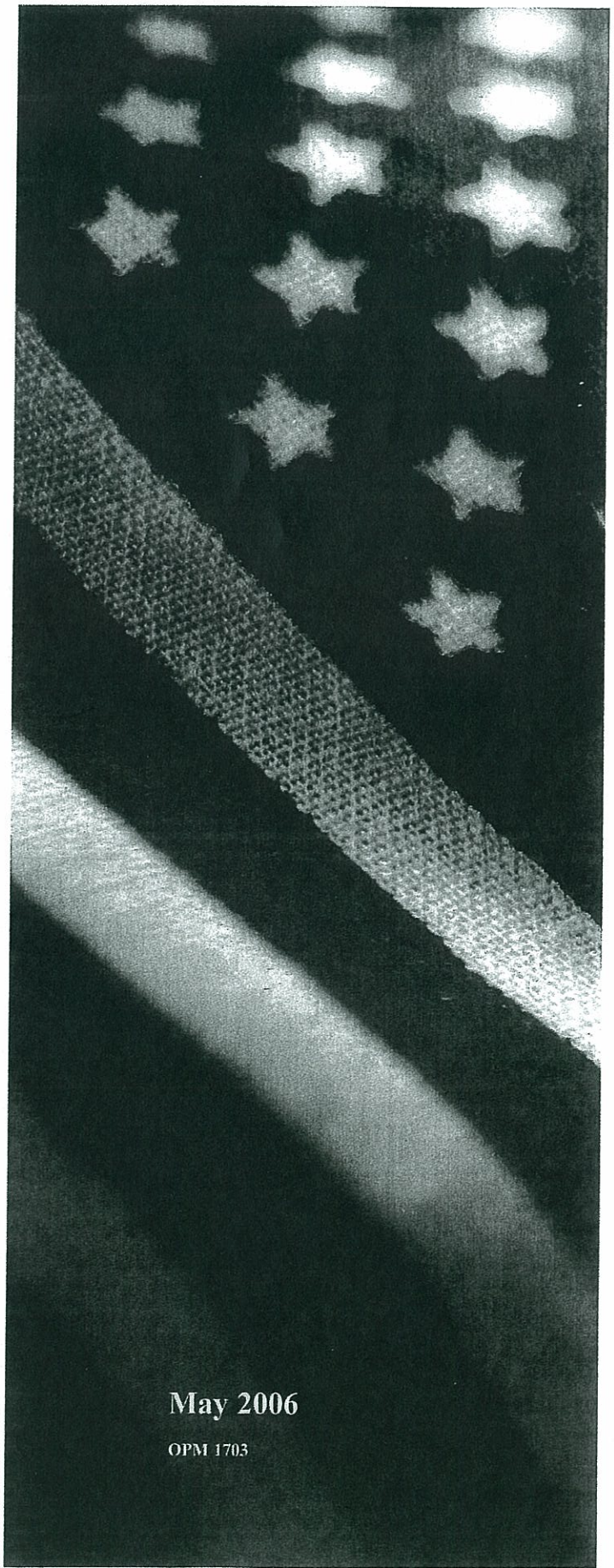

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT

PRIVACY IMPACT ASSESSMENT GUIDE

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Working for America

May 2006

OPM 1703

Revision History

Revision Number	Revision Date	Revision Summary	Authoring Office
1.1	April 2005	Initial Draft Release	MSD/CIS/PPG
1.2	August 2005	Revised Draft Release	MSD/CIS/PPG
1.3	December 2005	Revised Draft Release	MSD/CIS/PPG
1.4	March 2006	Revised Draft Release	MSD/CIS/PPG

Office of Personnel Management (OPM)
Privacy Impact Assessment (PIA) Guide

Table of Contents

Office of Personnel Management (OPM)
Privacy Impact Assessment Guide

General Information

1.1 Purpose

The following guide is designed to assist you in conducting an initial assessment to determine whether you need to complete a Privacy Impact Assessment (PIA), to certify that determination, and, if a PIA is required, to gather the information required and complete the PIA.

1.2 Scope

The scope of this document is limited to guidance for conducting an initial assessment and then if required, preparing a PIA for OPM. This guidance applies to all OPM information technology (IT) systems and information collections in accordance with OMB guidance for implementing privacy provisions of the E-Government Act of 2002. Throughout this document, the term information collection, as defined by the Paperwork Reduction Act of 1995, means to require, obtain, maintain, retain, or publicly disclose the same information from 10 or more members of the public. This includes questions posed to agencies, instrumentalities, or employees of the United States, if the results are to be used for statistical purposes. The term information technology (IT) means, as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

1.3 Background

The E-Government Act of 2002 requires that agencies:

- Conduct Privacy Impact Assessments (PIAs),
- Ensure the review of the Privacy Impact Assessment by the Chief Information Officer (CIO),
- Make them publicly available, and
- Provide a copy to the Office of Management and Budget (OMB).

The E-Government Act requires agencies to conduct PIAs ***before*** *developing or procuring information technology (IT) systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public; or 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.*

The E-Government Act stipulates that each PIA must address the following seven requirements:

- What information is to be collected;
- Why the information is being collected;
- The intended use of the agency of the information;
- With whom the information will be shared;

- What notice or opportunities for consent would be provided to individuals regarding what information is to be collected and how that information is shared;
- How the information will be secured; and
- Whether a System of Records is being created under the Privacy Act of 1974, 5 U.S.C. 552a.

In addition, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 requires agencies to indicate what opportunities individuals have to decline to provide information or consent to particular uses of the information. Additionally, PIAs must identify what choices the agencies made regarding an IT system or electronic information collection as a result of performing the PIA.

1.4 Applicability

All OPM Program Offices will perform an initial screening of any new or significantly modified IT system or electronic information collection to determine if a PIA is required when planning or developing the system or collection. If there is a question about whether or not your change is considered significant, please contact the IT Security and Privacy Manager, Management Services Division/Center for Information Services/Plans & Policies Group (MSD/CIS/PPG) at 202-606-2150.

This guidance is applicable to OPM Headquarters, all OPM regional offices, and all OPM contractors and vendors.

1.5 Responsibilities

The OPM Chief Information Officer (CIO) as the OPM Chief Privacy Officer, is responsible for the definition, implementation, adoption, and modification of this guidance and related processes and procedures and final review of all OPM PIAs.

The system owner is responsible for completing the initial screening and the PIA, if required, when planning or developing an IT system or electronic information collection. If significant changes are being planned or developed for an existing IT system or electronic information collection, the system owner must also complete the initial screening and the PIA, if required. Please contact the IT Security and Privacy Manager in MSD/CIS/PPG at 202-606-2150 for additional guidance on what constitutes a significant change and for requesting assistance in planning an electronic information collection.

The system owner must also review their existing PIA documentation as part of their annual Federal Information Security Management Act (FISMA) security review and submit evidence of the review by September 1 of each year to the IT Security and Privacy Manager in MSD/CIS/PPG via email at PIAmail@opm.gov.

Obtaining the CIO's review of the initial screening and the PIA is the responsibility of MSD/CIS/PPG. Posting the PIA to OPM's web site and ensuring a copy is sent to OMB is also the responsibility of MSD/CIS/PPG.

Sections 2 through 4 of this Guide provide guidance for completing the initial screening and the PIA.

1.6 Document Maintenance

We anticipate changes to this guidance. This document will be reviewed at least annually. Updates and changes are the responsibility of MSD/CIS/PPG.

1.7 Definitions

The term Information Collection, as defined by the Paperwork Reduction Act of 1995, means to require, obtain, maintain, retain, or publicly disclose the same information from 10 or more members of the public. This includes questions posed to agencies, instrumentalities, or employees of the United States, if the results are to be used for statistical purposes.

The term Information Technology, as defined in the Clinger-Cohen Act, means 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.

1.8 Authority

This guidance is based on the following authority:

- The e-Government Act of 2002 which requires each agency to conduct privacy impact assessments; "ensure the review of the [PIAs] by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and, if practicable, after completion of the review, make the PIA publicly available."

- The Clinger-Cohen Act of 1996 which requires that each agency assume responsibility and accountability for information technology investments, and "assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives."

- Office of Management and Budget (OMB) Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", which requires agencies to "conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available" and to "report annually to OMB on compliance with section 208 of the E-Government Act of 2002."

1.9 References

The following references are provided as guidance when conducting PIAs:

Clinger-Cohen Act of 1996, available online at
http://www.cio.gov/documents/it_management_reform_act_feb_1996.html.

Electronic Government (E-Government) Act of 2002, available online at
http://www.cio.gov/archive/e_gov_act_2002.pdf.

Federal Information Security Management Act (FISMA), Title III – Section 301, Information Security. (See E-Government Act of 2002.)National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems (February 2005), available online at http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.

National Institute for Standards and Technology (NIST) Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems (November 2001)*, available online at http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf.OMB Circular A-11, Part 7, Section 300, Section 300 – Planning, Budgeting, Acquisition, and Management of Capital Assets, available online at http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf.

OMB Circular A-130, Management of Federal Information Resources, Transmittal No. 4, available online at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

OMB M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999), available online at http://www.whitehouse.gov/omb/memoranda/m99-18.html.*

OMB M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000), available online at http://www.whitehouse.gov/omb/memoranda/m00-13.html.

OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003), available online at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

OMB M-05-23, Improving IT Project Planning and Execution (August 4, 2005), available at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-23.pdf.

Paperwork Reduction Act of 1995, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ13.104.pdf.

Privacy Act of 1974, 5 U.S.C. 552a, available at http://www.usdoj.gov/04foia/privstat.htm.

1.10 Using This Guide

To use this guide, Program Offices should complete the PIA Initial Screening Assessment in Section 2.

Your answer to question Section 2.2.c will help you determine whether you are required to complete a PIA. Follow the additional instructions provided there and throughout the Guide.

Submit all of the required documentation to the IT Security and Privacy Manager, MSD/CIS/PPG at PIAMail@opm.gov.

If you have any questions, contact MSD/CIS/PPG at (202) 606-2150 for more assistance.

2. PIA Initial Screening Assessment

2.1 IT System or Electronic Information Collection Identification

(a) Who is completing the initial screening assessment?		
Name: **Jennifer L. Mann**		Title: **EHRI Designated Security Officer**
Organization name and office symbols: **EHRI (eOPF)**	Telephone Number: **202-606-4744**	E-Mail Address: **jennifer.mann@opm.gov**
(b) Who is the IT system or electronic information collection owner?		
Name: **Reginald M. Brown**		Title: **Director of Modernization&HRLOB**
Organization name and office symbols: **OMHRLOB**	Telephone Number: **202-606-1332**	E-Mail Address: **reginald.brown@opm.gov**
(c) What is the IT system or electronic information collection name?		
Enter the name here: **EHRI Electronic Official Personnel File (eOPF)**		
(d) Does the activity represent a new or significantly modified IT system or information collection?		
Check one of the boxes below: ☒ Yes. Continue to the next question. ☐ No. Continue to the next question.		
(e) Is this an IT system or project or an electronic information collection? (If you don't know, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150 for assistance.)		
Check one of the boxes below: ☒ IT System or Project ☐ Electronic information collection ☐ Don't know		
(f) What is the Unique Project Identifier (UPI)? Insert the UPI from OMB Circular A-11, Part 7, Section 300, Exhibit 300, Part 1 Capital Asset Plan (CAP) if you are required to complete a CAP for this IT system or electronic information collection. If not applicable, check the box for N/A.		
Enter the UPI here: **999-99-01-99-01-019-03**	If not applicable, check the box below: ☐ N/A	
(g) Will this IT system or electronic information collection use web technology? If you don't know, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150 for assistance.		
Check one of the boxes below: ☒ Yes. Enter the URL: **HTTPS://eopf.nbc.gov/agency code/** ☐ No. ☐ Don't Know.		

(h) What is the purpose of the IT system or electronic information collection and why is the information being collected? Review OPM's web site development policy.
eOPF is the electronic version of the hard copy OPF that is accessible to all via the internet. eOPF offers a standard solution for all federal agencies- information is available on demand, 24/7.
(i) What is the IT system or electronic information collection status?
Check one of the boxes below: ☐ Planning ☐ Development ☒ Operational
(j) Is the IT system or electronic information collection operated by OPM staff, contractor staff, or a combination of OPM and contractor staff?
Check one of the boxes below: ☐ OPM Staff ☒ Contractor staff. Enter the contractor's company name: **National Business Center @ DOI** ☐ Combination of OPM staff and contractor staff. Enter the contractor's company name:
(k) Where is the IT system or electronic information collection physically located?
Street address (include city, state, and ZIP code):: **7301 W. Mansfield Avenue, Denver, Colorado 80235**
Contractor's company name, if applicable: **National Business Center (NBC) @ the U.S. Department of Interior (DOI)**

2.2 Initial Screening Assessment

(a) Is an OMB mandated PIA required for this IT system or electronic information collection?

Check one of the boxes below:
☒ Yes. A PIA must be conducted.
☐ No. Continue to the next question.

(b) Does the system or electronic information collection contain or collect any Personally Identifiable Information (PII)? (See page 4 for the definition of PII.)

"Personally identifiable information" is also referred to as "information in identifiable form" which is "information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."

For more information, see OMB Guidance for Implementing the Privacy Provisions of the e-Government Act of 2002, M-03-22, at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

Check one of the boxes below:
☒ Yes. Continue to the next question.
☐ No. Complete and sign the Certification page, Section 4 of this Guide.

(c) Is this an IT system that collects PII on members of the public? (See page 4 for the definition of IT system.)

For purposes of this screening assessment as required by the E-Government Act of 2002, Federal government employees, Federal consultants, and Federal contractors are **not** considered members of the public.

If you don't know, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.

If your IT system or electronic information collection was created prior to October 1, 2003, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150 for additional guidance.

Check one of the boxes below:
☐ Yes. You must complete a PIA. Complete Sections 3 and 4 of this Guide. Continue to the next question.
☒ No. Continue to the next question.
☐ Don't Know. Continue to the next question.

(d) Is this an electronic information collection that collects PII on members of the public?
For purposes of the Paperwork Reduction Act of 1995, Federal consultants and Federal contractors **are** considered members of the public.

If you don't know, contact the IT Security and Privacy Manager, MSD/CIS/PPG at PIAmail@opm.gov.

Check one of the boxes below:

☐ Yes. You must complete a PIA. Complete Sections 3 and 4 of this Guide. Continue to the next question.
☒ No. Continue to the next question.
☐ Don't know. Continue to the next question.

(e) Is this an electronic information collection that collects PII on Federal employees?
Special rules apply to Federal employees. Contact the IT Security and Privacy Manager, MSD/CIS/PPG at PIAmail@opm.gov for information.

Check one of the boxes below:

☒ Yes. Contact the IT Security and Privacy Manager, MSD/CIS/PPG at PIAmail@opm.gov.
☐ No, and if (c) and (d) above are No, no PIA is required. Complete and sign the Certification page, Section 4 of this Guide.
☐ No, and if (c) and (d) above are Yes, contact the IT Security and Privacy Manager, MSD/CIS/PPG at PIAmail@opm.gov.
☐ Don't know. Contact the IT Security and Privacy Manager, MSD/CIS/PPG at PIAmail@opm.gov.

3. The PIA

You must complete the following questions if the Initial Screening Assessment in the previous section indicates a PIA is required.

3.1 Nature and Source of Information to Be Collected

(a) What is the nature of the information to be collected? Review OPM's web site development policy. Provide a brief narrative describing the nature of the information, i.e., financial, investigative, pre-employment, human resources, etc.
Provide a brief narrative here: **Electronic data and images of employees career HR data (e.g., SF50s, NOAs, etc.)** **(See attached narrative for details)**
(b) What is the source of the information? Agencies maintaining a system of records are required to collect information to the greatest extent directly from the individual, when information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs. If you don't know, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.
Check all the boxes below that apply: ☐ Directly from the person to whom the information pertains ☐ From other people ☒ Other sources such as databases, web sites, etc. ☐ Don't know

3.2 Reason for Collection of Information

(a) Why is the information being collected?
Provide a brief narrative here: **Converts HR processes from paper based to electronic based processing.** **(See attached narrative for details)** **(3.2.b. Yes - Legal Authority: 5 USC 33, 5 CFR 930)**
(b) Is there legal authority for collecting the information?
Check one of the boxes below: ☒ Yes. Cite the legal authority for collecting the information: ☐ No

3.3 Intended Use of the Collected Information

(a) What is the intended use of the information?

Provide a brief narrative here:

Replace the paper based OPF with an electronic version to support knowledge based work force management.
(See attached narrative for details)

(b) For major IT investments as defined in OMB Circular A-11, a high-level data flow diagram must be prepared.

Provide a high-level data flow diagram (up to two pages) showing the steps in processing the data, and the uses to which the data will be put. Attach the data flow diagram to this assessment.

For more information, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.

Check the box below if a high-level data flow diagram has been attached.
☒ Yes.

Check the box below if the IT System is not a major IT investment as defined in OMB Circular A-11.
☐ Not Applicable.

3.4 Purpose and Identification of Information to Be Shared

a) Does the system share personally identifiable information (PII) in any form?
Provide a high-level data flow diagram (up to two pages) showing the steps in processing the data, and the uses to which the data will be put. Attach the data flow diagram to this assessment.

For more information, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.

Check the boxes below that apply:

☒ Yes. Specify with whom and for what purposes the system shares the PII and identify which PII is shared.

Check the boxes below that apply:

☒ Within OPM. Specify with whom and for what purposes the system shares the PII and identify which PII is shared.

All PII shared-Agencies use eOPF for employees HR processing

☒ With other Federal agencies. Specify with whom and for what purposes the system shares the PII and identify which PII is shared. **Employee transfers, retirements, etc.**

☐ With state or local governments. Specify with whom and for what purposes the system shares the PII and identify which PII is shared.

☐ With members of the public. Specify with whom and for what purposes the system shares the PII and identify which PII is shared.

☐ No
(b) Who will have access to the PII on the system?
Check all the boxes below that apply: ☒ Users ☒ Administrators ☐ Developers ☐ Contractors ☐ Public
(c) Is information part of a computer matching program? For more information, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.
Check one of the boxes below: ☐ Yes. Provide the agency name, computer match name, and number: ☒ No

3.5 Opportunities Individuals Have to Decline to Provide Information or to Consent to Particular Uses of the Information

(a) Is providing information voluntary?
Check one of the boxes below: ☐ Yes. What opportunities do individuals have to decline to provide the information? Briefly describe the details below: ☒ No.
(b) Are individuals informed about required or authorized uses of the information?
Check the boxes below that apply: ☒ Yes. Check one of the boxes below that indicates how individuals are informed: ☒ Privacy Act Statement. Attach a copy of the Privacy Act Statement to this submission. ☒ Other. Briefly describe and attach a copy to this submission. **Terms of Condition and Rules of Behavior** ☐ No
(c) Will other uses be made of the information than those required or authorized?
Check the boxes below that apply: ☐ Yes. Briefly explain what the other uses are and how individuals can grant consent to such uses: Briefly explain how individuals are informed of those other uses: Briefly explain how individuals are given the opportunity to grant those other uses: ☒ No.

3.6 Security of Information

(a) Has the system been authorized to process information?

Check the boxes below that apply:

☒ Yes. You must provide the following documentation to the IT Security and Privacy Manager, MSD/CIS/PPG via email at PIAMail@opm.gov:

- Information System Security Plan (ISSP)
- Risk Assessment and Mitigation Plan
- Security Requirements Traceability Matrix
- Security Test and Evaluation Report
- Contingency and Disaster Recovery Plans
- Certification Statement
- Accreditation Recommendation

☐ No. Briefly explain below and contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.

(b) Is an annual review of the IT system or electronic information collection conducted as required by the Federal Information Security Management Act (FISMA)?

Check one of the boxes below:

☒ Yes. Provide the FISMA assessment documentation to the IT Security and Privacy Manager, MSD/CIS/PPG via email at PIAMail@opm.gov.

☐ No. Briefly explain why the FISMA review was not conducted:

(c) Are security controls annually tested as required by FISMA?

OMB Circular A-130 stipulates that a system's security controls should be reviewed "when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system."

Check one of the boxes below:

☒ Yes. Provide the FISMA assessment documentation to the IT Security and Privacy Manager, MSD/CIS/PPG via email at PIAMail@opm.gov.

☐ No. Briefly explain why security controls were not tested as required by FISMA:

(d) Are contingency plans tested annually as required by FISMA?

OMB Circular A-130 stipulates that a system's security controls should be reviewed "when significant modifications are made to a system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system."

Check one of the boxes below:

☒ Yes. Provide the FISMA assessment documentation to the IT Security and Privacy Manager, MSD/CIS/PPG at PIAMail@opm.gov .

☐ No. Briefly explain why the contingency plan was not tested as required by FISMA:

(e) Have personnel using the system been trained and made aware of their responsibilities for protecting the PII being collected and maintained?
Agencies should provide users with training in their roles and responsibilities for protecting PII collected and maintained on the system.

Check one of the boxes below:
☒ Yes
☐ No. Briefly describe the steps you have planned to provide this training:

(f) Are rules of behavior in place for individuals who have access to the PII on the system?
Agencies should provide users with training in their roles and responsibilities for protecting PII collected and maintained on the system.

Check one of the boxes below:
☒ Yes. Indicate for whom the rules of behavior are in place:
☐ General users ☒ System/database, administrators, developers, etc.

☐ No. Briefly explain why rules of behavior are not in place:

3.7 System of Records as Required by the Privacy Act, 5 U.S.C. 552a

(a) Are records on the system routinely retrieved by a personal identifier?

Check one of the boxes below:

☒ Yes. The Privacy Act applies.

☐ No. The Privacy Act does not apply; complete Certification page, Section 4 of this Guide.

(b) Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Check one of the boxes below:

☒ Yes. Please provide the SORN name and number: **OPM/GOVT-1**

☐ No. Briefly explain why a SORN has not been published:

(c) Does the SORN address all of the required categories of information about the system?

Check the boxes below that apply:

☒ Yes. Check the required categories below that have been addressed:

- ☒ System name
- ☐ System location
- ☒ Categories of records
- ☒ Purpose
- ☐ Disclosure to consumer reporting agencies
- ☐ Contesting record procedure
- ☐ Notification procedure
- ☐ System exempted from certain provisions of the Act
- ☐ System classification
- ☐ Categories of individuals covered by the system
- ☒ Authority of maintenance
- ☐ Routine uses of records maintained
- ☐ System Manager and contact information
- ☐ Record access procedure
- ☐ Record source categories
- ☐ Policies and practices for storing, retrieving, accessing, retaining, and disposing of records

☐ No. An updated SORN must be published in the Federal Register.

(d) Has any of the information in the SORN changed since the information was published?

Check one of the boxes below:

☐ Yes. An updated SORN must be published in the Federal Register.

☒ No

(e) Are processes in place for periodic review of personally identifiable information contained in the system to ensure that it is timely, accurate and relevant?

Before disseminating any records about an individual to any person other than an agency, unless the dissemination is made under FOIA, agencies must make reasonable efforts to ensure that such records are accurate, complete, timely, and relevant on each system for agency purposes.

Agencies are responsible for ensuring processes are in place to verify and validate personally identifiable information as directed by the Privacy Act of 1974.

If you have any questions, contact the IT Security and Privacy Manager, MSD/CIS/PPG, at PIAmail@opm.gov.

Check one of the boxes below:

☒ Yes. Briefly describe the review process including the processes for retention and destruction of records or files deemed untimely, inaccurate or irrelevant (include the Record Schedule name and/or number which gives authority for retention or destruction of the records):
Agencies are responsible for accurate information. NARA Gen Rec Sched 20

☐ No. Briefly explain why not.

4. Certification

Check one of the boxes below:

☐ No PIA is required. The PIA Initial Screening Assessment is attached.
☒ A PIA is required. The PIA Initial Screening Assessment, the PIA, and all required documentation are attached.

Prepared by

Jennifer L. Mana
Printed Name and Signature

11/12/2008
Date (mm/dd/yyyy)

Reviewed by System Owner

Matthew E. Perry
Printed Name and Signature

11/12/2008
Date (mm/dd/yyyy)

Reviewed by OPM Chief Privacy Officer and Chief Information Officer

Janet Barnes
Printed Name and Signature

11/12/08
Date (mm/dd/yyyy)

PRIVACY IMPACT ASSESSMENT
SUPPLEMENTAL NARRATIVE STATEMENTS
EHRI ELECTRONIC OFFICIAL PERSONNEL FOLDER (EOPF) 2008

2.1 IT System or Electronic Information Collection Identification

(h) What is the purpose of the IT system or electronic information collection and why is the information being collected?

The eOPF is a web based electronic system based on the Official Personnel Folder (OPF). The purpose of eOPF is to provide an electronic means of gathering human resource processing form images and provide agency access to the form images via the internet. The eOPF system was developed in support of the e-Government initiative to move towards a paperless environment. The eOPF system provides agency users with the ability to view their personnel folder and Human Resource Specialists with the ability to improve operational efficiency by replacing a paper-based records management system with an electronic system.

3.1 Nature and Source of Information to Be Collected

(a) What is the nature of the information to be collected? Review OPM's web site development policy.
Provide a brief narrative describing the nature of the information, i.e., financial, investigative, pre-employment, human resources, etc.

Provide a brief narrative here:

Electronic data and images of employees career HR data (e.g., SF50s, NOAs, etc. The Official Personnel Folder is a file containing records that covers a civilian Federal employee's employment history. The Office of Personnel Management (OPM) and the agency human resources (HR) offices use these documents to make decisions about employees' rights, benefits, and entitlements throughout their careers.

The eOPF is an electronic version of the paper OPF, providing Web-enabled access for Federal employees and HR staff to view eOPF documents. Agencies may also provide eOPF access to special investigators, helping to speed the investigation process and save agency resources.

3.2 Reason for Collection of Information

(a) Why is the information being collected?

Provide a brief narrative here:

Converts HR processes from paper based to electronic based processing. The Office of Management and Budget (OMB) has established firm milestones that all Executive Branch Agencies eliminate paper OPFs by October 2012. EHRI offers proven, cost-effective solutions to ease an Agency's transition to electronic OPFs (eOPFs) and improve workforce planning with insightful analysis and reporting capabilities. All solutions are fully compliant with OPM and Federally mandated HR employee record management regulations.

The process of moving from a paper based system to electronic records management can be a daunting one, especially given scarce resources. The EHRI PMO has the expertise and established best practices to maximize Agency results while minimizing negative impacts.

3.3 Intended Use of the Collected Information

(a) What is the intended use of the information?

Provide a brief narrative here:

Replace the paper based OPF with an electronic version to support knowledge based work force management.

Benefits to Agency Executives using eOPF:

- Enterprise-wide workforce visibility by enabling departments with multiple HR systems to have visibility of their entire workforce
- Improved workforce management by providing access to personnel data across the Federal Government to facilitate analysis/planning for hiring, skills development, retention strategies, and forecasting employee movements to ensure qualified personnel are in place
- Cost savings by reducing document storage, maintenance, and retrieval costs as well as copying, filing, faxing, and mailing requirements Enhanced security via a multi-level secure environment with document access that is restricted to a need-to-know basis, as well as a comprehensive audit trail for all activity
- Continuity of operations and disaster recovery with offsite electronic record storage capabilities and backed-up data safeguarding against theft, fire, flood, and other damage to paper folders
- Better accessibility through immediate and secure Web-based access to folders, simplifying daily procedures, eliminating delays, supporting remote workers, and facilitating interagency collaboration

Benefits to HR Specialists using eOPF: EHRI's eOPF solution increases productivity and efficiency, and frees HR staff to work directly with the Federal employee to solve issues and answer questions.

- Reduce re-work caused by inaccurate or missing personnel data/folders
- Enable more efficient, accurate workforce planning and human capital management
- Eliminate oversight of employee review of personnel folders
- Enhance accuracy, portability and security of personnel records
- Provide Immediate access to employee data for a geographically dispersed workforce

Benefits to Employees using eOPF: An Agency may grant access to eOPF for all employees to view their personnel data, which increases employee awareness and accountability. Additionally, eOPF facilitates the electronic filing of SF-50 data and automates employee notification of actions through email alerts.

(b) For major IT investments as defined in OMB Circular a-11, a high-level Data flow diagram must be prepared.

Provide a high-level data flow diagram (up to two pages) showing the steps in processing the data, and the uses to which the data will be put. Attach the data flow diagram to this assessment.

For more information, contact the IT Security and Privacy Manager, MSD/CIS/PPG at 202-606-2150.

Reference attached document

- Title: NBC Lakewood – eOPF Production
- Filename: Q3.4 EHRI_eOPF Environment - IA Server 01 & 02.pdf

3.4 Purpose and Identification of Information to be Shared

(a) Does the system share personally identifiable information (PII) in any form?
The Guide to Personnel Record Keeping and the eOPF Master Forms list details what forms are maintained in the employee eOPF. These forms are images that contain PII information and are shared with agency Human Resource Subject Matter Experts (SMEs), agency managers, agency EEO personnel, OPM investigators, agency oversight personnel, and employees. The Guide to Personnel Record Keeping and eOPF Master Forms List are included in the eOPF PIA submission.

3.5 Opportunities Individuals Have to Decline to Provide Information or to Consent to Particular uses of the information

(b) Are individuals informed about required or authorized uses of the Information?
Yes - Reference attached documents: 1) **Privacy Act Statement** Document Title: Enterprise Human Resources Integration (EHRI) An OPM e-Gov Project Privacy Policy Filename: Q3.5b_EHRI PrivacyPolicy_eOPF and DW 2) **Terms of Condition** Document Title: Full Terms and Conditions of Use Filename: Q3.5b EHRI Full Terms and Conditions of Use eOPF and DW 3) **Rules of Behavior** Document Title: RULES OF BEHAVIOR FOR ALL PERSONS OF ENTERPRISE HUMAN RESOURCES INTEGRATION

(EHRI) SYSTEMS
Filename: Q3.5b EHRI_ eOPF Rules of Behavior

3.6 Security of Information

(a) Has the system been authorized to process information?

Yes - Reference attached documents:

1) **Information System Security Plan (ISSP)**
Document Title: Office of Personnel Management
Enterprise Human Resources Integration
Electronic Official Personnel Folder (eOPF) Security Plan
Filename: Q3.6a and 3.6b eOPF Final SP 092407

2) **Risk Assessment and Mitigation Plan**
Document Title: Office of Personnel Management
Enterprise Human Resources Integration
eOPF Risk Assessment
Filename: Q3.6a eOPF Final RA 092407

Document Title: Plan of Actions and Milestones
U.S. Office of Personnel Management
Human Resources Line of Business
EHRI eOPF 08/13/08
Filename: Q3.6a POA&M - EHRI eOPF 2008-08-13

3) **Self Assessment** (encompasses requested documents: Security Requirements Traceability Matrix; Security Test and Evaluation Report)

Document Title: Enterprise Human Resources Integration eOPF
Self Assessment
Filename: Q3.6a and 3.6c eOPF annual assessment 092407

4) **Contingency and Disaster Recovery Plans**
Document Title: United States Office of Personnel Management
Enterprise Human Resources Integration (EHRI)
eOPF Contingency Plan – Version 4.0
Filename: Q3.6a and 3.6d EHRI eOPF CP - Updated 082808 Final

5) **Certification Statement**
Document Title: eOPF Certification and Accreditation Package (Memo)
Filename: Q3.6a eOPF Cert Letter

6) **Accreditation Recommendation**
Document Title: Enterprise Human Resources Integration
eOPF Security Accreditation Statement
Filename: Q3.6a eOPF ATO Letter

(b) Is an annual review of the IT system or electronic information collection Conducted as required by the Federal Information Security Management Act (FISMA)?

Yes - Reference attached documents:

1) **Information System Security Plan (ISSP) – (See Appendix D)**
Document Title: EHRI eOPF Security Plan
Filename: Q3.6a and 3.6b eOPF Final SP 092407

(c) Are security controls annually tested as required by FISMA?

Yes - Reference attached documents:

1) **Self Assessment** (encompasses requested documents: Security Requirements Traceability Matrix; Security Test and Evaluation Report)

Document Title: Enterprise Human Resources Integration Data
eOPF Self Assessment
Filename: Q3.6a and 3.6c eOPF annual assessment 092407

(d) Are contingency plans tested annually as required by FISMA?

Yes - Reference attached documents:

1) **Contingency and Disaster Recovery Plans**
Document Title: United States Office of Personnel Management
Enterprise Human Resources Integration (EHRI)
eOPF Contingency Plan – Version 4.0
Filename: Q3.6a and 3.6d EHRI eOPF CP - Updated 082808 Final

RULES OF BEHAVIOR FOR ALL USERS FOR ENTERPRISE HUMAN RESOURCES INTEGRATION'S eHR SYSTEM

The EHRI project office is responsible for ensuring an adequate level of protection and security is afforded to the eHR system. The requisite level of protection and security is accomplished through an appropriate mix of technical, administrative, and managerial controls including written guidance. Because written guidance cannot cover every contingency, the following Rules of Behavior are provided to further stipulate the responsibility of the users of the eHR System.

All persons must understand that these Rules of Behavior are based on Federal laws and regulation and, as such, there are consequences for violation of these rules. Depending on the severity of the violation, at the discretion of management and with due process of law, consequences can include: reprimand; removal of access privileges; suspension, demotion, or termination from work; and criminal and civil penalties.

Rules of Behavior

I understand that, when using the eHR System, I am personally accountable for my actions and that I must:

1. Protect data in accordance with the Privacy Act of 1974;
2. Protect sensitive information from disclosure to unauthorized individuals or groups;
3. Acquire and use sensitive information only in accordance with the performance of my official government duties;
4. Agency point-of-contact must protect information security by properly identifying Agency employees eligible as users of EHRI;
5. Dispose of sensitive information contained in hardcopy or softcopy, as appropriate;
6. Ensure that sensitive information is accurate and relevant for the purpose which it is collected, provided, and used;
7. Protect my access codes from disclosure;
8. Report security incidents and vulnerabilities to the EHRI project office;
9. Comply with the provisions of copyrighted software by not infringing upon or compromising (copy, distribute, manipulate, etc.) software of this system.
10. Ensure all changes to eHR System components and data are done via approved configuration control procedures;
11. Use government equipment in accordance with my site's/Agency's policies and procedures;

I understand that all conditions and obligations imposed upon me by these rules apply during the time I am granted access to this system regardless of location.

I understand that the EHRI project office reserves the right, to terminate or suspend my access and use of the eHR System, without notice, if there is a violation of these Rules of Behavior.