Major" or "Moderate-Major".
    - The Privacy Analysis Worksheet (PAW), Appendix B, is required for all systems that are categorized as "High-Major" or "Moderate-Major", even if the system does not handle or collect personal information. The PAW serves as justification that privacy was assessed for this "Major" system. (Contact OIT Security at COPS@sec.gov for assistance.)

A PIA is **NOT** required in the following instances:

1. For government-run Web sites, IT systems, or collections of information that **do not** collect or maintain information in identifiable form about members of the general public, government employees, contractors, or consultants.
2. For government-run public Web sites where the user is given the option of contacting the site operator for the limited purpose of asking questions or providing comments.
3. For national security systems
4. When all elements of a PIA are addressed in a data matching or comparison agreement governed by the computer matching provisions of the Privacy Act.

[2] See OMB Circular No. A-11, Part 7, Section 300

5. When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act.
6. When developing IT systems or collecting non-identifiable information for a discrete purpose that does not involve matching with or retrieval from other databases that generate individual or business identifiable information.
7. For minor changes to an IT system or collection that do not create new privacy risks. Appendix A provides detailed examples of conditions that would prompt the need for a new or updated PIA.

PIA Requirements Related to Privacy Act Systems of Records Notice (SORN)

The Privacy Act requires agencies to publish a System of Records Notice (SORN) in the Federal Register that describes the categories of personally identifiable information collected, maintained and used in an automated system. In order for the system to fall under the requirements of a Privacy Act system of records, personal information must be collected on an individual AND retrieved by the individual's name or unique identifier, e.g., SS#. If personal information is collected but never retrieved by the unique identifier, it is not a system of records and a SORN is not required for the system.

Under the statute, any officer or employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5000.

The PIA

The PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. It identifies and assesses privacy implications in automated information systems. The system owner initiates the process by completing the *Privacy Analysis Worksheet*[3]. The responses on this worksheet will determine whether the proposed project meets the criteria requiring a full PIA. If required, the system owner conducts the PIA using the *PIA Template*[4] and the accompanying *PIA Writing Guide*[5]. The system owner responds to privacy-related questions regarding:

- Data in the system (e.g., what data is collected and why)
- Attributes of the data (e.g., use and accuracy)
- Sharing practices
- Notice to Individuals to Consent/Decline Use (e.g., SORN)
- Access to data (i.e., Administrative and Technological Controls)

[3] See Appendix B
[4] See Appendix C
[5] See Appendix D

All questions in the *PIA Template* may not be relevant to every system or may not reflect all the considerations that will be important for a particular system. During the process, the system owner may need to consult with the Chief Privacy Officer, Records Officer, PRA Liaison, and system developer. Refer to the *PIA Writing Guide* for additional guidance.

The depth and content of the PIA should be appropriate for the nature of the information to be collected, and the size and complexity of the system. For example, PIAs for major information systems should reflect an extensive analysis of the consequences of collection and flow of information, alternatives to the collection and handling of PII, appropriate measures to mitigate risks and the rationale for the final design choice or business process.

Steps for Completing a PIA

Who Does It	What is Done
Project Manager/ System Owner	▪ Complete the Privacy Analysis Worksheet (PAW) and, if applicable, the Privacy Impact Assessment (PIA). Consult with necessary parties (e.g. Chief Privacy Officer, Records Officer, PRA Liaison, and Procurement) to resolve any identified privacy risks, and incorporate any agreed upon adjustments. ▪ Sign and submit the PAW and/or PIA to the CPO. ▪ If required, develop SORN and forward to the CPO for review.
Chief Privacy Officer (CPO)	▪ Review PAW, PIA, and/or SORN ▪ Obtain clarification from system owner and project manager, as needed. All parties should reach agreement on design requirements to resolve identified risks. Unresolved issues are raised for resolution. ▪ Endorse PAW and/or PIA and submit to CISO. ▪ Forward SORN to GC for approval. (Allow at least 90 days)
Chief Information Security Officer (CISO)	▪ Review PAW and/or PIA ▪ Obtain clarification from system owner and developer, as needed. All parties should reach agreement on design requirements to resolve identified risks. Unresolved issues are raised for resolution. ▪ Endorse PAW and/or PIA and submit to CIO.
Chief Information Officer (CIO)	▪ Approve PAW and/or PIA ▪ After approval, return original to CPO for final distribution and posting. ▪ If required, submit document with budget submission to OMB
CPO	▪ Provide copies of approved PAW and/or PIA to all parties, and coordinate publishing/posting with the Office of the Secretary
Office of the Secretary (OS)	▪ Publish PIA on SEC Web site and, if applicable, in the *Federal Register* along with the SORN.

Table 1

Activities Which May Trigger a PIA

Conversions	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Functions applied to existing information collection changes anonymous information into information in identifiable form.
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how information in identifiable form is managed in the system. - *For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.*
Significant Merging	Agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated. - *For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.*
New Public Access	User-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.
Commercial Sources	Agencies systematically incorporate into existing information systems, databases of information in identifiable form purchased or obtained from commercial or public sources. - *Exception: Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement.*
New Interagency Uses	Agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA.
Internal Flow or Collection	Alteration of a business process that results in significant new uses or disclosures of information, including incorporation into the system of additional information in identifiable form.
Alteration in Character of Data	New information in identifiable form is added to a collection and thus, raises the risks to personal privacy. - *For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.*

Table 2

Privacy Analysis Worksheet

The Privacy Analysis Worksheet (PAW) is completed to determine whether a full Privacy Impact Assessment (PIA) and/ or a System of Records Notice (SORN) are required for your project.

This worksheet is to be completed by the project manager and system owner. Complete Section A below, sign and send the form to the Privacy Office. Upon receipt, the Privacy Office will review the form and may request additional information.

SECTION A

Summary Information

1. Name of project or system:
   <Please enter the project or system name here.>

2. Description of project or system and its purpose:
   <Please provide a general description of the project or system, and its purpose using a non-technical description, if statutory, provide citation.>

3. Contact Name, Title, Telephone Number and Organization:
   <Please provide information here.>

Specific Questions

1. Does this project or system collect, maintain, retrieve or share personal information that can be used to directly or indirectly identify an individual?

   □ NO. A PIA is not required for this project. Skip to Signature Page.
   □ YES. A PIA is required for this project.
   <Please provide a specific description of the information that might be collected or maintained.>

2. Does this project or system retrieve information using a personal identifier?

   □ NO. A Privacy Act SORN is not required for this project. Skip to Signature Page.
   □ YES. A Privacy Act SORN is required for this project.
   <Please provide a description of the data fields that might be used to retrieve the information.>

   Is there an existing Privacy Act System of Records Notice (SORN)?
   □ NO. <Contact privacyhelp@sec.gov for assistance.>
   □ YES. The existing SORN may need to be modified to reflect changes.
   <Please provide the system notice number.>

Privacy Analysis Worksheet

Signature of Individual(s) completing this form

_______________________________ _______________________________

System Owner/Date Project Manager/Date

SECTION B

Endorsement

_______________________________ _______________________________

Chief Privacy Officer/Date Chief Information Security Officer/Date

Approval

____

Chief Information Officer/Date

PIA Template

Refer to the PIA Writing Guide (Appendix D) for guidance in responding to the questions below. If not applicable, respond N/A.

CONTACT INFORMATION

Project Manager/ System Owner(s)

Name
Title
Organization
Telephone Number

GENERAL INFORMATION - Project/System Information

1. Name of Project or System.
2. Description of Project or System.
3. What is the purpose of the Project or System?
4. Requested Operational Date?
5. System of Records Notice (SORN) number?
6. Is this an Exhibit 300 project or system?
7. What specific legal authorities, arrangements, and/or agreements require the collection of this information?

SECTION I - Data in the System

1. What data is to be collected?
2. What are the sources of the data?
3. Why is the data being collected?
4. What technologies will be used to collect the data?
5. Does a personal identifier retrieve the data?

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern?
3. How will the data collected from individuals or derived by the system be checked for accuracy?

SECTION III - Sharing Practices

1. Will the data be shared with any internal or external organizations?
2. How is the data transmitted or disclosed to the internal or external organization?
3. How is the shared data secured by external recipients?

SECTION IV - Notice to Individuals to Decline/Consent Use

1. Was notice provided to the different individuals prior to collection of data?
2. Do individuals have the opportunity and/or right to decline to provide data?
3. Do individuals have the right to consent to particular uses of the data?

PIA Template

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the Records Officer? If so, what is the retention period for the data in the system?
2. What are the procedures for identification and disposition of the data at the end of the retention period?
3. Describe the privacy training provided to users, either generally or specifically relevant to the program or system?
4. Will SEC contractors have access to the system?
5. Is the data secured in accordance with FISMA requirements?
   - If **NO**, answer questions 6-9 below.
   - If **YES,** provide date that the Certification & Accreditation was completed.
6. Which user group(s) will have access to the system?
7. How is access to the data by a user determined? Are procedures documented?
8. How are the actual assignments of roles and rules verified according to established security and auditing procedures?
9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data?

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Signature of Individual(s) completing this form

________________________________ ________________________________
System Owner/Date Project Manager/Date

Endorsement

________________________________ ________________________________
Chief Privacy Officer/Date Chief Information Security Officer/Date

Approval

____
Chief Information Officer/Date

PIA Writing Guide

The PIA Template (Appendix C) has been developed for ease of use, which includes only the top level questions noted below. The sublevel examples in the below outline are to provide additional guidance in responding to the required questions.

CONTACT INFORMATION

Project Manager (Name, Title, Organization, Telephone Number)

- This is the official responsible for ensuring that appropriate security and privacy controls are in their system designs.

System Owner(s) (Name, Title, Organization, Telephone Number)

- Under the Privacy Act, the system owner is defined as the official responsible for the operation and management of the system of records
- For IT related responsibilities, the system owner is the IT official responsible for C&A activities throughout the system's life cycle.

GENERAL INFORMATION – System/Project Information

1. Name of Project or System.

2. Description of Project or System.

2.1 Provide a general description of the information in the system and the functions the system performs that are important to the division/office's and SEC's mission.

3. What is the purpose of the Project or System?

3.1 Include a statement of why this PARTICULAR personally identifiable information that is collected and stored in the system is necessary to the SEC's mission. *Merely stating the general purpose of the system without explaining why particular types of personally identifiable information should be collected and stored is not an adequate response to this question.*

3.2 For example, a statement that a system may collect name, date of birth and biometrics in order to verify an individual's identity when visiting the SEC buildings is adequately specific. However, only stating that the above data will be collected to verify identity is not sufficient.

4. Requested Operational Date?

4.1 In responding to this question refer to the date in the Life Cycle Plan of the IT Investment Plan. This will assist in establishing a timeline for a System of Records Notice, if required.

5. System of Records Notice (SORN) number?

5.1 If your system collects, maintains, uses and disseminates information **AND** retrieves that information by the name or other identifier particular to an individual(s), a Privacy Act System of Records Notice will need to be published in the *Federal Register*. Approval of the SORN is made by the Office of the General Counsel. Allow time for approval, which may take at least 90 days.

5.2 For systems that are already covered by an existing SORN, the Privacy Act requires that amendments to an existing system be addressed in a *Federal Register* notice.

6. Is this an Exhibit 300 project or system? If yes, this PIA must be submitted to OMB.

6.1 Exhibit 300 refers to Part 7 (section 300) of OMB Circular No. A-11 (2005), which establishes policy for planning, budgeting, acquisition and management of Federal capital assets, and instructs on budget justification and reporting requirements for major information technology (IT) investments.

7. What specific legal authorities, arrangements, and/or agreements defined the collection of data?

7.1 Cite the statutory provisions or Executive Orders that authorize the collection, maintenance, use and dissemination of the data to meet an official program mission or goal?

SECTION I – Data in the System

The following questions define the scope of the data collected and reasons for its collection as part of the system and/or technology being developed.

1. What data is to be collected?

1.1 List all personal data that is collected and stored in the system. This could include, but is not limited to, name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code address, facsimile number, 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 number, uniform resource locators (URLs), education record, internet protocol addresses, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

1.2 When necessary, a general summary of the data may be provided along with an appendix with the full list attached.

2. What are the sources of the data?

2.1 List the individual, entity, or entities providing the specific data identified above. For example, is the data collected directly from the individual as part of a registration statement, or is it collected from another source, such as commercial data aggregators.

2.2 Describe why data from sources other than the individual are required. For example, if a program is using data from a commercial aggregator of information, state the fact that this is where the data is coming from and indicate why the program is using this source of data.

3. Why is the data being collected?

3.1 Include a statement of why this PARTICULAR personally identifiable information (PII) that is collected and stored in the system is necessary to the SEC's mission. Merely stating the general purpose of the system without explaining why particular types of personally identifiable information should be collected and stored is not an adequate response to this question.

3.2 For example, a statement that a system may collect name, date of birth and biometrics in order to verify an individual's identity when visiting the SEC buildings is adequately specific. However, only stating that the above data will be collected to verify identity is not sufficient.

4. **What technologies will be used to collect the data?**

   4.1 Describe how the data will be collected and why specific collection technologies were chosen.

5. **Does a personal identifier retrieve the data?**

   5.1 This question identifies for which systems a System of Records Notice needs to be published in the Federal Register. If yes, list the identifiers that will be used to retrieve data on the individual. If the data is collected but never retrieved by the unique identifier, it is not a system of records and a SORN is not required for the system.

   5.2 Note: Even though information on individuals may not be retrieved by a personal identifier and therefore not covered by the Privacy Act, other laws such as the Freedom of Information Act (FOIA) apply in protecting privacy.

SECTION II – Attributes of the Data (use and accuracy)

The following questions delineate the uses and accuracy of the data.

1. **Describe all uses of the data.**

   1.1 Identify and list each use (internal and external to SEC) of the PII data collected or maintained.

   1.2 If a SORN has been published for the system, summarize the most relevant routine uses from the SORN in this section. In addition, list the uses internal to SEC since the routine uses listed in the SORN are limited to disclosures made outside of SEC.

2. **Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining)**

   2.1 Many systems sift through large amounts of information in response to a user inquiry or programmed functions to make determinations and, sometimes, conclusions based upon the information they analyze. This is loosely known as data mining.

   2.2 If the system creates or makes available new or previously unavailable information about an individual, state/explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to government employees who make determinations about the individual? If so, explain fully under what circumstances that information will be used and by whom.

3. **How will the data collected from individuals or derived by the system be checked for accuracy?**
   3.1 Explain whether data in the system is checked against any other source of information (within or outside the SEC) before the information is used to make decisions about an individual. If not, explain whether your organization has any other rules or procedures in place to reduce the instances in which inaccurate data is stored in the system.
   3.2 If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

SECTION III – Sharing Practices

The following questions define the content, scope, and authority for information sharing, internally and externally, which includes Federal, state and local government, and the private sector.

1. **Will the data be shared with any internal or external organizations?**
   1.1 Identify and list the name(s) of any offices and divisions within the SEC and any external entities with whom the data will be shared.
   1.2 If shared externally, cite the specific authority which allows sharing of the data.
   1.3 Consider any Memoranda of Understanding (MOU) or sharing agreements that may be in force or effect. Is a MOU, contract, or agreement in place with any external organization(s) with whom data is shared, and does the MOU reflect the scope of the data currently shared?
   1.4 You may also need to consider a review of the appropriate Privacy Act System of Records Notice to determine whether the uses of the data as represented in the SORN allows for that data to be exchanged and used for these new purposes or uses.
   1.5 If a MOU or sharing agreement is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

2. **How is the data transmitted or disclosed to the internal or external organization?**
   2.1 Describe how the data is transmitted to external organizations. For example is the data transmitted electronically, in bulk, by paper, direct access, or by some other means?

3. **How is the shared data secured by external recipients?**
   3.1 List who is responsible for assuring the security and privacy of the data once it is shared; and if possible, include a reference to and quotation from any MOU, contract, or other agreement that defines the parameters of the sharing agreement.
   3.2 Explain whether any system where information is being shared externally has undergone a Security Certification & Accreditation (C & A). If the external system has not completed C&A, how have the external system's security issues been addressed to ensure the privacy and security of the information once it is shared?

SECTION IV – Notice to Individuals to Decline/Consent Use

The following questions address actions taken to provide notice to individuals of their right to consent/ decline to collection and use of information

1. **Was notice provided to the individual prior to the collection of data? A notice may include a posted privacy policy, a Privacy Act notice on forms, or a System of Records Notice published in the Federal Register. If notice was not provided, explain why not.**
   1.1 This question is directed at the notice provided prior to collection of the data. This refers to whether the person is made aware that his or her data is being collected.

2. **Do individuals have the opportunity and/or right to decline to provide data?**
   2.1 This question is directed at whether the person from or about whom data is collected can decline to provide the data and if so, whether a penalty or denial of service results.

3. **Do individuals have the right to consent to particular uses of the data? If so, how does the individual exercise the right?**
   3.1 This question is directed at whether the consent given to the collection of data covers all uses (current or potential) of their information or if an individual may provide specific consent for each use. If such consent is required, how would the individual consent to each use.

SECTION V – Access to Data (administrative and technological controls)

The following questions describe administrative controls, technical safeguards and security measures.

1. **Has the retention schedule been established by the SEC Records Officer? If so, what is the retention period for the data in the system?**
   1.1 The retention periods of data/records that the SEC manages are contained in its General Records Schedule (GRS). For the particular data being created or maintained in this system/project, the GRS is the authoritative source for this information. For more information on the GRS, contact the SEC Records Officer.

2. **What are the procedures for identification and disposition of the data at the end of the retention period?**
   2.1 Where are the procedures documented? Also consider the retention of all generated reports.

3. **Describe the privacy training provided to users either generally or specifically relevant to the program or system?**
   3.1 All employees, including contractors have the requirement for protecting Privacy Act protected information. Address the privacy and security awareness program and controls, including any training programs or materials.

4. **Will SEC Contractors have access to the system?**
   4.1 If **YES**, what controls are planned to ensure appropriate access and what Privacy Act clauses were inserted in their contracts. (Refer to Procurement Branch for your particular contract).

5. **Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?**
   5.1 Affirm that the system/project is following IT security requirements and procedures required by federal law and policy to ensure that the information is appropriately secured.
   5.2 Acknowledge that a risk assessment is conducted, identify appropriate security controls to protect against that risk and implement those controls.
   5.3 Describe in general how regular monitoring, testing, or evaluating is performed to ensure that controls continue to work properly, safeguarding the information.

6. **Which user group(s) will have access to the system?**
   6.1 List the types of users. For example: managers, system administrators, contractors, developers and any staff which may have access to the system.
   6.2 List user groups or positions from other agencies that may have access to the system and under what roles do these individuals have access to the system.

7. **How is access to the data by a user determined? Are procedures documented?**
   7.1 For example, does the system use "roles" to assign privileges to users of the system?
   7.2 Describe in general terms the different "roles" that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be able to make certain amendments or changes to the data.

8. **How are the assignments of roles and rules verified?**
   8.1 For example, when an employee no longer works for the organization or in a specific job function, is there a written procedure for removing his or her access?

9. **What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data?**
   9.1 As appropriate, discuss how new or existing data controls are strengthened to ensure that the data is not accessed inappropriately or by someone unauthorized to access the data.
   9.2 Discuss technical measures/controls of identification and authentication that prevents unauthorized people or processes from accessing the data. The IT Security C&A process require a system security plan outlining the implementation of the technical controls associated with identification and authentication.

PIA Writing Guide

SECTION VI - Privacy Analysis

This section discusses the analysis that was performed to identify any potential privacy risks in the system and the evaluation of any alternatives to mitigate such risks.

1. Describe the process through which design choices were made and how privacy was considered during the design process.
2. Describe any types of controls that may be in place to protect personal information. For example:
   2.1 Were decisions made to encrypt certain data sets and not others?
   2.2 Have access controls been implemented and are audit logs reviewed to ensure appropriate uses?
   2.3 Were decisions made to collect less data?