

ELECTRONIC RECORDS ARCHIVES

PRIVACY IMPACT ASSESSMENT (PIA v 6)

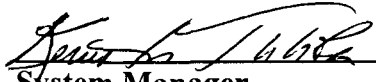
for the

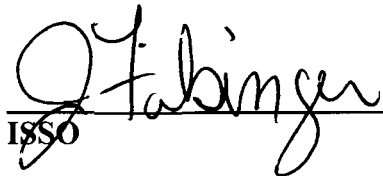
**NATIONAL ARCHIVES AND
RECORDS ADMINISTRATION**

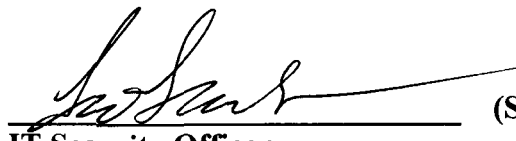
**ELECTRONIC RECORDS ARCHIVES
PROGRAM MANAGEMENT OFFICE
(NARA ERA PMO)**


September 27, 2008

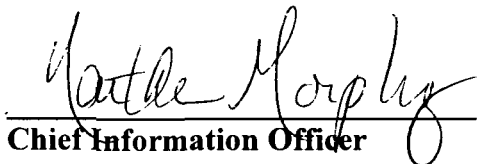
The Following Officials Have Approved this PIA

 (Signature) 9.30.08 (Date)
System Manager

 (Signature) 15 Oct '08 (Date)
ISSO

 (Signature) 10/1/08 (Date)
IT Security Officer

 (Signature) 10/2/08 (Date)
Senior Agency Official for Privacy

 (Signature) 10/1 08 (Date)
Chief Information Officer

ERA Program Management Office (ERA PMO)

Document Change Control Sheet

Document Title: Privacy Impact Assessment (PIA)

Date	Filename/version #	Author	Revision Description
08/30/02	ERA.DC.PIA.1.0.doc	Dr. Allen Church	Baseline PIA
06/25/03	ERA.DC.PIA.2.0.doc	Dr. Allen Church	Revision following IV&V review Refer to ERA Documentation Review Comment Form for PIA.
09/10/04	ERA.DC.PIA.3.0.doc	H. Feldman, F. Samuels	Revision to address comments from ERA QM/GRT and NPOL reviews
08/25/05	ERA.DC.PIA.4.0.doc	H. Feldman, F. Samuels	Final of scheduled annual update to PIA to include Government comments from the Deliverable Review Comment Forms. See Change Request: ERA00000720
06/22/06	ERA.DC.PIA.5.0.doc	F. Samuels	Draft of scheduled annual update to PIA. See Change Request: ERA000001066
08/11/06	ERA.DC.PIA.5.0.doc	F. Samuels	Final of scheduled annual update to PIA. See Change Request: ERA000001066. Incorporates Government comments.
7/11/07	ERA.DC.PIA.5.1.doc	J. Filsinger	2007 Update
8/31/08	ERA.DC.PIA.6.0.doc	J. Filsinger	2008 Update

Table of Contents

1	Introduction.....	1
1.1	PURPOSE	1
1.2	ERA PIA PROCESS.....	2
1.3	INFORMATION AND PRIVACY	2
1.4	DOCUMENT CONFORMANCE	2
1.5	ERA PROGRAM OVERVIEW	3
1.6	ACRONYMS	3
2	References.....	4
2.1	APPLICABLE FEDERAL LAWS, MANDATES, NARA REGULATIONS AND POLICIES.....	4
2.2	STANDARDS AND GUIDELINES	5
2.3	ERA PROGRAM MANAGEMENT OFFICE (PMO) DOCUMENTS.....	6
3	Privacy – Data in the ERA System	6
3.1	GENERAL DESCRIPTION OF SYSTEM INFORMATION	7
3.2	SYSTEM INFORMATION SOURCES	9
3.2.1	<i>Which ERA files and databases are used?</i>	9
3.2.2	<i>What Federal Agencies are providing data for use in the ERA system?</i>	9
3.2.3	<i>What State and Local Agencies are providing data for use in the ERA system?</i>	9
3.2.4	<i>What other third party sources will provide data?</i>	9
3.2.5	<i>What information will be collected from the public/employee?</i>	10
3.3	HOW WILL EXTERNAL DATA BE VERIFIED FOR ACCURACY?	10
3.4	HOW WILL DATA BE CHECKED FOR COMPLETENESS?.....	11
3.5	IS THE DATA CURRENT? HOW DO YOU KNOW?	11
3.6	ARE THE DATA ELEMENTS DESCRIBED IN DETAIL AND DOCUMENTED?.....	11
4	Privacy – Access to the Data	12
4.1	WHO WILL HAVE ACCESS TO THE DATA IN THE ERA SYSTEM?.....	12
4.2	USER DATA ACCESS METHODOLOGY	12
4.3	USER ACCESS RESTRICTIONS	13
4.4	CONTROLS TO PREVENT MISUSE OF DATA BY THOSE WITH ACCESS	13
4.5	DO OTHER SYSTEMS SHARE DATA OR HAVE ACCESS TO DATA IN THIS SYSTEM?.....	13
4.6	RESPONSIBLE PARTY FOR PROTECTING THE PRIVACY OF AFFECTED INDIVIDUALS.....	13
4.7	WILL OTHER AGENCIES SHARE DATA OR HAVE ACCESS TO DATA IN THIS SYSTEM?	14
4.7.1	<i>How will the data be used by the agency?</i>	14
4.7.2	<i>What system controls ensure such proper use?</i>	15
5	Privacy – Attributes of the Data	15
5.1	IS THE DATA USE BOTH RELEVANT AND NECESSARY TO THE SYSTEM PURPOSE?	15
5.2	WILL THE SYSTEM DERIVE NEW DATA THROUGH INFORMATION AGGREGATION?	15
5.3	IF DATA IS BEING CONSOLIDATED, ARE CONTROLS EFFECTIVE?	15
5.4	IF PROCESSES ARE BEING CONSOLIDATED, ARE CONTROLS EFFECTIVE?	15
5.5	CAN THE DATA BE RETRIEVED BY PERSONAL IDENTIFIERS?	15
5.6	POTENTIAL EFFECTS ON THE DUE PROCESS RIGHTS OF THE PUBLIC	16
5.6.1	<i>Consolidation and linkage of files and systems</i>	16
5.6.2	<i>Derivation of data</i>	16
5.6.3	<i>Accelerated information processing and decision-making</i>	16
5.6.4	<i>Use of new technologies</i>	17
5.7	HOW ARE THE EFFECTS ON THE PUBLICS’ RIGHT TO DUE PROCESS MITIGATED?	17
6	Privacy – Maintenance of Administrative Controls.....	17
6.1	CONTROLS TO ENSURE EQUITABLE TREATMENT OF NARA’S CUSTOMERS.	17
6.1.1	<i>Consistent use of the system and data across a distributed site system</i>	17

ERA Program Management Office (ERA PMO)

6.1.2 Possibility of disparate treatment of individuals or groups 17

6.2 WHAT ARE THE RETENTION PERIODS OF DATA IN THIS SYSTEM? 17

6.3 PROCEDURES FOR ELIMINATING DATA AT END OF THE RETENTION PERIOD 18

6.4 DATA ACCURACY, RELEVANCY, TIMELINESS, AND COMPLETENESS..... 18

6.5 IS THE SYSTEM USING TECHNOLOGIES IN NEW WAYS (E.G., CALLER-ID)? 18

6.6 HOW DOES THE USE OF THIS TECHNOLOGY AFFECT PUBLIC/EMPLOYEE PRIVACY? 18

6.7 DOES THE SYSTEM HAVE THE CAPABILITY TO IDENTIFY, LOCATE, AND MONITOR INDIVIDUALS? 18

6.8 DOES THE SYSTEM HAVE THE CAPABILITY TO IDENTIFY, LOCATE, AND MONITOR GROUPS OF PEOPLE?..... 18

6.9 DOES THE SYSTEM HAVE CONTROLS TO PREVENT UNAUTHORIZED MONITORING? 18

6.10 SYSTEMS OF RECORDS (SOR) NOTICE..... 19

6.10.1 Name and Number... .. 19

7 Compliance with Privacy Provisions of E-Government Act of 2002..... 19

8 Assessment Maintenance..... 23

Appendix A: ERA PIA Process A-1

Appendix B: Terminology B-1

Appendix C: User Account Information C-1

List of Tables

Table 1-1: Acronyms List 4

Table 3-1: ERA Privacy Act Information..... 8

Table A-1: Steps for Completing the ERA PIA..... A-1

Table B-1: PIA Specific Definitions..... B-2

Privacy Impact Assessment (PIA)

1 Introduction

Increasingly, records are created and maintained in electronic formats. To continue to fulfill its mission, the National Archives and Records Administration (NARA) needs to respond effectively to the challenge posed by the diversity, complexity, and enormous volume of electronic records being created today and the rapidly changing nature of the systems that are used to create them. This challenge will be met by a new system, the Electronic Records Archives (ERA). The Project unique identifier is: ERA 393-00-01-03-01-0001-00 and received the Authority to Operate in June 2007.

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.

1.1 Purpose

The purpose of the ERA PIA is to demonstrate how ERA complies with the privacy provisions as required by the E-Government Act 2002, Title II *Federal Management and Promotion of Electronic Government Services*, Sec. 208.

Per the National Institute of Standards and Technology's (NIST's) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Appendix A. *Glossary of Terms*, a PIA is defined as "An OMB-mandated 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."

The ERA PIA incorporates privacy requirements into the development lifecycle so that the ERA development effort can appropriately consider privacy issues from the earliest stages of design.

DRAFT

While both the ERA system owner and ERA staff must work together, in conjunction with the NARA Senior Agency Official for Privacy, to complete the PIA, ultimately the ERA Security Officer is responsible for this assessment. The ERA system owner must address what data is to be used, how the data is to be used, and who will use the data. The ERA system developers must address whether the implementation of the ERA requirements presents threats to privacy.

The PIA will be updated to address these statutory requirements based upon, and in conjunction with, the progression of the ERA system through its lifecycle. In addition, the PIA will also be updated on an annual basis, or as necessary in accordance with guidance provided by OMB Memorandums M-03-22 and M-05-04.

1.2 ERA PIA Process

The ERA PIA end-to-end process is based on the Federal Chief Information Officer's Council Best Practice for Privacy document (Internal Revenue Service – Model Information Technology Privacy Impact Assessment) and OMB M-03-22. The initial definition of the process is included in **Appendix A, ERA PIA Process**. The primary purpose of the process definition is to ensure the systematic and structured development of the PIA.

1.3 Information and Privacy

To fulfill the commitment of NARA to protect the public's personal information, several issues must be addressed with respect to privacy.

- The use of information must be controlled.
- Information may be used only for a necessary and lawful purpose.
- Individuals must have access to the principal purpose and routine uses of the information being collected from them.
- The least amount of information necessary to fulfill the principal purpose is collected.
- Information collected for a particular purpose should not be used for another purpose without the data subjects' consent unless such other uses are specifically authorized or mandated by law.
- Any information used must be sufficiently accurate, relevant, timely, and complete to ensure fair treatment of the individual.

1.4 Document Conformance

The structure of this PIA is based on the PIA template contained within the Federal Chief Information Officer's Council Best Practice for Privacy document (Internal Revenue Service - Model Information Technology Privacy Impact Assessment), hereafter referenced as CIO/PIA, and referenced in OMB M-01-05, Section 8. The content of the PIA maps as closely to OMB M-03-22 Attachment A, (II)(C)(1) as is practical. **Sections 3.0, Privacy - Data in the ERA System through 7.0, Compliance with Privacy Provisions of E-Government Act of 2002**, provides a cross-referencing between OMB M-03-22, Attachment A, and the ERA PIA. The CIO/PIA and M-03-22 materials are used as analytic and conformance frameworks respectively. The Best

DRAFT

Practices reference and OMB M-03-22 provide definitions that are specific to a PIA. These definitions are included in **Appendix B, Terminology**.

1.5 ERA Program Overview

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.

1.6 Acronyms

The technical terms used in this PIA are defined in Institute of Electrical and Electronics Engineers (IEEE) Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology* **Table 1-1, Acronyms List**, contains a list of acronyms used in this PIA.

ACRONYM	DEFINITION
AES	Advanced Encryption Standard
AFRY4	Assessment Final Report Year 4
AS	Acquisition Strategy
CCB	Change Control Board
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CMP	Configuration Management Plan
ConOps	Concept of Operations
DAC	Discretionary Access Control
DSS	Digital Signature Standard
ERA	Electronic Records Archives
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act (5 U.S.C. 552, as amended)
FRA	Federal Records Act (44 U.S.C. chaps 21, 29, 31, 33)
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
IV&V	Independent Verification and Validation
IVVP	Independent Verification and Validation Plan
NARA	National Archives and Records Administration
NGC	NARA General Counsel
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

ACRONYM	DEFINITION
OMPF	Official Military Personnel File
PA	Privacy Act of 1974 (5 U.S.C. 552a, as amended)
PIA	Privacy Impact Assessment
PL	Protection Level
PMO	Program Management Office
PMP	Program Management Plan
PRA	Presidential Records Act (44 U.S.C. chap. 22)
QM	Quality Management
QMP	Quality Management Plan
RD	Requirements Document
RKM	Risk Management Plan
SC	Security Category
SDLC	System Development Lifecycle
SOR	System of Records
SP	Special Publication
SRVM	Security Requirements Verification Matrix
SSP	System Security Plan
ST&EP	Security Test and Evaluation Plan
U.S.C.	United States Code

Table 1-1: Acronyms List

2 References

The following sections list the applicable laws, regulations, guidance, and resource materials that apply to information that will be contained in ERA.

2.1 Applicable Federal Laws, Mandates, NARA Regulations and Policies

The following apply to ERA.

- Federal Records Act (FRA), 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

DRAFT

- 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)

2.2 Standards and Guidelines

The following apply to ERA.

DRAFT

- 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

2.3 ERA Program Management Office (PMO) Documents

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), Version 5.1
- Concept of Operations (ConOps), Version 4.0
- Risk Management Plan (RKM), Version 3.0
- Program Management Plan (PMP), Version 3.1
- Requirements Document (RD), Version 3.1
- System Security Plan (SSP), Version 4.1
- Security Test and Evaluation Plan (ST&EP), Version 1.1
- Configuration Management Plan (CMP), Version 3.0
- ERA Account Management Plan, Version 3.0
- Independent Verification and Validation Plan (IVVP), Version 3.0

3 Privacy – Data in the ERA System

To fulfill the commitment of the NARA ERA to protect data in its holdings, several issues must be addressed with respect to privacy.

- The use of information must be controlled.
- Information may be used only for a necessary and lawful purpose.
- Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
- Information collected for a particular purpose should not be used for another purpose without the subject of the data's consent unless such other uses are specifically authorized or mandated by law.

DRAFT

- Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Given the availability of vast amounts of stored information and the expanded capabilities of ERA to process the information, it is foreseeable that there will be increased requests, from both inside and outside NARA, to share that information. With the potential expanded uses of data in automated systems it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses.

These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of NARA and ERA to the laws which protect the public and employee privacy rights and which provide redress for violations of those rights.

This PIA addresses the three (3) sources of personal information within ERA:

- Accessioned information (or information on deposit) covered by the FOIA, PRA, deed of gift, or deposit agreement;
- Unaccessioned information awaiting final disposition regardless of whether or not they are covered by PA systems of records of originating agencies; and
- Information that NARA collects on users of ERA.

The ERA contains two (2) general categories of information about individuals:

- Information about users of the ERA system (see Appendix C for more information),
 - ERA account information
 - ERA audit trail information
- Information contained in records and other documentary materials received, for storage in the ERA system, from various sources, e.g., Federal Agencies/Departments and Commissions, Presidential Administrations, and donations.

There will be four (4) basic categories of users:

- NARA employees,
- Other Federal employees,
- Government contractors,
- Privileged users who manage and maintain the ERA system

3.1 General Description of System Information

A description of the types of privacy related information that will be contained in ERA is provided in **Table 3-1, ERA Privacy Act Information**.

Information Domain	Information Description
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.
Information on individuals contained in records stored in the ERA system, but are <u>under the legal control of the Federal agency that created the records</u>	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.
Information on individuals contained in Federal records stored in the ERA system as <u>accessions of the National Archives (under the legal control of NARA)</u>	Information subject to the FOIA <i>that may not be releasable under exemptions (b)(6) and (b)(7)(C) of the FOIA.</i> Note: Accessioned records are specifically exempt from most provisions of the Privacy Act
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 13233, Further Implementation of the Presidential Records Act (which prevents the disclosure of presidential records "unless and until" the former president approves their release); and the privacy exemptions - <i>(b)(6) and (b)(7)(C)-of the FOIA.</i>
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
Information on individuals contained in donated archival materials	Information not subject to the PA, but controlled by directions of the <i>donor's deed of gift</i>

Table 3-1: ERA Privacy Act Information

With respect to the confidentiality of information that is subject to the Privacy Act; NIST SP 800-60, Appendix C, Section C.2.1.1 - *Corrective Action Information Type* states:

“Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will probably be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a moderate confidentiality impact level.

The Security Category (SC) for instances of the ERA system processing and housing data up to and including Sensitive But Unclassified (SBU), as defined by Federal Information Processing

DRAFT

Standard Publication (FIPS PUB) 199 and documented in the *ERA System Security Plan (SSP)*, is:

SC information system = {(confidentiality, High), (integrity, High), (availability, Moderate)}.

As the ERA system matures, this section of the PIA will be updated to remain compliant with the Federal Enterprise Architecture Security and Privacy Profile Phases (as they are developed), and the NARA Information Technology (IT) Security Architecture.

3.2 System Information Sources

This section *answers* questions about the sources of information used by ERA.

3.2.1 Which ERA files and databases are used?

The PII information stored in the LDAP directory for ERA system management purposes.

3.2.2 What Federal Agencies are providing data for use in the ERA system?

ERA achieved Initial Operating Capability (IOC) in June 2008, and the data is expected to be provided by the following federal agencies.

- U.S. Patent and Trademark Office
- Naval Oceanographic Office
- National Nuclear Security Administration
- U.S. Bureau of Labor Statistics

As system functionality and capabilities are increased through incremental development, potentially all Federal agencies will provide electronic records for storage within the ERA. 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.

3.2.3 What State and Local Agencies are providing data for use in the ERA system?

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.

3.2.4 What other third party sources will provide data?

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

DRAFT

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.

3.2.5 What information will be collected from the public/employee?

Public access is not implemented within ERA at this time. External agency and NARA employees and contractors provide the information shown on the account management forms in Appendix C.

3.3 How will external data be verified for accuracy?

For information about users of the ERA system, NARA will authenticate and verify accuracy using guidelines provided by OMB M-04-04, E-Authentication Guidance for Federal Agencies and by collecting information, as much as possible, directly from the individuals. The accuracy of audit trail data about use of the ERA system will be guaranteed by systematic controls within the ERA system.

For records of other Federal agencies that may be temporarily stored in ERA, the records are subject to the PA processes of those agencies. As such, any requests for alteration of a record would need to be addressed to the agency that created the record. If the agency agrees to modify the record in question, the newly modified record would be accepted by NARA from the agency making the modification and inserted into the file in the ERA in place of the previous record. Similarly, if the subject individual wishes to file a statement of disagreement with the record, this action will need to be addressed to the responsible agency. The agency in turn would be responsible for forwarding the statement to NARA for inclusion in the appropriate file in ERA.

Once records are transferred to the legal custody of NARA they cannot be changed. The Privacy Act allows the subject (individual) of a record to request corrections to the record when they are in the legal custody of the originating agency. However, once the records are transferred to the legal custody of NARA, an individual's right to request an amendment or file a statement of disagreement is terminated.

NARA holds a unique status under the Privacy Act. Archival records that are accessioned into the National Archives are exempt from most provisions of the Privacy Act (see 5 U.S.C. 552a(1)(2) and (1)(3)). NARA must, however, publish in the Federal Register a statement generally describing the agency records transferred into its legal custody that had been covered by the PA while in active use.

In any case, it is important to understand that NARA does not have the responsibility for verifying the accuracy of information in holdings of Federal records or other archival materials preserved in the National Archives or a Presidential library, nor does it have authority to change the records. Its responsibility is for preserving authentic records, as produced and delivered by their originators.

DRAFT**3.4 How will data be checked for completeness?**

For ERA system users, individuals will be responsible for supplying complete data as needed by NARA to manage access rights. The methodology for confirming completeness is defined in the ERA Account Management Document version 3, 2008.

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.

3.5 Is the data current? How do you know?

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 5USC 552 (b)(6) and (b)(7)(C). NARA provides redacted copies of textual records and public use versions of electronic records.

3.6 Are the data elements described in detail and documented?

For ERA users, the data elements reflecting information required to be collected, from individuals during registration, is described and documented as part of the account management process. See ERA Account Management Document, Version 3, 2008.

For archival records, NARA preserves documentation provided by the originators. Due to the enormous variety of information type and content there is no document that lists all the data elements present in NARA's archival holdings. NARA anticipates implementing a Lifecycle Data Repository as a component of ERA in which data elements will be identified for all the different record and data types.

4 Privacy – Access to the Data

This section contains information about ERA user access and restrictions, as well as data use.

4.1 Who will have access to the data in the ERA system?

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 user performing system management can retrieve user account information by a search on a unique user identifier or user name. Reports containing user account information are not generated at this time.

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.

4.2 User data access methodology

ERA implements security controls consistent with guidelines specified by NIST SP 800-53/FIPS PUB 200. The ERA system employs a role-based access control mechanism. For initial release of the ERA system, the roles (user classes) currently anticipated are listed below.

- Access Reviewer
- Appraiser Level 1 Manager
- Appraiser Level 2 Manager
- Appraiser Level 3 Manager
- Authority List Manager
- Certifying Official
- Lifecycle Management Team (LMT) Member
- NARA Accessioning Manager
- NARA Receiving Manager
- Records Appraiser
- Records Processor
- Records Scheduler
- Records Scheduler (NARA)
- Transferring Official (Agency)
- Transferring Entity (Agency)
- Transferring Official (NARA)
- Transferring Entity (NARA)
- Transfer Staff

DRAFT

4.3 User access restrictions

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.
- 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.

4.4 Controls to prevent misuse of data by those with access

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 controls can detect unauthorized access and unauthorized monitoring.

4.5 Do other systems share data or have access to data in this system?

NARA will have Memorandums of Agreement (MOAs) and Interconnection Service Agreements (ISAs) with all owners of systems connecting to ERA. The ISA will outline the sharing of and access to data within ERA. The data shared is archival records that may contain PII data.

4.6 Responsible party for protecting the privacy of affected individuals.

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 specifically stored within the ERA system.

DRAFT

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.

4.7 Will other agencies share data or have access to data in this system?

Other agency access to personal information will be governed in accordance with the provisions of the Privacy Act; 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.

For agency records stored temporarily in ERA, NARA serves only as the custodial agent for the agency. Under NARA's PA regulations (36 CFR 1202.2 (b)), records of other agencies that are stored in NARA record centers on behalf of that agency are governed by the PA rules of the transferring agency. When ERA is operational, the provision will be amended to account for the temporary storage of such records within ERA.

4.7.1 How will the data be used by the agency?

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).

4.7.2 Who is responsible for ensuring proper use of the data?

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.

4.7.2 What system controls ensure such proper use?

The ERA system is implementing the controls in NIST 800-53. The ERA system security controls include but are not limited to strong passwords, encryption, two (2) -factor authentication for privileged users, Role Based access control, and auditing. These controls are applied to external agency users of ERA as well as NARA staff.

The PII placed on back up media will be encrypted when it is transported outside the ERA Security boundary.

5 Privacy – Attributes of the Data

This section discusses the attributes of the data collected and used by ERA.

5.1 Is the data use both relevant and necessary to the system purpose?

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.

5.2 Will the system derive new data through information aggregation?

ERA will not create new personally identifiable data through information aggregation.

5.3 If data is being consolidated, are controls effective?

The only anticipated consolidation of personally identifiable data will be in the accumulation of back up media and audit trails pertaining to system usage. ERA Program is addressing the requirements from OMB M-07-16 in the ERA Incident Response plan.

5.4 If processes are being consolidated, are controls effective?

No processes related to determinations about individuals have been identified as candidates for consolidation.

5.5 Can the data be retrieved by personal identifiers?

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

DRAFT

Delegated Account Representatives 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.

5.6 Potential effects on the due process rights of the public

The following sections deal with the question of whether ERA capabilities or processes could compromise the public's right to due process.

5.6.1 Consolidation and linkage of files and systems

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

ERA may offer services to link files or systems for records it stores under the control of other agencies, when such services are requested by the originating agencies and are consistent with law and policy. Such linkages are likely to improve the exercise of rights by the public. For example, NARA assists veterans in obtaining benefits to which they are entitled by delivering information from the Department of Defense's OMPF to other agencies such as the Department of Veterans Affairs and the Social Security Administration.

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

5.6.2 Derivation of data

No potential effects anticipated. No personally identifiable data is expected to be derived by the ERA system.

5.6.3 Accelerated information processing and decision-making

Accelerated information processing and decision-making could potentially provide an enhancement of the due process rights of the public by allowing NARA to more rapidly respond to requests for information and provide quicker access to its holdings. However, accelerated information processing and decision-making could also potentially have a negative impact on due process rights of the public by aggravating the risk of releasing inappropriate data to the public or providing inappropriate access to sensitive or classified data. Please refer to **Section 5.7** for information concerning the mitigation of this effect.

5.6.4 Use of new technologies

While it is expected that ERA will make full use of technologies to allow NARA to continue fulfilling its mission into the future, those components selected for use within the ERA system will be of proven, mainstream technologies.

5.7 How are the effects on the public's right to due process mitigated?

ERA is not a public facing web site at this time.

6 Privacy – Maintenance of Administrative Controls

This section details the maintenance of administrative controls.

6.1 Controls to ensure equitable treatment of NARA's customers

NARA's vision for ERA, as outlined within the ERA Vision Statement document, states that:

“... We will ensure that anyone, at anytime, from any place, has access to the best tools to find and use the records we preserve. Our staff will be capable and consistent users of the electronic tools at every point of the lifecycle. We will sustain widespread support from all our stakeholders and customers by listening to their needs, meeting their requirements, and seeking their feedback.”

6.1.1 Consistent use of the system and data across a distributed site system

ERA is not a distributed site system. This information will be added in future updates to the PIA as the ERA system matures.

6.1.2 Possibility of disparate treatment of individuals or groups

The ERA system will not provide the capability for disparate treatment of individuals or groups. The ERA system will not be used to make any determinations affecting individuals except for their access to information in the ERA system. Determinations on access will be made in accordance with applicable laws and regulations, without regard to the characteristics of individuals or groups.

6.2 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 indefinitely. 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.

DRAFT

6.3 Procedures for eliminating data at end of the retention period

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 all other PII, will be determined by the operations staff of the ERA system. At that time, the procedures will be defined in ERA operations and user manuals.

6.4 Data accuracy, relevancy, timeliness, and completeness

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 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.

6.5 Is the system using technologies in new ways (e.g., Caller-ID)?

This information will be added in future updates to the PIA as the ERA system matures.

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

This information will be added in future updates to the PIA as the ERA system matures.

6.7 Does the system have the capability to identify, locate, and monitor individuals?

It is anticipated that the ERA system will provide the capability to identify, and monitor the use of the ERA system by individuals. ERA requires the ability to identify and monitor system usage in order to prevent or mitigate various threats such as malicious code, intrusions, and/or unauthorized system access, in an effort to protect and preserve the archival records.

6.8 Does the system have the capability to identify, locate, and monitor groups of people?

There is no requirement for the ERA system to identify, locate, or monitor groups of people; therefore, there is no intention to include such capability in the design of the ERA system.

6.9 Does the system have controls 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 approval. The CCB and the ERA security officer will not approve devices which would permit monitoring.

DRAFT

6.10 Systems of Records (SOR) Notice

There is no SOR within ERA at this time.

6.10.1 Name and Number

Not applicable at this time.

7 Compliance with Privacy Provisions of E-Government Act of 2002

OMB Memorandum M-03-22 documents OMB guidance for implementing the privacy provisions of the E-Government Act of 2002. The objective of this section is to demonstrate current and planned conformance with this guidance as ERA progresses through its lifecycle. Text pulled directly from M-03-22 is *italicized*.

I. General

A. Requirements - Agencies are required to.

- 1 *Conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),*

This document provides the vehicle for conducting a PIA for ERA.

- 2 *Post privacy policies on agency websites used by the public (see Section III),*

It is expected that ERA's privacy policy will reflect the provisions of M-03-22, Attachment A, Section III in their entirety.

- 3 *Translate privacy policies into a standardized machine-readable format (see Section IV), and*

It is expected that ERA's privacy policy will reflect the provisions of M-03-22, Attachment A, Sections IV and VII.

- 4 *Report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).*

ERA reports annually to OMB on compliance with Section 208 of the E-Government Act subject to the current lifecycle phase of the ERA system.

B. Application - This guidance applies to:

- 1 *All executive branch departments and agencies ("agencies" and their contractors that use information technology or that operate websites for purposes of interacting with the public,*

It is expected that ERA will operate a website for purposes of interacting with the general public in a future release of ERA.

- 2 *Relevant cross-agency initiatives, including those that further electronic government*

Not applicable. While ERA will clearly have an impact across Government agencies, it is not identified as a cross-agency initiative.

II. Privacy Impact Assessment

A. When to conduct a PIA

1. *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*
 - 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).*

ERA has conducted a PIA prior to the development or procurement of an IT system as described in B(I)(a) and B(I)(b), and will continue to perform updates to the PIA on an annual basis (at a minimum) throughout the ERA lifecycle.

2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*

It is expected that the PIA will be included in ERA's continuous programmatic risk assessment process as documented in the *ERA Risk Management Plan (RKM)* and security risk assessment process. Any changes that affect controls that protect the confidentiality, integrity, and availability of information subject to regulatory and NARA privacy provisions will be reviewed in accordance with ERA's review process.

3. *Not Applicable*
4. *Update of PIAs: Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.*

Refer to item two (2) above. PIA update is part of the ERA PIA process.

B. Conducting a PIA

1. Content

- a. *PIAs must analyze and describe:*
 - i. *what information is to be collected;*

ERA information will be from a variety of sources as summarized in **Table 3-1** and explained in **Sections 3.0, 3.1, and 3.2** of the PIA.

- ii. *why the information is being collected;*

The reasons for collecting PA protected information and FOIA protected privacy-related information (contained in Federal records) are explained in **Section 3.2.5, and 5.5** of the PIA. Reasons for collecting FOIA protected privacy-related information also relate to the agency mission of NARA.

- iii. *intended use of the information;*

Agency use of PA information is addressed in **Sections 3.2.5, 4.1, and 4.7.1** of the PIA.

- iv. *with whom the information will be shared;*

Sharing of information is explained under **Section 4.7** of the PIA.

ERA Program Management Office (ERA PMO)

DRAFT

- v. *what opportunities individuals have to decline to provide information or to consent to particular uses of the information, and how individuals can grant consent;*

An individual who declines to provide account information will not receive an account on the ERA system. Individuals are aware of system monitoring and possible release of the information to ERA maintenance staff when they sign the Rules of Behavior. A Privacy Act statement to individuals regarding the purpose and use of the information being collected will be provided at the time that such information is being solicited from said individuals.

- vi *how the information will be secured; and*

ERA implements security controls recommended in NIST 800-53.

- vii. *whether a system of records is being created under the Privacy Act 5 US C. 552a.*

ERA does not require a system of records at this time.

- b. *Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.*

The collection of privacy information was reviewed during the development of the account creation forms. These forms minimize the collection of privacy information.

- 2. *Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection.*
 - a. *Specificity - The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.*

Privacy impact controls identified in NIST SP 800-55 and NIST SP 800-44 will be addressed in future releases of the ERA system to address the information collection and use of this information. This PIA adequately documents the existing privacy controls.

- b. *Information lifecycle analysis/collaboration*

The ERA system was granted authority to operate in June 2008. No public access and a limited number of government and contractor ERA users are expected in 2008.

3 *Review and publication*

- a. *Agencies must ensure that:*

- i. *the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);*

The current, in-place review processes, as detailed in the ERA *Quality Management Project Management Procedures*, and the **Review and Audits** section of the ERA *Quality Management Plan (QMP)* are sufficient to ensure conformance with this requirement. The process for specifically reviewing the PIA will be addressed in more detail as outlined in **Appendix A, ERA PIA Process**.

- ii *for each covered IT system for which 2005* funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003**

ERA Program Management Office (ERA PMO)

DRAFT

(submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300); and

*With regard to the dates listed in subsection ii above: while these dates are referenced directly from the original OMB M-03-22, dated 26 Sep 2003; ERA will continue to conform to all current OMB reporting requirements.

iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

A summary of this PIA will be prepared for public release.

C. Relationship to requirements under the Paperwork Reduction Act

Additional information will be added to this section in future updates to this PIA as the ERA system matures.

D. Relationship to requirements under the Privacy Act of 1974, 5 U.S.C. 552a.

Archival records that are accessioned (transferred to the legal custody of NARA) and become part of the National Archives of the United States are exempt from most provisions of the Privacy Act (see 5 U.S.C. 552a (1)(2) and (1)(3)).

III. Privacy Policies on Agency Websites

It is expected that all pertinent OMB guidance such as M-00-13 and M-99-18, and NIST guidance such as SP 800-44, will be applied at the appropriate time. The NARA/ERA Privacy Policy will be updated to include any additional, unique information specific to the users of the ERA system and will be accessible from the ERA user interface Web Site portal..

IV. Privacy Policies in Machine-Readable Formats

The ERA/NARA privacy policy will be machine-readable when ERA has public access.

V. Privacy Policies Incorporated by this Guidance

ERA is updating the privacy policy to comply with this guidance..

VI. Agency Privacy Activities/Designation of Responsible Official

The Senior Agency Official for Privacy is the NARA General Counsel. The General Counsel will provide legal guidance and is ultimately responsible for enforcement of NARA privacy policy. As such, the designated NARA Senior Agency Official for Privacy, with the assistance of the NARA Privacy Act Officer, will have overall agency-wide responsibility for information privacy issues.

As required by OMB guidance, and reiterated in NARA Notice 2005-144, 10 Mar 2005, the Senior Agency Official for Privacy "...will oversee NARA's implementation of information privacy protections, and compliance with information privacy laws, regulations, and policies, such as the Privacy Act. This role includes reviewing NARA's information privacy procedures to ensure that they are comprehensive and up-to-date, and developing new NARA policy on information privacy issues."

VII. Reporting Requirements

DRAFT

ERA follows the reporting requirements outlined in Interim Guidance 1603-2 External Breach Notification.

8 Assessment Maintenance

As a part of process improvement (e.g., Independent Verification and Validation (IV&V) assessments as defined in the *ERA Independent Verification and Validation Plan (IVVP)*, lessons learned, Quality Management (QM) assessments, as defined in the *ERA QMP*), the PIA, and the overall approach to the privacy impact assessment, will continue to evolve. The assessment will be updated as needed to maintain current and sufficient quality management activities.

DRAFT

Appendix A: ERA PIA Process

The ERA PIA Process is under development. However, the steps that are required to complete the ERA PIA are summarized below in **Table A-1, Steps for Completing the ERA PIA**.

Note: Where listed in **Table A-1** NARA staff and ERA staff references will include the ERA system developer as well as representatives of NARA and the ERA PMO.

Step	Responsible Stakeholders	Activity
1	System Owner and NARA staff	Request and complete Privacy Impact Assessment (PIA) Training.
2	System Owner and NARA staff	Answer the questions presented in Sections 3.0 through 6.0 of this PIA.
3	System Owner and ERA staff	Submit the PIA document to the NARA Senior Agency Official for Privacy.
4	Senior Agency Official for Privacy (NGC)	Review the PIA document to identify privacy risks from the information provided. The NARA Senior Agency Official for Privacy will get clarification from the System Owner and ERA staff as needed.
5	System Owner, ERA staff, Senior Agency Official for Privacy, and CIO	The System Owner, ERA staff, and the Senior Agency Official for Privacy should reach agreement on design requirements to resolve all identified risks. If an agreement cannot be reached then issues will be raised to the CIO for resolution.
6	System Owner and ERA staff	The System Owner and ERA staff will incorporate the agreed upon design requirements and resolve the identified risks.
7	System Owner, ERA staff, and Senior Agency Official for Privacy	Participate in the System Development Lifecycle (SDLC) required reviews to ensure satisfactory resolution of identified privacy risks and obtain formal approval.

Table A-1: Steps for Completing the ERA PIA

Appendix B: Terminology

Term	Definition	Definition Source
Accuracy	Within sufficient tolerance for error to assure the quality of the record in terms of its use in making a determination	CIO/PIA
Completeness	All elements necessary for making a determination are present before such determination is made	CIO/PIA
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	CIO/PIA
Individual	A citizen of the United States or an alien lawfully admitted for permanent residence	OMB M-03-22
Information in identifiable form	Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)	OMB M-03-22
Information Technology (IT)	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	OMB M-03-22
Major information system	Embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), 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.	OMB M-03-22
National Security Systems	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) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of	OMB M-03-22

DRAFT

Term	Definition	Definition Source
	military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management	
Necessary	A threshold of need for an element of information greater than mere relevance and utility	CIO/PIA
Privacy Impact Assessment (PIA)	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks	OMB M-03-22
Privacy policy in standardized machine-readable format	A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser	OMB M-03-22
Record	Any item, collection or grouping of information about an individual and identifiable to that individual that is maintained by an agency	CIO/PIA
Relevance	Limitation to only those elements of information which clearly bear on the determination(s) for which the records are intended	CIO/PIA
Routine Use	With respect to the disclosure of a record under the PA, the use of such record for a purpose that is compatible with the purpose for which it was collected	CIO/PIA
ERA System Owner	The ERA System Owner is the official who has primary responsibility for determining that an IT system meets the business requirements of the agency, and who has responsibility for the procurement, development, or operation and maintenance of that system. The System Owner also evaluates the cost and benefits of system features.	NIST SP800-37
System of Records	As established under the PA, is a group of records under the control of an 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.	CIO/PIA

Table B-1: PIA Specific Definitions

Appendix C: User Account Information

The following information is solicited from individuals requesting an EOP account.

INSTRUCTION AND INFORMATION SHEET FOR ERA USER REQUEST

The user must complete all required fields and sign the User Request Form before returning the form to the Delegated Account Representative (DAR). The DAR is required to store a hard copy of the User Request Form on file in chronological order.

Fields that are required are denoted with the character ().*

Section 1: Action. Check appropriate box – Create New User or Modify Existing User.

Section 2: User. Provide ALL User information in fields marked as required.

Section 3: Agency. Provide ALL Agency information in fields marked as required.

- **Major Division:** Name of the Agency Major Division.
- **Minor Division:** Name of the Agency Minor Division.

Section 4: ERA Information. Provide ALL ERA Information in fields marked as required.

- **ERA Role:** The ERA Role requested to be assigned to the User. The list of available roles is included at the end of the instructions under the section titled “Available ERA Roles”. (Appendix C also includes a full description of each role)
- **Handling Restrictions:** Any special handling restrictions granted to this user. The list of available Handling Restrictions is included at the end of the instructions under the section titled “Available Handling Restrictions”.
- **Transfer Entity:** Check the box if the user will be transferring files to ERA
- **Security Question:** Question asked by Helpdesk personnel to identify the User.
- **Security Answer:** Answer to the Security Question.
- **Delegated Account Representative (DAR):** The local Point of Contact at the Agency to whom the form is submitted
- **NARA Account Representative (NAR):** If the account request is from an Agency Other than NARA, a NAR is required to approve the account.

Section 5: Signatures. The form must be signed by the user and the DAR.

Available ERA Roles:

- Access Reviewer
- Appraiser Level 1 Manager
- Appraiser Level 2 Manager
- Appraiser Level 3 Manager
- Authority List Manager
- Certifying Official
- Lifecycle Management Team (LMT) Member
- NARA Accessioning Manager
- NARA Receiving Manager
- Records Appraiser
- Records Processor
- Records Scheduler
- Records Scheduler (NARA)
- Transferring Official (Agency)
- Transferring Entity (Agency)
- Transferring Official (NARA)
- Transferring Entity (NARA)
- Transfer Staff

Available Handling Restrictions:

- Donated - Statute
- Donor Restricted
- Executive Privilege
- Freedom of Information Act (FOIA)
- FOIA (b)(1) National Security
- FOIA (b)(2) Internal Personnel Rules and Practices
- FOIA (b)(3) Statute
- FOIA (b)(4) Trade Secrets and Commercial or Financial Information
- FOIA (b)(5) Inter-agency or Intra-agency Memorandums or Letters Not Available by Law
- FOIA (b)(6) Personal Information
- FOIA (b)(7) Law Enforcement
- FOIA (b)(8) Regulation or Supervision of Financial Institutions
- FOIA (b)(9) Geological or Geophysical Information and Data
- House Rule
- John F Kennedy Assassination Records Collection Act
- Presidential Records Act (p)(1) National Security Classified
- Presidential Records Act (p)(2) Appointments to Federal Office
- Presidential Records Act (p)(3) Statute
- Presidential Records Act (p)(4) Trade Secrets and Commercial or Financial Information
- Presidential Records Act (p)(5) Confidential Communications
- Presidential Records Act (p)(6) Personal Privacy
- Presidential Records Act (PRA)
- Presidential Recordings and Materials Preservation Act of 1974 (PRMPA)

DRAFT

- PRMPA - Individual Rights Pending (C)
- PRMPA - Investigatory Information (F)
- PRMPA - National Security Classified (B)
- PRMPA - Non-Historical Information (H)
- PRMPA - Personal Information (G)
- PRMPA - Personal Privacy (D)
- PRMPA - Statute (A)
- PRMPA - Trade Secrets and Commercial or Financial Information (E)
- Senate

Privacy Act Statement

Sections 2104(a) and 2108 of Title 44 of the U.S. Code authorize the collection of this information. The primary use of this information is to process and track your ERA User Account Request. The information in this request will be stored by ERA to authenticate and process future account requests. Furnishing the information requested on this form is voluntary, but failure to complete all required fields will prevent NARA from processing your request.

DRAFT



Electronic Records Archive (ERA) - User Request Form

* Denotes Required Field

SECTION 1: ACTION

* Action Requested: Create New User Modify Existing User

SECTION 2: USER

* First Name: _____ Middle Name: _____

* Last Name: _____ Suffix: _____

* Job Title: _____ * E-Mail: _____

* Telephone Number: _____ Fax Number: _____

* Employee Status:
 Federal Employee Contractor

SECTION 3: AGENCY

* Agency Name: _____ * Street Address: _____

* City: _____ * State: _____

* Zip Code: _____ * Country: _____

* Major Division: _____ * Minor Division: _____

SECTION 4: ERA INFORMATION

* ERA Role: _____ Handling Restrictions: _____

Transferring Entity: _____

* Security Question: _____ * Security Answer: _____

* Delegated Account Representative (DAR): _____ NARA Account Representative (NAR): _____

SECTION 5: SIGNATURES

* Applicant Signature

Signature _____ Date _____

* DAR Signature

Signature _____ Date _____

DRAFT

The following information is solicited from individuals requesting an EOP account.

The user must complete all required fields and sign the User Request Form before returning the form to the Delegated Account Representative (DAR). The DAR is required to store a hard copy of the User Request Form on file in chronological order.

Fields that are required are denoted with the character (*).

Section 1: Action. Check appropriate box – Create New User or Modify Existing User.

Section 2: User. Provide ALL User information in fields marked as required.

Section 3: EOP Information. Provide ALL EOP information in fields marked as required.

- **EOP Role:** The EOP Role requested to be assigned to the User. The list of available roles is included below:
 - Presidential Records Processor (PRP)
 - Search and Access Support Staff (SASS)
 - Potentially Classified Asset Reviewer (PCAR)
- **Presidential Administration:** The name of the Presidential Administration.
- **Record Status Assignment:** Special access restrictions granted to this user. The list of available Record Status restrictions is included below:
 - President
 - Vice President
 - Federal
 - Presidential Library Users
- **Security Question:** Question asked by Helpdesk personnel to identify the User.
- **Security Answer:** Answer to the Security Question.
- **Delegated Account Representative (DAR):** The local Point of Contact to whom the form is submitted.

Section 5: Signatures. The form must be signed by the user and the DAR.

DRAFT



Executive Office of the President (EOP) User Request Form

* Denotes Required Field

SECTION 1: ACTION

* Action Requested: Create New User Modify Existing User

SECTION 2: USER

* First Name: _____ Middle Name: _____

* Last Name: _____ Suffix: _____

* Job Title: _____ * E-Mail: _____

* Telephone Number: _____ Fax Number: _____

* Employee Status:
 Federal Employee Contractor

* Street Address: _____

* City: _____ * State: _____

* Zip Code: _____ * Country: _____

SECTION 3: EOP INFORMATION

* EOP Role: _____

* Presidential Administration: _____ * Record Status Assignments: _____

* Security Question: _____ * Security Answer: _____

* Delegated Account Representative (DAR): _____

SECTION 5: SIGNATURES

* Applicant Signature

Signature _____ Date _____

* DAR Signature

Signature _____ Date _____