National Archives and Records Administration

NARA 1609
September 30, 2009

SUBJECT: Initial Privacy Reviews and Privacy Impact Assessments

Part 1 General

1609.1 What is the purpose of this directive?

This directive provides procedures and requirements for completing Initial Privacy Reviews (IPRs) and Privacy Impact Assessments (PIAs).

1609.2 Authorities for this directive

a. Federal Statutes

(1) Federal Records Act (44 U.S.C. § 2108);

(2) Privacy Act of 1974, as amended (5 U.S.C. § 552a);

(3) Freedom of Information Act, as amended (5 U.S.C. § 552);

(4) Federal Information Security Management Act of 2002 (44 U.S.C. § 3541);

(5) E-Government Act of 2002 (44 U.S.C. § 3501, note);

(6) Paperwork Reduction Act of 1995 (44 U.S.C. §§ 3501-3520);

(7) Information Technology Management Reform Act, also known as the Clinger-Cohen Act of 1996 (40 U.S.C. §§ 1401-1503).

b. OMB Issuances

(1) OMB Circular A-130, "Management of Federal Information Resources" issued November 28, 2000;

(2) OMB Memorandum M-03-22, "Implementing the Privacy Provisions of the E-Government Act," issued September 26, 2003;

(3) OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," issued May 22, 2006;

(4) OMB Memorandum M-06-16, "Protecting Sensitive Agency Information," issued June 23, 2006; and

(5) OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” issued May 27, 2007.

1609.3 Definitions

The following definitions apply to terms used in this directive:

a. **Information in identifiable form –** information in an IT system or online collection:

(1) That directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, e-mail address, etc.); or

(2) 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).

b. **Information Technology (IT) –** 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.

c. **Information Technology (IT) Privacy –** the protection of personally identifiable information (PII) that is collected from individuals through information collection activities or from other sources and that is maintained by NARA in its information technology (IT) systems.

d. **Initial Privacy Review (IPR) –** an initial assessment of an IT system to determine if it contains personally identifiable information (PII).

e. **Personally Identifiable Information (PII) –** information that can be used to distinguish or trace an individual's identity, such as name, social security number, medical or biometric records, either alone, or combined with other personal or identifying information that may be linked to a specific individual, such as date and place of birth and mother's maiden name.

f. **Privacy Impact Assessment (PIA) –** an analysis of how personally identifiable information is collected, used, disseminated and maintained:

(1) To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) To determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and,

(3) To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks to an individual.

1609.4 Responsibilities

a. **Chief Information Officer (CIO), NH –**

(1) Provides oversight and technical assistance to all system owners during the IPR and PIA process,

(2) Is the final approval authority for all PIAs, and

(3) Transmits final PIAs to OMB consistent with OMB instructions.

b. **Senior Agency Official for Privacy (SAOP), NGC –**

(1) Develops IPR and PIA templates and instructions on how to complete them,

(2) Provides guidance and assistance on meeting OMB and NARA privacy requirements,

(3) Reviews and analyzes each IPR and PIA and recommends approval to the CIO, and

(4) Publishes approved PIAs on NARA's web site.

c. **Chief Information Security Officer (CISO), NHI –** is responsible for managing the NARA IT Security Program, with the mission and resources to ensure agency compliance with FISMA and other government-wide IT security policies through the development, implementation, and management of NARA IT systems. The CISO works with system owners and the Senior Agency Official for Privacy to resolve technical issues that impact on privacy.

d. **Inspector General –** evaluates and provides recommendations for NARA's PIA compliance in accordance with FISMA and related laws and regulations.

e. **Office heads/staff directors, Presidential library directors, and regional administrators –** ensure compliance with this directive within their respective offices.

f. **System administrators –** implement, operate, and monitor all NARA IT systems in compliance with established protocols to ensure that personally identifiable information is only accessed by appropriate users who need access to that information to perform their work.

g. **System owners –** are responsible for completing IPRs to determine if an IT system contains personally identifiable information. If the IPR results in the need for a PIA, the system owner is responsible for ensuring that the PIA is submitted to the Senior Agency Official for Privacy for review and approval. The system owner also monitors compliance with security and privacy provisions in each PIA for each IT system under his or her authority. The System Owner has the responsibility to structure system design to control access to PII and protect it from disclosure. The System Owner must also operate and maintain the system in such a way as to protect this data.

h. **System Users –** adhere to the terms of NARA acceptable use policy (see NARA 802, Appropriate Use of NARA Office Equipment) and all other privacy and security requirements.

1609.5 What systems are covered by this directive?

This directive applies to all NARA owned information technology systems and new electronic information collections in identifiable form from the public.

Part 2 Initial Privacy Reviews (IPRs)

1609.6 What is the purpose of conducting an IPR?

An IPR helps determine if personally identifiable information is collected, used or maintained within a NARA owned IT system or a new electronic information collection. For IT systems, the IPR must be completed as part of the overall Security Plan and must be completed during the creation of the project plan to guide the development, budget and schedules of the new system under NARA's System Development Guidelines. For electronic information collections, the IPR must be completed before initiating the new information collection. If any changes are required to be made to the IT System Security Plan, those changes may need to take into account and be reconciled with the information contained within the IPR.

1609.7 What systems need an IPR?

All new IT systems and electronic information collections must complete an IPR prior to connecting the system to the NARA IT Network or prior to collecting information in identifiable form from the public. System owners of all NARA IT systems and users responsible for NARA initiated electronic information collections from the public must complete an IPR using NA 8011, provided in Appendix A.

1609.8 What is the process for review of the Initial Privacy Review?

When a system owner conducts an IPR, they must determine whether the IT system or information collection evaluated contains personally identifiable information. He or she must confirm their determination in the IPR and submit it to the Senior Agency Official for Privacy (SAOP) for review and approval. The SAOP transmits the IPR to the CIO for final approval.

Part 3 Privacy Impact Assessments (PIAs)

1609.9 Why are IT system owners required to complete PIAs?

A Privacy Impact Assessment (PIA) must be completed for all IT systems and electronic information collections that are found to contain personally identifiable information. IT system owners are required to complete PIAs to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system and to demonstrate that they have consciously incorporated privacy protections throughout the development life cycle of a system or program. The E-Government Act requires agencies to conduct a PIA before:

a. Developing or procuring 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).

1609.10 What must the PIA address?

The PIA must analyze and describe:

a. What information is being collected (e.g., nature and source);

b. Why the information is being collected (e.g., to determine eligibility);

c. The intended use of the information (e.g., to verify existing data);

d. Who has access to that information, either physically or through other means (whether full access or limited access rights);

e. With whom the information will be shared (e.g., another agency for a specified programmatic purpose);

f. What administrative controls and guidance are in place to ensure that only information that is necessary and relevant to NARA's mission is maintained in the system; and

g. Whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a.

1609.11 When must a PIA be conducted?

PIAs are required for all NARA owned IT systems and new electronic information collections. PIAs must be conducted prior to the launch of a new system or electronic information collection when:

a. An IPR identifies that a NARA owned IT system or electronic information collection contains PII;

b. NARA begins to develop a new IT system that an IPR has identified will contain PII;

c. A NARA owned IT system previously designated as containing PII is significantly modified as detailed in para.1609.12, below, and confirmed by an annual review conducted by the System Owner and the SAOP; or

d. A new electronic information collection containing PII is being proposed.

System owners must notify NGC annually of any modifications to any IT system or electronic information collection which has a PIA and submit a newly amended PIA prior to the end of the fiscal year in which the modification was made. System owners for NARA IT systems that do not have any modifications to report must also confirm in writing to NGC that there are no changes in status to the NARA owned IT system prior to the end of the fiscal year.

1609.12 What are examples of when a PIA must be completed for an IT system or when a PIA must be modified?

Complete or modify a PIA when:

a. A paper based records system is converted to an electronic system;

b. An existing electronic system is modified so that previously anonymous information becomes identifiable to specific individuals;

c. New uses of an existing IT system, such as the application of new technologies, significantly change how PII is managed in the system;

d. Databases or other information systems holding PII are merged, centralized, matched with other information systems, or otherwise significantly manipulated;

e. User-authenticating technology (e.g., password, digital certificate, or biometric) is newly applied to an electronic information system accessed by members of the public;

f. Alteration of a business process results in significant new uses, disclosures of information, or incorporation into the system of additional items of PII;

g. New PII that is added to the system increases the risks to personal privacy (e.g., the addition of medical or financial information);

h. A system with PII is relocated to a remote site or a facility not under the direct control of NARA (e.g., a contractor's processing facility); or,

i. NARA is initiating, consistent with the Paperwork Reduction Act, a new or significantly revised electronic collection of information in identifiable form for 10 or more persons.

1609.13 When is a PIA not required?

If a completed IPR determines that no PII exists within the IT system or electronic information collection, a PIA is not required. A PIA also may not be required when information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged. Examples of additional circumstances that may not require the completion of a PIA may include, but are not limited to:

a. NARA-run web sites, IT systems, or collections of information that do not collect or maintain PII;

b. 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;

c. National security systems defined at 40 U.S.C. § 11103 as exempt from the definition of information technology;

d. 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;

e. When system owners are developing IT systems or collecting non-personally identifiable information for a discrete purpose that does not involve matching with or retrieval from other databases that generate PII;

f. Minor changes to an IT system or collection that do not create new privacy risks; or,

g. For legacy systems and currently operational systems that have had a previous PIA completed, a new one is not required unless a major upgrade or significant change relative to the content or protection of data within the system is anticipated.

1609.14 What must the PIA cover?

The PIA is an analysis of how PII is handled, including the physical and technical safeguards that are in place to protect such information from inappropriate disclosure. NARA offices writing PIAs must answer all the questions in the PIA form, NA 8012, provided in Appendix B.

1609.15 How much information needs to be included in the PIA?

The depth and content of the PIA must reflect the size and nature of the information system being assessed, the sensitivity of the information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information. For example, PIA statements for major information systems must reflect a more extensive analysis of the consequences of the collection and flow of information; the alternatives to collection and handling as designed; privacy risk mitigation measures for each alternative; and, the rationale for the final design choice or business process. System owners must answer all questions asked in Appendix B; they should, however, feel free to supplement that information with additional information concerning the nature and scope of the system and how those factors impact on the protection of PII within the system.

1609.16 What is the relationship between the PIA and requirements under the Paperwork Reduction Act?

a. All new electronic information collections subject to the Paperwork Reduction Act must be submitted to OMB for review and approval. NARA units undertaking new information collections using electronic means for collecting, processing, or storing the information must conduct an IPR. If the results of the IPR indicate that a PIA is required, the resulting PIA must be submitted to OMB with the information collection request unless the PIA has already been submitted to OMB as part of the business case development process.

b. NARA units are not required to conduct a new PIA for simple renewal requests for information collections under the Paperwork Reduction Act. However, units must separately consider the need for a PIA when amending an information collection request to collect information that is significantly different in character from the original collection. Please see NARA 108, Information Collection, for additional information.

1609.17 What is the process for review and approval of the PIA?

System owners must submit draft PIAs to the SAOP for review. The SAOP and the NARA Privacy Act Officer review the PIA and work with the system owner or system manager to resolve any concerns. When the PIA has been approved by the SAOP, it is submitted to the CIO for final approval. As appropriate, the CIO submits the PIA to OMB. System owners have the responsibility of ensuring that the information contained within both IPRs and PIAs is complete and accurate.

1609.18 How are PIAs published or disclosed to the public?

Appendix A, Section II, C3 of OMB memo M-03-22, "Implementing the Privacy Provisions of the E-Government Act," requires that PIAs or summaries be made publicly available. Accordingly, NARA publishes all approved PIAs on the NARA privacy web page, http://www.archives.gov/foia/privacy-act/.

Part 4 Records Management

1609.19 How are Initial Privacy Review and Privacy Impact Assessment records created by this directive maintained under the NARA records schedule?

a. NGC and the SAOP maintain records under NARA file no. 1103-6, “FOIA/PA (Advice/Operations).”

b. NH (CIO) maintains the official record copy of IPRs and PIAs in accordance with

NARA 801-2, para. 13.

c. System managers, system owners, CISO and staff maintain records of IPRs and PIAs under file no. 812, Oversight and Compliance File or 814-1, Financing of IT Resources and Services, as appropriate.

d. NHI (IT Security Staff) maintains records of IPRs and PIAs under NARA file no. 830-2 “Documents identifying IT risks . . . .”

Appendix A

INITIAL PRIVACY REVIEW (IPR)
Name of Project (include recognized acronyms as appropriate)
CONTACT INFORMATION
Who is completing this document?
Name
Title
Organization

Phone ( ) -	e-mail . @ nara.gov	other contact info

Who is the system owner (product owner)?
Name
Title
Organization

Phone ( ) -	e-mail . @ nara.gov	other contact info

Who is the system manager (project manager) for this system or application?
Name
Title
Organization

Phone ( ) -	e-mail . @ nara.gov	other contact info

SYSTEM APPLICATION/GENERAL INFORMATION:

Does this system contain any information about individuals? □ **Yes** □ **No**

If so, is this information identifiable to specific individuals? □ **Yes** □ **No**

If you answered **NO** to this question, you are affirming that the IT system being evaluated does not collect, maintain or use any personally identifiable information. You do not have to complete a Privacy Impact Assessment for this system. Please have the proper NARA officials sign the signature page.

If you answered **YES** to this question, you need to complete a Privacy Impact Assessment (PIA). (There is no need to have the IPR approved if you must complete a PIA for the system. Please attach the IPR to your completed PIA prior to submission for approval. See the attached template for minimum PIA requirements.)

Appendix A

Initial Privacy Review Approval	
System Owner (Product Owner)	
(Signature)	(Date)
(Name, please print or type)	
System Manager (Project Manager)	
(Signature)	(Date)
(Name, please print or type)	
Senior Agency Official for Privacy (or designee)	
(Signature)	(Date)
(Name, please print or type)	
Chief Information Officer (or designee)	
(Signature)	(Date)
(Name, please print or type)	

Appendix B

Privacy Impact Assessment (PIA)

Name of Project:	
Project's Unique ID:	
Legal Authority(ies):	

Purpose of this System/Application:

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		
External Users		
Audit trail information (including employee log-in information)		
Other (describe)		

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

NARA operational records		
External users		
Employees		
Other Federal agencies (list agency)		
State and local agencies (list agency)		
Other third party source		

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

2. Is there another source for the data? Explain how that source is or is not used?

Section 3: Intended Use of this Information

1. 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?

2. Will the new data be placed in the individual’s record?

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

4. How will the new data be verified for relevance and accuracy?

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

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

7. Generally, how will the data be retrieved by the user?

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an 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. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.

12. What kinds of information are collected as a function of the monitoring of individuals?

13. What controls will be used to prevent unauthorized monitoring?

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

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

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

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 inserted in their contracts and other regulatory measures addressed?

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

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

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

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

3. What are the retention periods of data in this system?

4. 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? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

6. How does the use of this technology affect public/employee privacy?

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?

8. Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

2. If so, what changes were made to the system/application to compensate?

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

Appendix B

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
(Signature)	(Date)
Name:	
Title:	
Contact information:	
Senior Agency Official for Privacy (or designee)	
(Signature)	(Date)
Name:	
Title:	
Contact information:	
Chief Information Officer (or designee)	
(Signature)	(Date)
Name:	
Title:	
Contact information:	