Privacy Impact Assessment (PIA)

Name of Project: Electronic Records Archive (ERA)

Project's Unique ID: ERA 393-00-01-03-01-0001-00

Legal Authority(ies):	**This Privacy Impact Assessment (PIA) serves to document the types of personal information protected under the Privacy Act (PA; 5 United States Code (U.S.C.) 552a, as amended), under the personal privacy exemption of the Freedom of Information Act (FOIA; 5 U.S.C. 552, as amended), or under the Presidential Records Act (PRA; especially 44 U.S.C. 2204) that the ERA System will process and store. Furthermore, this PIA incorporates directives documented in the Office of Management and Budget (OMB) Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of Act 2002. Directives stated in OMB M-04-04, E-Authentication Guidance for Federal Agencies; OMB M-05-04, Policies for Federal Agency Public Websites; and OMB M-06-16, Protection of Sensitive Agency Information will be addressed in ERA specific content as the ERA system matures. The PIA is required by OMB Circular A-11, Preparation, Submission and Execution of the Budget; OMB Exhibit 300, Capital Asset Plan and Business Case; and Sec. 208 of the E-Government Act of 2002.**

Purpose of this System/Application: The ERA System is intended to preserve authentically any type of electronic record, created using any application on any computing platform, delivered electronically and on any digital medium, from any entity in the Federal Government and any donor, and to provide discovery and delivery to anyone with an interest and legal right of access, now and for the life of the republic. The ERA System is intended to support selected archival management tasks for non-electronic records, such as the scheduling and appraisal functions.

Section 1: Information to be Collected

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

Employees		Users of the ERA system - user registration and identification, access rights, and system use data. Information gathered in accordance to NIST Guidelines 800-53 Recommended Security Controls For Federal Systems. This information is used to enforce access control. No personal information is requested, only agency specific information, such as work phone number, work address, etc. The fields required to create and account in ERA are: First Name, Middle Name, Last Name, Jobe Title, E-mail, Telephone Number, Fax Number, Employee or Contractor, Agency Name, Agency Address, Agency Major Division, Agency Minor Division, Request ERA Role, Security Question (for password reset),

		Security Answer, Designated Account Representative, NARA Account Representative.
External Users		Users of the ERA system - user registration and identification, access rights, and system use data. Information gathered in accordance to NIST Guidelines 800-53 Recommended Security Controls For Federal Systems. This information is used to enforce access control. No personal information is requested, only agency specific information, such as work phone number, work address, etc. Public users of OPA are not required to provide any information for basic use of the system. Advanced use of OPA requires personal information to create an account. The sole personal information gathered by OPA to create and account is a username, password and e-mail address. The e-mail address does not specify work or personal, so users are given the option to give any e-mail address they chose.
Audit trail information (including employee log-in information)		The only anticipated consolidation of personally identifiable data will be in the accumulation of back up media and audit trails pertaining to system usage. Backup information and audit logs stored outside the ERA security boundary are encrypted. The audit data contains login information such as username for each access to ERA and OPA. When accounts are created in ERA and OPA all fields are included in audit data.
Other (describe)		
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		Information on individuals contained in records stored in the ERA system, but are under the legal control of the Federal agency that created the records. Information subject to the full requirements of the PA and governed by the PA systems of records of the originating agencies with NARA providing access only as specifically authorized by each agency. Additionally access under FOIA (5 U.S.C. § 552, as amended) is also provided by NARA as implemented by the originating agency.
External users		N/A
Employees		N/A
Other Federal agencies (list agency)		Information on individuals contained in Federal records stored in the ERA system as accessions of the National Archives (under the legal control of NARA). Information subject to the FOIA that may not be releasable under exemptions (b)(6) and (b)(7)(C) of the FOIA. Note: Accessioned records are specifically exempt from most provisions of the PA. Information on individuals contained in Presidential records stored in the ERA system by NARA and under its legal control. Information not subject to the PA but controlled by the PRA (44 U.S.C. Chapter 22); Presidential Executive Order 13489, further implementation of the PRA; and the privacy exemptions - (b)(6) and (b)(7)(C) - of the FOIA. Information on individuals contained in records of the Congress, legislative

		branch agencies, and judicial branch records contained in the ERA system. Information not subject to the PA, but controlled by directions of the originating governmental body. Data is expected to be provided by all federal agencies, starting with: • U.S. Patent and Trademark Office • Naval Oceanographic Office • National Nuclear Security Administration • U.S. Bureau of Labor Statistics • Executive Office of the President G.W. Bush Administration. Some of these records will remain under the legal authority of the originating agency. The originating agency's statutes and policies will govern the personal data in such records, and the records will be maintained in accordance with authorized records schedules. Other records will be accessioned into the National Archives of the United States where they will be subject to NARA's regulations and procedures for protection of personal data in archival materials.
State and local agencies (list agency)		No state or local governmental agencies will provide data directly to NARA for use in the ERA system. However, there may be personal data, previously received by Federal agencies from state and local government sources, that is present in the Federal records stored in the ERA system.
Other third party source		Information on individuals contained in donated archival materials. Information not subject to the PA, but controlled by directions of the donor's deed of gift. As indicated above, the holdings of the National Archives of the United States, the Presidential Libraries, and the NARA Records Centers stored in the ERA system will include documentary materials from other sources and originators, including items received as donations and deeds of gift. Any personal data contained in such holdings will be managed in accordance with applicable laws, regulations, policies, deposit agreements, or deeds of gift. Apart from such holdings, NARA intends to collect data needed in the operation and use of the ERA system directly from the subject individuals as much as possible.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
ERA and OPA request the minimum information required to uniquely identify users as well as provide contact information which is used to determine or verify access to data stored within the system.

Data identifying ERA users and their access rights, and describing their use of the ERA system will be necessary for system management and security and as a control against fraud, waste, and abuse.

Development and implementation of the ERA system is essential to allowing NARA continued fulfillment of its mission to ensure, for the private citizen and all branches of the Government, ready access to essential evidence that documents the rights of citizens, the actions of Federal officials, and the national experience, and protect the rights and entitlements of the individuals they identify. Providing preservation of, and ready access to, the data contained in records temporarily or permanently stored in ERA is the purpose of the ERA system.

2. Is there another source for the data? Explain how that source is or is not used?
The information is not available from a different source.

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?
ERA will not create new personally idenfifiable data through information aggregation.

2. Will the new data be placed in the individual's record?
N/A

3. Can the system make determinations about employees/the public that would not be possible without the new data?
No potential effects anticipated. No personally identifiable data is expected to be derived by the ERA system.

4. How will the new data be verified for relevance and accuracy?
For ERA users, the currency of the data provided for user registration and for use in identification and authentication of users will be verified at the time of registration and granting of access rights. NARA implements procedures for updating user data appropriately (e.g., routine notification when an employee separates from services or changes positions).

For holdings of records that remain under the legal control of the originating agency, this element is not applicable because NARA grants access to such records only when authorized to do so by the originating agency. NARA is responsible for providing access to and enforcing the appropriate access rights of individuals as provided by the originating agency. Additional information will be added in future updates to this document as the ERA system design matures.

For archival records in the legal custody of NARA, the data in the records must remain unchanged from what it was at the time NARA assumed custody in order for the records to remain authentic. In order to protect personal privacy of living persons, NARA screens name retrievable files, investigatory files, and other records likely to contain personal information under FOIA exemptions stated in 5 USC 552(b)(6) and (b)(7)(C). NARA provides redacted copies of textual records and public use versions of

electronic records.

For ERA system users, individuals will be responsible for supplying complete account data as needed by NARA to manage access rights. The methodology for confirming completeness is defined in the ERA Account Management Document, Version 3.4, 2010.

For archival materials, completeness is the responsibility of the originating source. These records will be compared against the planned content resulting from the schedule and appraisal process. Once these archival materials have been processed for long-term preservation, ERA will implement controls for maintaining and determining the integrity of these preserved records. For the records of other Federal agencies that may be temporarily stored in ERA, completeness is the responsibility of the originating agency.

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

NARA staff and government contractors responsible for managing and operating the ERA system will have access to the PII data about ERA system users. Help Desk staff responsible for responding to users requests for assistance will have access to data necessary to provide such response. ERA users performing system management can retrieve user account information by a search on a unique user identifier or user name. Reports containing User Name, Agency, Role and account status (active or terminated) are published to NARA Staff monitoring User Account usage.

Authorized employees of other Federal agencies retain responsibility for determining who should have access (and what those access rights are) to records stored in the ERA system. The ERA users from external agencies supply the ERA user account information, but do not have access to it within the ERA system.

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

Management, operational, and technical controls to prevent misuse of data by those with privileged access will be selected in accordance with NIST SP 800-53/FIPS PUB 200. These ERA system components that implement these controls detect unauthorized access and unauthorized monitoring. Transportation of ERA PII data outside the boundary of ERA physical control is encrypted to prevent unauthorized access.

NARA does not plan to consolidate or link data about ERA system users with other files or systems.

NARA does not plan to offer any services for consolidation of files or systems of records preserved in the ERA system.

7. Generally, how will the data be retrieved by the user?
The following restrictions on user access to information apply to ERA.

- For NARA operational PII data - NARA Delegated Account Representatives (DAR) will have user account information for those users they recommend for ERA accounts. The DAR will not have access to any other ERA user information. Appropriate ERA system maintenance staff will have access to all user account information. Appendix C contains account information.
- For agency records stored temporarily in ERA – Authorized employees of other Federal agencies retain responsibility for management of and access to those agencies' legally controlled records that are stored in ERA.
- For archival materials in ERA - the information that will be processed by ERA is substantially the same as that which is currently made available electronically or on paper. Therefore, access restrictions will be (at a minimum) the same as currently in place.

As specified in 5 U.S.C. 552a (l)(3), federal records transferred to NARA are not subject to most of the PA provisions. NARA's implementation of FOIA regulations (36 CFR 1250), governing access to records containing personal information, will also apply to the access of electronic materials that will be contained in ERA.

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.
Help desk and support staff with access to the authentication system can retrieved data by searching on username, first name, last name or e-mail address. SSN and other PII data is not stored in the system.

Data about registered ERA system users will be retrievable by personal identifiers from privileged users who maintain ERA. The ERA account request forms maintained by the DARs are not retrievable by personal identifiers. These forms are maintained in date order when the ERA account is requested.

Where allowed, appropriately controlled and enabled by capabilities in the ERA system, information from archival materials will be retrievable by personal identifier. Such retrieval is necessary to satisfy two (2) major types of demands for retrieval to archival records: for family history, and for historical studies of Federal officials and other prominent individuals.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
Reports are not produced specifically on individuals. Regular reports can be generated on system accounts that have passed thresholds for inactivity or expiration. These reports are generated for maintenance of the system and are not determined by individual's information.s

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
ERA and OPA differentiate users to determine access to the system. OPA allows everyone to access data stored on the system, but requires users to register in order to save results and provide additional features. Specific NARA employees have elevated access to manage and approve user comments and tagging abilities.

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.
No.

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

13. What controls will be used to prevent unauthorized monitoring?
The ERA system implements controls to prevent unauthorized system monitoring. Hardware and software used within ERA is subject to Configuration Control Board (CCB) approval. The CCB and the ERA security officer will not approve devices which would permit unauthorized monitoring. The ERA System implements controls to monitor unauthorized use with accountability and audit. These controls detect who accesses ERA PII information and account information.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
ERA and OPA use session cookies to maintain sessions for users, but do not create persistent cookies for user identification.

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)?
NARA staff and government contractors responsible for managing and operating the ERA system will

have access to the PII data about ERA system users. Help Desk staff responsible for responding to users requests for assistance will have access to data necessary to provide such response. ERA users performing system management can retrieve user account information by a search on a unique user identifier or user name. Reports containing User Name, Agency, Role and account status (active or terminated) are published to NARA Staff monitoring User Account usage.

Authorized employees of other Federal agencies retain responsibility for determining who should have access (and what those access rights are) to records stored in the ERA system. The ERA users from external agencies supply the ERA user account information, but do not have access to it within the ERA system.

Public users will have access to OPA. OPA only contains data determined applicable for public release.

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?

The following restrictions on user access to information apply to ERA.

- For NARA operational PII data - NARA Delegated Account Representatives (DAR) will have user account information for those users they recommend for ERA accounts. The DAR will not have access to any other ERA user information. Appropriate ERA system maintenance staff will have access to all user account information. Appendix C contains account information.
- For agency records stored temporarily in ERA – Authorized employees of other Federal agencies retain responsibility for management of and access to those agencies' legally controlled records that are stored in ERA.
- For archival materials in ERA - the information that will be processed by ERA is substantially the same as that which is currently made available electronically or on paper Therefore, access restrictions will be (at a minimum) the same as currently in place.

As specified in 5 U.S.C. 552a (1)(3), federal records transferred to NARA are not subject to most of the PA provisions. NARA's implementation of FOIA regulations (36 CFR 1250), governing access to records containing personal information, will also apply to the access of electronic materials that will be contained in ERA.

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

User access is determined by role. Some NARA users have access to all data. Agency users are given access to their own data and may be further segregated by their role within the agency. No public access is granted to ERA. System maintenance staff (by virtue of their elevated privilege) have technical access to the data, but are not given permission to access the data unless it is required to

perform a specific task to maintain the system.

OPA grants access to all data on the system to all users. Registered users are given the ability to create supplmental data sueh as comments or keywords, but are not given any other elevated privilege on the system.

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?

Management, operational, and technical controls to prevent misuse of data by those with privileged access will be selected in accordance with NIST SP 800-53/FIPS PUB 200. These ERA system components that implement these controls detect unauthorized access and unauthorized monitoring. Transportation of ERA PII data outside the boundary of ERA physical control is encrypted to prevent unauthorized access. Continous monitoring is in place to periodically review security controls to determine the effectiveness and viability.

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?

Contractors are involved in the design, development and maintenance of the system. All contractors with access to the system are required to sign Non-Disclosure Agreements (NDA).

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.

Other systems do not have access to ERA data.

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

N/A

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

General responsibility for protecting personal privacy information in materials in NARA's custody rests with the Archivist of the United States in accordance with 5 U.S.C. 552, as amended; 5 U.S.C. 552a, as amended; 44 U.S.C. 2108; 44 U.S.C. 2204; and 44 U.S.C. 2207.

The ERA Designated Approving Authority will have the responsibility for protecting the privacy of personal information that is required submit an account on the ERA system.

For records not yet transferred to NARA's legal custody, NARA will act under the direction and on the behalf of originating agencies to protect privacy.

The NARA Senior Agency Official for Privacy is the NARA General Counsel (NGC). The General Counsel will provide legal guidance and has overall responsibility and accountability for ensuring NARA's implementation of information privacy protections, including NARA's full compliance with federal laws, regulations, and policies relating to information privacy. The ERA Designated Approving Authority will have the responsibility for ensuring the controls implemented within ERA are protecting the privacy of personal information that is specifically stored within the ERA system.

The responsibility of the NARA Office of the Inspector General (OIG) includes, but is not limited to, ensuring compliance with laws, regulations, and internal policies in carrying out the ERA program. As such, the OIG may conduct audits and investigations concerning all aspects of the ERA program, including compliance with laws, regulations, guidelines, and internal policies.

NARA has no direct control over the proper use of privacy data by another agency. It is assumed that the agency has designated an agency level official responsible for privacy per OMB M-05-08, Designation of Senior Agency Official for Privacy; and that in cooperation with the agency's Inspector General will be responsible for assuring proper use of data.

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.

Other agency access to personal information will be governed in accordance with the provisions of the PA, which allows access for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency, or his or her other designated representative, has made a written request to NARA specifying the particular portion desired and the law enforcement activity for which the record is sought.

With regard to non-PII, other agencies have access to their own data, and no other data residing in ERA.

Data collected about ERA system users will be used for the responsible management and protection of the ERA system and the information contained within it (i.e., verification of user ID, prosecution of users for improper or illegal use of data, and deterrence to unauthorized system access and improper use of data).

Data collected about ERA system users will be used for the responsible management and protection of the ERA system and the information contained within it (i.e., verification of user ID, prosecution of users for improper or illegal use of data, and deterrence to unauthorized system access and improper use of data).

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?

ERA Account Management form lists the data required for an account on the system. The required fields are designated and users can decline providing the additional information. The required fields are needed for access to ERA.

OPA can be browsed anonymously, but requires a usemame, password and e-mail address to create an account. If users do not wish to provide this information to NARA, they cannot create an account, but are allowed to browse and view all data.

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

N/A

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.).

Relevant information collected by the ERA system will be verified, to the extent practicable, for accuracy, and that the information is current and complete. This information will be used to verify the identity of ERA users to ensure the privacy protection of records within ERA. The electronic account information stored in ERA is verified for accuracy, relevancy, timeliness, and completeness on an annual basis.

The originating/transferring entities (external to NARA itself) are responsible for the quality (accuracy, relevancy, timeliness, and completeness) of data for documentary materials that are transferred to NARA for storage in the ERA system. However, the ERA system will provide the capability to replace a record that has been identified as being incorrect by the originating or transferring entity with a newly modified record submitted by that same entity.

The following ERA Program Management Office (PMO) documentation was used to support the development of this document using the versions listed below unless superseded by a newer version.

- Acquisition Strategy (AS)
- Concept of Operations (ConOps)
- Risk Management Plan (RKM)
- Program Management Plan (PMP)
- Requirements Document (RD)
- System Security Plan (SSP)
- Security Test and Evaluation Plan (STE&P)
- Configurafion Management Plan (CMP)
- ERA Account Management Plan
- Independent Verification and Validation Plan (IVVP)

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?
System is only maintained at one site.

3. What are the retention periods of data in this system?
Data identifying users and their access rights, and describing their use of the ERA system and all resulting transactions, will be retained in within the ERA audit logs for five (5) years. Paper copies of account forms are maintained as long as the account is required by the ERA user. Once the account is retired and no longer needed, the paper account form request may be destroyed.

Federal records will be maintained in accordance with records disposition schedules approved by The Archivist of the United States. Other materials will be retained in accordance with applicable laws, regulations, deposit agreements, or deeds of gift.

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.
All data appraised by NARA as having sufficient historical or other value are transferred to the legal custody of the Archivist of the United States for permanent retention. Thus there will be no procedure for eliminating archival records in ERA.

Procedures for disposal of PII paper records are through shredding. Electronic records stored on media are degaussed. Destruction of storage media devices is compliant with NARA policies.

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.
This information will be added in future updates to the PIA as the ERA system reaches final operating capability.

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

7. **Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?**
ERA and OPA follow the follow Federal and NARA requirements:

- Federal Records Act (ERA), 44 U.S.C. Chaps 21, 29, 31 and 33.
- Responsibility for custody, use, and withdrawal of records, 44 U.S.C. 2108
- Inspection of agency records, 44 U.S.C. 2906
- Presidential Records Act, 44 U.S.C. 2201-07
- Restrictions on access to Presidential Records, 44 U.S.C. 2204
- E-Government Act of 2002, Public Law 107-347, Section 208(b)
- Freedom of Information Act (FOIA)(as amended), 5 U.S.C. 552
- Privacy Act (PA) of 1974 (as amended), 5 U.S.C. 552a
- Code of Federal Regulations (CFR)
- Regulations Implementing the Privacy Act of 1974, 36 CFR §1202
- Public Availability and Use of Federal Records, 36 CFR §1250
- Restrictions On The Use Of Records, 36 CFR §1256
- OMB Circular A-130, "Management of Federal Information Resources." Appendix III, "Security of Federal Automated Information Resources." updated in 2000
- Census – Information as confidential, 13 U.S.C. 9(a)
- NARA Policy Directive - NARA 804, Information Technology (IT) Systems Security and the associated IT Security Handbooks
- NARA IT Security Architecture Version 4.6 (28 Feb 2007)
- Federal Information Security Management Act of 2002 (FISMA), Public Law 107- 347, 44 U.S.C., Sec 3541
- OMB Memorandum M-08-09, New FISMA Privacy Reporting Requirements for FY 2008 (18 Jan, 2008)
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

(12 Jul 2006)
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information (23 Jun 2006)
- OMB Circular A-11, Preparation, Submission and Execution of the Budget (Revised 21 Jun 2005)
- OMB Memorandum M-05-04, Policies for Federal Agency Public Websites (17 Dec 2004)
- OMB Memorandum M-04-04, E-Authentication Guidance (16 Dec 2003)
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (26 Sep 2003)
- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (20 Dec 2000)
- Letter from John Spotila (Chair, CIO Council Office of Information and Regulatory Affairs) to Roger Baker (CIO, Department of Commerce Co-Chair Security, Privacy, and Critical Infrastructure Committee), on clarification of OMB Cookies Policy (5 Sep 2000)
- Letter from Roger Baker (CIO, Department of Commerce Co-Chair Security, Privacy, and Critical Infrastructure Committee) to John Spotila (Chair, CIO Council Office of Information and Regulatory Affairs) on Federal agency use of Web cookies (28 July 2000)

- OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites (22 Jun 2000)
- OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites (2 Jun 1999)
- OMB Memorandum M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information (22 May 2007)
- OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of 14 May 1998, "Privacy and Personal Information in Federal Records" (7 Jan 1999)
- Federal Enterprise Architecture Security and Privacy Profile Phase 1 Final
- Federal Information Processing Standard 200, March 2006, Minimum Security Requirements for Federal Information and Information Systems
- Federal Information Processing Standard 199, December 2003, Standards for Security Categorization of Federal Information and Information Systems
- Federal Information Processing Standard 197, November 2001, Advanced Encryption Standard (AES)
- Federal Information Processing Standard 186-2, January 2000, Digital Signature Standard (DSS)
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I and II
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-55, Security Metrics Guide for Information Technology Systems
- NIST SP 800-44, Guidelines on Securing Public Web Servers

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?**
ERA meets both NARA and Federal laws governing unclassified system. ERA Follows the NIST guidelines and standards which requires risk assessment and continuous monitoring in order to maintain security and information integrity. ERA maintenance staff periodically scans the ERA components to detect unauthorized changes. System Authorization has been granted for ERA and OPA

and continuous monitoring is in place to maintain the accuracy of the security of the systems. A Plan of Action and Milestones (POAM) is maintained to document risks and track actions performed for each risk.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
A System Security Plan (SSP) is documented and maintained for each system. The SSP documents compliance with NIST 800-53 and describes the the security controls in place to protect the system and any data contained. A dedicated staff provides monitoring capabilities for the system. In addition, network monitoring is provided by NARA and other Federal agencies since does not have dedicated network connectivity and relies on common network services.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Information System Security Officer
Ben McElyea
ben.mcelyea@nara.gov
304.726.7821

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.
There is no SOR within ERA at this time.

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

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?
No.

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

<u>See Attached Approval Page</u>

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

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
Mary Winstead (Signature)	8/12/11 (Date)
Name: Mary Winstead	
Title: ERA project manager	
Contact information: 301-837-3167	
Senior Agency Official for Privacy (or designee)	
(Signature)	8/31/11 (Date)
Name: Gary M Stern	
Title: SAOP and General Counsel	
Contact information: 301-837-3026	
Chief Information Officer (or designee)	
(Signature)	8 26 11 (Date)
Name: Michael Wash	
Title: CIO	
Contact information: 301-837-1992	