Department of Energy
Procedures
For Conducting
Privacy Impact Assessments

Abel Lopez, Director
Freedom of Information Act
and Privacy Act Group

January 2007

PRIVACY IMPACT ASSESSMENT

Introduction

On December 17, 2002, President George Bush signed the E-Government Act (E-Gov Act) into law. E-Government is designed to make it easier for citizens and business to access government information and services by encouraging interagency information technology (IT) initiatives that, while improving customer service, also consolidate redundant systems, decrease paperwork, increase productivity and save money.

The E-Gov Act also requires agencies to (1) ensure the protection of the personally identifiable information they collect, store, transmit, and (2) retain and or transfer information in accordance with National Archives and Records Administration (NARA) approved records disposition schedules.

With a thriving digital economy, agencies are collecting large amounts of personal information. Instances of past abuse, misuse, and egregious errors in management of personal information by federal agencies, combined with growing public concern about the U.S. Government's ability to protect their private information, have increased congressional scrutiny and expectations for compliance with federal privacy laws and regulations. Protection of the Government's accumulation of this vast amount of personal information begins with the responsibility of federal employees at all levels and in all positions.

Purpose

The purpose of this document is to (1) establish procedures to address privacy concerns during the systems development process; (2) describe the steps required to conduct a Privacy Impact Assessment (PIA); and (3) define the privacy issues a project must address when completing a PIA.

Background

The Department of Energy (DOE) is responsible for ensuring the confidentiality, integrity, and availability of information contained within its information systems. DOE must at times collect, use, analyze, and store personally identifiable information of its employees and customers. DOE remains vigilant in protecting all its information technology resources, but this is especially true of those systems that contain personally identifiable information.

DOE employees and customers also have the right to expect that the DOE will collect, maintain, use, disseminate, and retain or transfer personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities. Employee and customer personal information is protected by some of the following:

- The Privacy Act of 1974, as amended, 5 U.S.C. 552a, affords individuals the right to privacy in records that are maintained and used by Federal agencies. Section 552a of Title 5 also includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503);

- The Computer Security Act of 1987 (Public Law 100-234), which includes minimum security practices of Federal computer systems;

- OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with fair information practices and security requirements to operate automated information systems and implement Records Management;

- The Freedom of Information Act, as amended, 5 U.S.C. 552, which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

What is a Privacy Impact Assessment?

A process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

When to conduct a Privacy Impact Assessment?

The E-Gov Act requires agencies to conduct a PIA before

a. developing or procuring Information Technology (IT) systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or

b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. The following circumstances are examples where a PIA is needed:

a. Conversions – when converting paper-based records to electronic systems;

b. Anonymous to non-anonymous – when functions applied to an existing information collection change anonymous information into information in identifiable form;

c. Significant system management changes – when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system (e.g., when an agency employs new relational database technologies or web-based processing to access multiple data stores; such addition could create a more open environment and avenues for exposure of data that previously did not exist);

d. Significant merging – when 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 (e.g., 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 at issue);

e. New public access – when user authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by a member of the public;

f. Commercial sources – when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

g. New interagency uses – when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Gov Act initiatives; in such cases, the lead agency should prepare the PIA;

h. Internal flow or collection – when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form; and

i. Alteration in character of data – when new information in identifiable form added to a collection raises the risks to personal privacy (e.g., the addition of health or financial information).

A PIA is not required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged. The following circumstances are examples when a PIA is not required:

a. For government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the public (this includes government personnel and government contractors and consultants);

b. For government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;

c. For national security systems defined at 40 U.S.C. 11103 and exempt from the definition of information technology (see section 202(i) of the E-Gov Act);

d. When all elements of a PIA are addressed in a matching agreement governed by the computer matching provision of the Privacy Act (see 5 USC 552a (8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide for privacy protection for matched information;

e. When all elements of a PIA are addressed in an interagency agreement that permits 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-Gov Act;

f. If agencies are developing IT systems or collecting non-identifiable information for a discrete purpose that does not involve matching with or retrieval from other data bases that generates information in identifiable form;

g. For minor changes to a system or collection that do not create new privacy risks.

PIAs must be updated to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

Must a PIA be conducted for information technology systems that contain or administer information in identifiable form strictly about agency employees or agency contractors?

The legal and policy requirements that address federal agency computer security apply equally to federal IT systems containing identifiable information about members of the public and to systems containing identifiable information solely about agency employees or contractors. As a practical matter, all systems containing information in identifiable form are subject to the same technical, administrative and operational security controls.

Section 208 of the E-Gov Act nor OMB's implementing guidance (Memorandum 03-22) mandate agencies to conduct PIAs on electronic systems containing information about federal employees and contractors. However, OMB suggests that agencies conduct PIAs on all systems that contain or administer information in identifiable form about its employees, contractors or members of the public. For this reason, it will be the policy of DOE to conduct PIAs on all systems that contain or administer information in identifiable form about its employees, contractors or members of the public. All PIAs will be reported to OMB as part of the Federal Information Security Management Act (FISMA)

reporting requirement. However, only those PIAs that contain information about members of the public will be posted on the DOE Headquarters FOIA web page.

Who Completes the Privacy Impact Assessment?

Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

The Privacy Impact Assessment Document

Preparing the PIA documents requires the system owner and system developer to answer the privacy questions in Attachment A. A brief explanation should be written for each question. Issues that do not apply to a system should be noted as "Not Applicable." During the development of the PIA, personnel in the FOIA and Privacy Act Office will be available to answer questions related to the PIA process and other concerns that may arise.

Privacy Impact Assessment Document Review and Approval Process

The completed PIA must be submitted to the Headquarters Privacy Act Officer, who is the Director of the FOIA and Privacy Act Group, for review. The purpose of the review is to ensure all privacy concerns have been identified and addressed, and any corrective actions have been taken. The Privacy Act Officer will work with the system owner and system developer to identify and resolve any privacy concerns. The document will be reviewed by the Office of the Chief Information Officer (CIO) and signed by the Privacy Act Officer. The Senior Agency Official for Privacy Policy also will review and sign the PIA. The review and signature of the Senior Agency Official for Privacy Policy validates the incorporation of the design requirements to resolve the privacy risks.

Steps for Completing a Privacy Impact Assessment

Steps	Who Does It	What is Done
1.	Owner and Developer	Obtain a copy of the PIA template from the Headquarters Privacy Act Officer and answer all questions on the PIA. Consult with the Privacy Act Officer about any Privacy Act questions or concerns. The template also is available by clicking on the FOIA link at the bottom of

		www.energy.gov.
2.	Owner	Consult with the appropriate Program Records Official (PRO) to ensure that the value of the data in the information systems has been established and is protected as set forth by the National Archives and Records Administration (NARA) through the records disposition schedules. Contact information for the PRO can be obtained from the Departmental Records Officer in the Office of the CIO.
3.	Owner, Developer, CIO, Privacy Act Officer, IT Security Officer	All parties should reach an agreement on design requirements and resolve any identified privacy or security risks.
4.	Owner, IT Security Officer	Review PIA for IT Security Certification and Accreditation (C&A) purposes. System Owner signs PIA and sends the PIA to the Headquarters Privacy Act Officer for approval and signature.
5.	Headquarters Privacy Act Officer	Obtains approval and signature of the Senior Official for Privacy Policy and provides a copy of the signed PIA to the System Owner. Copies of the signed PIA are also provided to CIO who will send the PIA to OMB as part of the Exhibit 300 reporting requirement.
6.	Headquarters Privacy Act Officer	Posts signed PIAs about member of the public on

		the FOIA/Privacy Act web page.

Section I

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project:
Bureau: Department of Energy
Project's Unique ID:
Date: _____

A. CONTACT INFORMATION:

1) Who is the person completing this document?

2) Who is the system owner?

3) Who is the system manager for this system or application?

4) Who is the IT Security Manager who reviewed this document?

5) Who is the Privacy Act Officer who reviewed this document?

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

a. Is this information identifiable to the individual[1]?

b. Is the information about individual members of the public?

c. Is the information about DOE or contractor employees?

2) What is the purpose of the system/application?

[1] "Identifiable Form" – According to the OMB Memo M-02-22, this means 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 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. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptor).

3) What legal authority authorizes the purchase or development of this system/application?

C. <u>DATA in the SYSTEM:</u>

1) What categories of individuals are covered in the system?

2) What are the sources of information in the system?

a. Is the source of the information from the individual or is it taken from another source?

b. What Federal agencies are providing data for use in the system?

c. What Tribal, State and local agencies are providing data for use in the system?

d. From what other third party sources will data be collected?

e. What information will be collected from the individual and the public?

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?

b. How will data be checked for completeness?

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

d. Are the data elements described in detail and documented?

D. <u>ATTRIBUTES OF THE DATA:</u>

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

3) Will the new data be placed in the individual's record?

4) Can the system make determinations about employees/public that would not be possible without the new data?

5) How will the new data be verified for relevance and accuracy?

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

8) How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

10) What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?

E. <u>Maintenance and Administrative Controls:</u>

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

2) What are the retention periods of data in the system?

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

4) Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

5) How does the use of this technology affect public/employee privacy?

6) Will this system provide the capability to identify, locate, and monitor individuals?

7) What kinds of information are collected as a function of the monitoring of individuals?

8) What controls will be used to prevent unauthorized monitoring?
9) Under which Privacy Act system of records notice does the system operate?

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

F. <u>Access to Data:</u>

1)Who will have access to the data in the system?

2) How is access to the data by a user determined?

3) Will users have access to all data on the system or will the user's access be restricted?

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?

6) Do other systems share data or have access to the data in the system? If yes, explain.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

8) Will other agencies share data or have access to the data in this system?

9) How will the data be used by the other agency?

10) Who is responsible for assuring proper use of the data?

The Following Officials Have Approved this Document

System Manager

_____ (Signature) _____(Date)
Name:

Title:

Privacy Act Officer (Field Site if Applicable)

_____ (Signature) _____(Date)
Name:

Title:

Privacy Act Officer (Headquarters)

_____(Signature) _____(Date)
Name: Abel Lopez

Title: Director, FOIA and Privacy Act Group

Senior Agency Official for Privacy

_____ (Signature) _____ (Date)
Name: Ingrid A.C. Kolb

Title: Director, Office of Management

Section II

Guidelines for Completing
Privacy Impact Assessments

The template for completing PIAs is available by clicking on the FOIA link at the bottom of www.energy.gov or you may contact the DOE Headquarters Privacy Act Officer on (202) 586-5955. The completed PIA should be submitted to the Privacy Act Officer at DOE Headquarters for review and approval by the appropriate DOE officials.

Name of Project: The name of the system as it is described on the Exhibit 300 or Exhibit 53.

Bureau: The name of the agency

Project's Unique ID:

Date: The date the PIA is being submitted for approval

A. CONTACT INFORMATION:

1) Who is the person completing this document? (Name, title, organization and contact information)

This section should provide the name, title, organization and contact information of the person completing the PIA.

2) Who is the system owner? (Name, title, organization and contact information)

This section should provide the name of the agency official who is responsible for the data (also known as the business owner of the information that is being maintained in the system.

3) Who is the system manager for this system or application? (Name, title, organization and contact information)

This section should provide the name of the official who is responsible for operating and maintaining the system application.

4) Who is the IT Security Manager who reviewed this document? (Name, title, organization and contact information)

This section should provide the name of the individual responsible for overseeing the security of the system. This is usually the person who is responsible for

coordinating and completing the Certification and Accreditation (C&A) of the system.

5) Who is the Privacy Act Officer who reviewed this document? (Name, title, organization and contact information)

This section should provide name and title of the Headquarters Privacy Act Officer and if applicable the name of field Privacy Act Officer.

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

This is usually a yes or no answer. You must review the type of information that is being collected and maintained to determine if the information is about members of the public, agency employees, contractor employees, etc.

a. Is this information identifiable to the individual?

(Yes or No) Information identifiable to the individual is any information that pertains to an individual. This may include, but not limited to, the following:

- Information that relates to race, national or ethnic origin, religion, age, marital or family status;
- Information that relates to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

b. Is the information about individual members of the public?

(Yes or No) This pertains to information about an individual who is not an employee or a contractor for the agency (e.g., homeowners, vendors, requesters, etc.).

c. Is the information about employees?

(Yes or No) This would include agency, contractor, and subcontractor employees of the agency.

If you have answered no to these questions, a PIA is not required for FISMA reporting. However, the DOE policy is to conduct a PIA on all systems that contain or administer information in an identifiable form about its employees, contractors or members of the public.

A copy of the PIA should be provided to the following offices to verify that the system has been evaluated for privacy concerns:

(1) The Office of the Associate CIO for Cyber Security, IM-30, with the C&A package;

(2) The Office of the Associate CIO for Information Technology Reform, IM-20, with the Exhibit 300; and

(3) The Headquarters Privacy Act Officer, MA-74.

2) What is the purpose of the system/application?

What are the primary uses of the system/application? How will it support the program's mission? This information is included when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act systems of records. It also is included in the Privacy Act systems notice published in the *Federal Register*. If the system has a Privacy Act system of records notice, the response to this question should reflect the information in the narrative and notice.

3) What legal authority authorizes the purchase or development of this system/application?

What statutory provisions or Executive Order authorizes the collection and maintenance of the information to meet an official program mission or goal? This information is included when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act systems of records.

The information provided is used to prepare or amend Privacy Act systems notices. If the system has a Privacy Act system of records notice, the response to this question should reflect the information published in the notice. For more information about Privacy Act systems notices contact the Headquarters FOIA and Privacy Act Office.

C. <u>DATA IN THE SYSTEM:</u>

1) What categories of individuals are covered in the system? (e.g., agency employees, contractor employees, visitors, volunteers, etc.)

The information provided is included in the narrative statement when submitting reports to OMB and Congress for new and major amendments to Privacy Act systems of records. This information also is used in preparing Privacy Act systems notices. If the system already has a Privacy Act system of records notice, the response to this question should reflect the information published in the notice. For more information about Privacy Act systems notices contact the Headquarters FOIA and Privacy Act Office.

2) What are the sources of information in the system?

a. Is the source of the information from the individual or is it taken from another source?

You should explain from whom or where the information is being obtained. Usually information is obtained from the individual to whom it pertains. However, there are instances when data is obtained from other sources (e.g., other departmental data bases, credit reporting agencies). If the system has a Privacy Act system of records notice, your response should reflect the information published in the notice.

b. What Federal agencies are providing data for use in the system?

If information is obtained from a federal agency, those agencies should be listed in this section. (e.g., Department of Justice, OPM, etc.).

c. What Tribal, State and local agencies are providing data for use in the system?

If information is obtained from state or local agencies, those entities should be listed in this section. A tribal government is the governing body of any Indian tribe, band, nation or any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

d. From what other third party sources will data be collected?

A third party is usually a non-Federal person or entity, who may be a source of data/information (e.g., informant, an internet service provider, a neighbor or friend, etc).

e. What information will be collected from the individual and the public?

Be as specific as possible and list information on individuals collected from the public, such as name, address, social security number, telephone numbers, health information. If the system has a Privacy Act system of records notice, the information provided for this question should reflect the information in the notice.

3) Accuracy, Timeliness, and Reliability

The Privacy Act of 1974 requires that each agency that maintains a system of records shall "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." (5 U.S.C. 552a (e)(5)). If the data does not meet any one of these components, fairness in making any determination is compromised.

a. How will data collected from sources other than DOE records be verified for accuracy?

The information must have some form of verification for accuracy because of the Privacy Act provision that requires that only relevant and accurate records should be collected and maintained about individuals. Data accuracy and reliability are important requirements in implementing the Privacy Act.

b. How will data be checked for completeness?

The data must be complete before that the data is deemed accurate. Therefore, this section should state the steps the agency has taken to ensure the data is complete.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

If the data is not current, then the relevancy and accuracy of the data are called into question. When possible, the data should be obtained from and/or verified with the individual to whom it pertains.

d. Are the data elements described in detail and documented?

This section should describe the type of information that is being collected and maintained, and the legal authorities for the collection and maintenance of the information.

D. <u>ATTRIBUTES OF THE DATA:</u>

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The Privacy Act at 5 U.S.C. 552a(e)(1) requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant <u>and</u> necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President."

Refer to DOE's Privacy Act regulations found at Title 10, Code of Federal Regulations (CFR), Part 1008.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

What is meant by derived and aggregation? All enhanced or modernized systems most likely will derive new data and create previously unavailable data about an individual from the information collected through aggregation.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data.

3) Will the new data be placed in the individual's record?

Will the information be placed in a new file or a file with existing information that pertains to the individual? If the information is placed in a file that pertains to the individual and is retrieved by a personal identifier, a Privacy Act system of records must be established or amended.

4) Can the system make determinations about employees/public that would not be possible without the new data?

If the answer is no, your answer should be N/A.

5) How will the new data be verified for relevance and accuracy?

Refer to Sections C. 3 a., b., and c.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

If the data is being consolidated (i.e, combined or united into one system, application or process), the existing controls, if any, should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not accessed by someone unauthorized to access the data. These controls will help prevent unauthorized use from occurring. Minimum sets of controls are outlined in OMB A-130 Appendix III and NIST 853A.

The IT Security Plan also describes the practice of identification and authentication, which is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security C&A process requires a system security plan that outlines the implementation of the technical controls associated with identification and authentication.

8) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

In this section you should describe the controls that are in place to prevent the information from being compromised. You should describe the risk management for the system.

The NIST SP-800-30 Risk Management Guide for Information Technology (IT) Systems outlines principles and practices that should be used for securing IT systems. When processes are consolidated, management must maintain proper controls minimizing the risk to all systems. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. The IT Security C&A process requires that a risk assessment be performed regularly on an agency's major applications, networks, and computer installations.

9) How will data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved a number of ways, but there is usually a personal identifier associated with a data retrieval mechanism. A system with data on individuals that is retrieved by a name or personal identifier is a Privacy Act system of records and will need a published system of records notice or an amended notice in the *Federal Register*. If you do not have a published system of records notice, contact the DOE Headquarters Privacy Act Officer on (202) 586-5955.

10) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

If any reports about individuals are created from the data, then a detailed explanation describing the reports, the use of the reports, and who will have access to them should be described in this section.

11) What opportunities do individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?

This section should describe if there is a mechanism available for the individual to accept or decline the personal information being provided and if there are any penalties if the information is not provided.

E. <u>Maintenance and Administrative Controls:</u>

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

All sites should be identified and the use of the system data should be outlined in the system security plan.

2) What are the retention periods of data in the system?

The system owner should consult with the Program Records Official and the Liaison Officer to obtain appropriate NARA approved records disposition schedules.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The system owner should consult with the Program Records Official and the Liaison Officer to obtain information on how the records should be retained, destroyed or transferred.

4) Is the system using technologies in ways that the DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

This section should describe all new system technologies. If there are no new technologies you should answer no.

5) How does the use of this technology affect public/employee privacy?

This section should describe any enhancements to the system and the level of controls that were put in place to protect the data.

6) Will this system provide the capability to identify, locate, and monitor individuals?

The response to this section and sections 7 and 8 should address any tracking and monitoring of individuals to whom the information pertains. This does not include system audit trails, user activity, logon attempts or access to data.

7) What kinds of information are collected as a function of the monitoring of individuals?

See section 6.

8) What controls will be used to prevent unauthorized monitoring?

See section 6.

9) Under which Privacy Act system of records notice does the system operate?

If you do not know the Privacy Act system of records notice, contact the Headquarters Privacy Act Officer. The Privacy Act requires publication of a notice in the *Federal Register* describing each system of records subject to the Act. Any officer of 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 $5,000.

If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system of records. However, even if information may not be subject to the Privacy Act requirements, the information may be protected from disclosure under the Freedom of Information Act.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

The system may already have a Privacy Act system of records notice that applies. However, the Privacy Act requires that amendments to an existing system or the creation of a new system must be published in the *Federal Register* and notice sent to OMB and Congress. Consult with the Headquarters Privacy Act Officer.

F. <u>Access to Data:</u>

1) Who will have access to the data in the system?

Usually access to data is on a need-to-know basis in accordance with the roles and responsibilities of an individual. This section should describe who will have access to the data, e.g., contractors, system administrators. NIST 800-53A provides access control to data and should be incorporated and documented in the systems security plan. In addition, if the data is in a system of records you should include those who may have access in the "Routine Use" section of the notice.

2) How is access to the data by a user determined?

The system owner determines who has access; however, access to data is on a need-to-know basis in accordance with the job roles and responsibilities of individuals.

3) Will users have access to all data on the system or will the user's access be restricted?

Usually access to data is on a need-to-know basis in accordance with the job roles and responsibilities of individuals. It may not be necessary to provide all individuals access to all of the data. Individuals could be provided access to only part of the data maintained in the system.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

This section should summarize the controls that are in place to prevent misuse of the data. Details of these controls should be outlined in the security plan for the system.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?

When a contract provides for the operation of a Privacy Act system of records on behalf of the DOE, the Privacy Act requirements and Departmental regulations on the Privacy Act must be applied to such a system. The Federal Acquisition Regulations also require that certain information be included in contract language and certain processes must be in place.

6) Do other systems share data or have access to the data in the system? If yes, explain.

This question deals primarily with interfaces between processes, systems and applications. You should identify any systems that share or may have access to the system, and specify the purpose for the access. This should be discussed in the security plan and a Memorandum of Understanding should be in place to manage and control the interface.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

All employees and contractor employees who have access to information in a Privacy Act system of records have a responsibility of protecting personal information subject to the Privacy Act; however, the system owner and system manager share responsibilities.

8) Will other agencies share data or have access to the data in this system?

This question concerns agencies outside of the DOE. If you are not sure if other agencies share data or have access to the data in the system/application/process, you should contact either the owner of the data or the IT services group.

You must first review appropriate Privacy Act systems of records notices to determine whether any information obtained from an existing Privacy Act system of records allows for its exchange and use for these new purposes or uses. There are statutory restrictions on use and disclosure of information obtained from a Privacy Act system of records. Please consult with your Headquarters Privacy Act Officer.

9) How will the data be used by the other agency?

If data is being shared with another agency, has the DOE entered into a Matching Agreement with the other agency? Refer to OMB Memo M 01-05 dated December 20, 2000 "Interagency Sharing of Personal Data" at http://www.whitehouse.gov/OMB/memorandum/m01-05.html.

10) Who is responsible for assuring proper use of the data?

This may be stipulated in the language contained in the inter-agency agreement.

Section III

Definitions

1. ***Accuracy*** – to assure within sufficient tolerance for error the quality of the record in terms of its use in making a determination.

2. ***Completeness*** – all elements necessary for making a determination are present before such determination is made.

3. ***Determination*** – any decision affecting an individual which, in whole or in part, is based on information contained in the record and which is made by any person or agency.

4. ***Individual*** – means a citizen of the United States or an alien lawfully admitted for permanent residence.

5. ***Information in Identifiable Form*** – is 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. (These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.)

6. ***Information Technology (IT)*** – means, as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

7. ***Maintain*** – includes collect, use or disseminate.

8. ***Major Information System –*** a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.

9. ***National Security Systems*** – means, as defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but

does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

10. ***Necessary*** – a threshold of need for an element of information greater than mere relevance and utility.

11. ***Personally Identifiable Information (PII) (as defined by OMB)*** – any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. In some instances PII overlaps with Privacy Act information.

12. ***Privacy Impact Assessment (PIA)*** – is 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.

13. ***Privacy Policy in Standardized Machine-Readable Format*** – means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

14. ***Record*** – any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency.

15. ***Relevance*** – a limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

16. ***Routine Use*** – with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

17. ***System of Records*** – a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

18. ***Timeliness*** – sufficiently current to ensure that any determination based on the record will be accurate and fair.

Section IV

References and Related Documents

1. The Privacy Act of 1974, as amended, 5 U.S.C. 552a.

2. DOE regulations implementing the Privacy Act, Title 10, Code of Federal Regulations (CFR) Part 1008.

3. The Freedom of Information Act (FOIA), 5 U.S.C. 552.

4. DOE Regulations Implementing the FOIA, 10 CFR Part1004.

5. DOE Privacy Act Systems of Records, is available by clicking on the FOIA link at the bottom of www.energy.gov.

6. DOE Cyber Security Program Protection of Sensitive Unclassified Information, Including Personally Identifiable Information Guidance, DOE CIO Guidance CS-38A.

7. The Federal Acquisition Regulations (FAR) 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 to the contractor and its employees working on the contract (FAR 48 CFR 24.102(a)).

8. FAR Contracting Officers and System Managers responsibilities (FAR 48 CFR 24.103).

9. Children's On-Line Privacy Protection Act of 1998, Title XIII, Section 1301.

10. COPPA – Children's On-Line Privacy Protection, www.ftc.gov and www.coppa.org/comply.htm.

11. Office of Management and Budget (OMB) Memorandum Privacy Policies on Federal Web Sites, M-99-18, dated June 2, 1999.

12. OMB Memo Privacy and Personal Information in Federal Records, M-99-05, dated May 14, 1998.

13. Letter from OMB Office of Regulatory Affairs, Administrator, John Spotila, on the Use of "Cookies" on Federal Government Web Sites, dated September 5, 2000.

14. OMB Memo M-00-13, “Privacy Policy and Data Collection on Federal Web Sites,” dated June 22, 2000.

15. General Accounting Office (GAO) Report, GAO-01-147R, “Internet Privacy, Agency Use of Cookies,” dated October 20, 2000.

16. GAO Report, GAO-01-424, “Internet Privacy, Implementation of Federal Guidance for Agency Use of Cookies,” dated April 2001.

17. OMB Circular A-130, “Management of Federal Information Resources.”

18. Section 208 of the E-Government Act of 2000.

19. OMB Memo M-03-22, “OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002.”

20. OMB Memo M-05-08, “Designation of Senior Officials for Privacy,” dated February 11, 2005.

21. OMB Memo M-06-15, “Safeguarding Personally Identifiable Information,” dated May 22, 2006.

22. OMB Memo M-06-16, “Protection of Sensitive Agency Information,” dated June 23, 2006.

23. OMB Memo M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” dated July 12, 2006.