Office of Inspector General

Privacy Program

Review of the Federal Labor Relations Authority's FY 2015 Privacy Program

Fiscal Year 2015

Report No. AR-15-04

Federal Labor Relations Authority
1400 K Street, N.W. Suite 250, Washington, D.C. 20424

TABLE OF CONTENTS

OBJECTIVE

The objective was to perform a privacy and data protection review. The contractor performed the following:

- Conducted a review of the FLRA's privacy and data security policies, procedures, and practices in accordance with regulations.
- Reviewed the agency's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form.
- Reviewed the agency's stated privacy and data protection procedures with regard to the collection, use, sharing, disclosure, transfer, and security of personal information in identifiable form relating to agency employees and the public.
- Performed an analysis of the agency's intranet, network, and websites for privacy vulnerabilities (through review of source documents):
    - Noncompliance with stated practices, procedures, and policy.
    - Risks of inadvertent release of information in an identifiable form from the website of the agency.
- Issued recommendations for improvements or enhancements to management of information in identifiable form, and the privacy and data protection procedures of the agency.

BACKROUND

Dembo, Jones, Healy, Pennington & Marshall, P.C. (contractor), on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General (OIG), conducted an independent evaluation of the quality and compliance of the FLRA privacy program with applicable Federal computer security laws and regulations. The vulnerabilities discussed in this report should be included in FLRA's Fiscal Year (FY) 2015 report to the Office of Management and Budget (OMB).

The Privacy Act of 1974 regulates the use of personal information by the United States Government. Specifically it establishes rules that determine what information may be collected and how information can be used in order to protect the personal privacy of U.S. citizens.

The Privacy Act applies to *Federal Government Agencies* and governs their use of a system of records, which is defined as "any group of records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

The following rules govern the use of a system of records:

- No Federal Government record keeping system may be kept secret.
- No agency may disclose personal information to third parties without the consent of the individual (with some exceptions).
- No agency may maintain files on how a citizen exercises their First Amendment rights.
- Federal personal information files are limited only to data that is relevant and necessary.

6010 Executive Blvd • Suite 900
Rockville, MD 20852
P 301.770.5100 • F 301.770.5202

Dembo, Jones, Healy, Pennington & Marshall, PC
A Member of PKF International, Limited
www.dembojones.com

6711 Columbia Gateway Drive • Suite 550
Columbia, MD 21046
P 410.995.5200 • F 410.995.5204

- Personal information may be able to be used for the purposes it was originally collected unless consent is received from the individual.
- Citizens must receive notice of any third party disclosures including with whom the information is shared, the type of information disclosed and the reasons for its disclosure.
- Citizens must have access to the files maintained about them by the Federal Government.
- Citizens must have the opportunity to correct or amend any inaccuracies or incompleteness in their files.

EXECUTIVE SUMMARY

The OIG performed a Privacy and Data Protection review in accordance with privacy and data protection related laws and guidance (e.g. Privacy Act of 1974, OMB memorandums, Consolidated Appropriations Act of 2005 etc.). The Consolidated Appropriations Act of 2005 requires agencies to assign a Chief Privacy Officer who is responsible for identifying and safeguarding personally identifiable information (PII) and requires an independent third-party review of agency use of PII and of its privacy and data protection policies and procedures periodically.

SUMMARY OF RESULTS

Overall, the FLRA's Privacy program is strong. Out of 27 different testing areas, this year's Privacy audit resulted in only four findings. The overall summary of those findings were as follows:

- There is a difference in inventory between the IT Department and the Office of Privacy.
- Routine uses are not described. SORNs are also not reported for specific systems.
- There are missing Privacy Impact Assessments.
- The agency's website needs to be updated to comply with the Privacy regulations with regards to machine readable technology and reporting mechanisms to the viewers of the Agency's website.

Finding No. 1 - IT and Privacy Coordination

Condition:

There are 11 systems at the FLRA that reside within different offices at the agency. The areas of responsibility reside with the Privacy Act Officer, Senior Agency Official for Privacy (SAOP), and the respective managers of systems of records. The Privacy Act Officer works toward the implementation and enforcement of the Privacy Act. For example, publishing systems of records in the Federal Register, reviewing privacy policies, and coordinating with the SAOP. The SAOP ensures steps are taken to protect personal data from unauthorized use in consultation with managers and the Privacy Act Officer. The SAOP also conducts periodic reviews of privacy documentation. The managers of systems of records; inform the Privacy Act Officer regarding the existence of systems, as well as monitors routine use, and is engaged in the safeguarding of privacy data. The list of agency systems is noted below:

Privacy Systems
1. GSS Network (electronic system) 2. Third party systems a. OFF (Managed by the Interior Business Center) b. FPPS (Managed by the Interior Business Center) c. Quickbase (Managed by Intuit) d. Case Management (part of Quickbase) e. FOIAOnline (Managed by the EPA) f. PRISM (Managed by Treasury's Administrative Resource Center) g. CONCUR (Managed by the Treasury's Administrative Resource Center) h. E-OPF (Managed by OPM) i. WebTA (Interior Business Center) 3. Paper-based systems

Specifically, the following was noted:

1. The IT Department and the Office of Privacy contained different inventories of the systems residing at the FLRA for some of the systems noted above. The privacy requirements should be known to the IT Department since it is within their responsibility to manage security over privacy related data on IT systems.
    i. FOIAOnline, WebTA and the various paper-based systems were not contained within the IT system inventory.
    ii. The GSS network was not contained within the Privacy system inventory.

2. All systems housing PII should be assessed to determine if a privacy impact assessment (PIA) is warranted. The PIA will help to ensure that controls are deployed on those systems that are commensurate with the PII residing on those systems. Of the 11 systems, two (Case Management e-filing system and FOIA Online) have current PIAs in place. The need for a PIA covering the remaining eight systems was succinctly evaluated in the FLRA's 2014 Systems Inventory; however, that limited evaluation should be examined in a traditional Privacy

Threshold Analysis. Finally, the FLRA has not analyzed whether any of its paper-based systems, including those identified as Systems of Records under the Privacy Act, require a PIA. All completed PIAs should be placed on the FLRA website.

Criteria:

- The National Institute of Standards and Technology (NIST) describes how an agency can identify personally identifiable information, which enables the agency to properly maintain an inventory of systems and what PII resides on each of those systems. The NIST guidance also provides guidance on how to perform a PIA. The guidance below was provided by **NIST 800-122 section 2.1:**

"Organizations should use a variety of methods to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII. Some organizations require a PTA to be completed before the development or acquisition of a new information system and when a substantial change is made to an existing information system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs should be submitted to an organization's privacy office for review and approval. PTAs are often comprised of simple questionnaires that are completed by the system owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer. Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, or checking with system owners."

- NIST also describes the various elements making up PII. The elements below shall be considered when assessing the PII in systems maintained by the FLRA, as noted in **NIST 800-122 section 2.1:**

"This publication uses the definition of PII from OMB Memorandum No. 07-16, which is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. To distinguish an individual is to identify an individual."

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;

- Asset information, such as Internet Protocol (IP) or Media Access Control address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

- The OMB has specific requirements regarding when and how a PIA should be conducted. This criteria states the instances when a PIA shall be performed as noted by **OMB Memorandum No. 03-22 section II.B.2:**

The E-Government Act of 2002 requires agencies to conduct a PIA. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;
- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Cause:

There is a lack of communication between IT and the Privacy Act Officer, leading to the absence of PIAs for approximately one system, as well as there being a discrepancy between the Privacy and IT system inventories.

Risk:
Without IT and Privacy's awareness of systems residing on the FLRA network, and without PIAs for some of the Privacy systems, there may be PII vulnerable to exposure.

Recommendation(s):

1. The CIO and the Privacy Act Officer should hold annual meetings to discuss the various requirements for all FLRA systems to determine the security requirements of protecting the PII residing within those systems. Those meetings should discuss the following:
    a. Complete inventory of systems and the type of data residing on those systems.
    b. The safeguarding of data on those systems.
    c. The management of the systems. For example, are the systems managed by a third party or managed in-house by the FLRA?
    d. Electronic versus paper-based systems.
    e. The types of controls deployed and whether or not this is commensurate with the data residing on the systems.
    f. PIAs for each system.
    g. SORNs and routing uses for each system.

It was determined through interview that this finding has been resolved. The CIO and the SAOP have scheduled quarterly meetings beginning in September 2015 to discuss the privacy matters and PIA requirements listed in this recommendation. We therefore close this recommendation.

2. The CIO should work with the Privacy Act Officer to determine if there are PIAs needed for those systems that have not had a PIA. Furthermore, the Privacy Act Officer should determine whether the PIAs should be posted on the FLRA's website.

Finding No. 2 - System of Records Notices and Routine Use Review

The Privacy Act of 1974 places restrictions on the ability of Federal agencies to share a system of records with third parties, including other agencies. However, the Privacy Act does recognize the need of the Government to share records in order to improve security, maintain accuracy and consolidate resources. This is often accomplished through matching programs which allow certain data elements in one system of records to be searched against records in another system in order to find any data matches. Such matches would link together the information from both systems.

The Privacy Act contains a "routine use" exception which allows the disclosure of information without the notice or consent of the individual. Routine use is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected." As long as the SORN contains a listing of the routine uses of the information, an agency is considered compliant with the Privacy Act.

"A System of Records is a group of any 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."

A SORN informs the public of the existence of a system of records and describes the type of information that an agency will be collecting, who will be collecting the information, how it will be safeguarded, the purpose for collecting such information, etc. It is an advanced notice to the public that must be given before an agency begins to collect, is given access to or can retrieve personal information for a new system of records and must be published in the Federal Register.

Agencies are also required to periodically review their systems and ensure the SORN listing maintained on the agency website is current. Agencies are also required to identify those systems without a SORN and assess if there are PII records within those systems that should have been communicated to the public via a SORN.

Condition:

3. "Routine Uses" are not described for all FLRA systems (applicable to the Privacy Act and considered a System of Records), with the exception of the paper-based systems.

Criteria:

The OMB provides guidance regarding publishing of system records to ensure the public's trust, as stated by the **OMB Memorandum No. 99-05, section 4:**

"In passing the Privacy Act, the Congress made a strong policy statement that in order to ensure fairness, there shall be no record keeping systems, the very existence of which is secret. Therefore, each agency shall review its operations to identify any *de facto* systems of records for

which no system of records notice has been published. If the agency identifies any such unpublished systems of records, then the agency should publish a system of records notice for the system promptly. Agencies shall implement appropriate measures (e.g., training) to ensure that system of records are not inadvertently established, but instead are established in accordance with the notice and other requirements of the Privacy Act."

- Lastly, the OMB provides guidance on the periodic reviews of systems to ensure that unpublished records are complete and accurate, as stated in **OMB Memorandum No. 99-05, attachment B**:

"The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of systems of records containing personal information, to give individuals access to records about themselves in a system of records, and to manage those records in a way to ensure fairness to individuals in agency programs.

For the Privacy Act to work effectively, it is imperative that each agency properly maintain its systems of records and ensure that the public is adequately informed about the systems of records the agency maintains and the uses that are being made of the records in those systems. Therefore, agencies must periodically review their systems of records and the published notices that describe them to ensure that they are accurate and complete. OMB Circular A-130, "Management of Federal Information Resources," (61 Fed. Reg. 6428, Feb. 20, 1996) requires agencies to conduct periodic reviews, in accordance with the schedule in Appendix I of the Circular."

- Each agency shall conduct a thorough review of its systems of records, system of records notices, and routine uses in accordance with the criteria and guidance below, as described by **OMB Memorandum No. 99-05, section 2:**

"Non-statutory disclosures created by administrative mechanisms should only be made when appropriate. Therefore, each agency shall review its "routine uses" to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected. The Privacy Act requires agencies to include in their systems of records notices a description of the routine uses for which information in a system of records may be disclosed. 5 U.S.C. § 552a(e)(4)(D)."

Cause:

IT has not complied with its requirements and responsibilities with regard to SORNs and Routine Use review.

Risk:

Currently, the public may be unaware of all FLRA Systems of Records because the system listing on the FLRA website may be incomplete. The FLRA is responsible to ensure that systems have published SORNs so that the public may be adequately informed of the systems that are in the agency's inventory, as well as the PII contained within those systems. Without knowing if there are any unpublished systems, the public at large will be unaware of the complete listing of systems presented by the FLRA. Also, documenting the "Routine Uses" enables IT to adequately protect the PII residing on systems. Without a full understanding of "Routine Uses," the data may not be adequately protected.

Recommendation(s):

3. SAOP and IT should review all routine uses for all systems and coordinate this review. If any of those routine uses are no longer appropriate, IT should work with the Privacy Act Officer to delete those routine uses from the SORN and update accordingly on the agency's website.
4. IT should publish a SORN for the GSS Network if upon determination that this system contains records of individuals covered by the Privacy Act.

Finding No. 3 - Privacy Impact Assessments

A PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Condition:

5. PIAs are required to be updated every 3 years (or earlier if the system had a significant change). PIAs are also required for new systems. A PIA has not been performed on 1 system:
    i. GSS Network.

Criteria:

- The OMB has specific requirements regarding when and how a PIA should be conducted. This criteria states the instances when a PIA shall be performed as noted by **OMB Memorandum No. 03-22 section II.B.2:**

The E-Government Act of 2002 requires agencies to conduct a PIA. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;
- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Cause:

IT and Privacy haven't had the appropriate coordination to identify those systems needing a PIA.

Risk:

With incomplete PIAs, FLRA may not be deploying security controls that are commensurate with the PII that resides on those systems.

Recommendation(s):

5. IT should complete a new PIA for the GSS network. The PIAs should be approved and reviewed by the SAOP.

Finding No. 4 Website Updates

Privacy regulations stipulate that an agency's website requires notification of those voluntary and involuntary actions regarding privacy while browsing an agency's website. Specifically, Privacy act statements must notify users of the authority, purpose and use of the collection of information. Those statements must also notify whether providing information is mandatory or voluntary, and the effects of not providing all or any part of the requested information. Additionally, the FLRA must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences.

Condition:

6. The FLRA website didn't contain the following:

    i. Notification of the authority, purpose and use of the collection of information.
    ii. Notification of whether providing information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
    iii. Machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences.

It was also determined through interview that this finding has been resolved; however, this will be tested in August/September of 2015, as the closure of this finding occurred in early June of 2015.

Criteria:

- The OMB has specific requirements regarding machine readable technology. **OMB Memorandum No. 03-22 section IV.A:**

Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.

- The OMB has specific requirements regarding Privacy Act statements and notifying users of the agency's website. **OMB Memorandum No. 03-22 section III.D:**

A. *Content of Privacy Policies.*
    1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
        a. *Consent to collection and sharing*. Agencies must now ensure that privacy policies:

i. inform visitors whenever providing requested information is voluntary;
ii. inform visitors how to grant consent for use of voluntarily-provided information; and
iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.

b. *Rights under the Privacy Act or other privacy laws*. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
i. in the body of the web privacy policy;
ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at
iv.
v. www.Firstgov.gov).

2. Agency Privacy Policies must continue to address the following, modified, requirements:
a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
1. at the point of collection, or
2. via link to the agency's general Privacy Policyhttp://www.whitehouse.gov/omb/memoranda/m03-22.html - 18.
ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.

Cause:

IT and Privacy haven't had the appropriate coordination to identify those website requirements to ensure that the website is compliant with the latest Privacy requirements.

Risk:

Visitors to the agency's website may be unaware of the site practices and collection measures, thereby violating the trust of that respective visitor.

Recommendation(s):

6. IT and Privacy should meet to discuss the various website requirements and then update the website accordingly.

Dembo, Jones, Healy, Pennington & Marshall, P.C.

June 18, 2015

APPENDIX A:

Management Comments to the Draft Report

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

June 5, 2015

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: Fred B. Jacob, Solicitor and Senior Agency Official for Privacy
Michael Jeffries, Chief Information Officer

THROUGH: Sarah Whittle Spooner
Executive Director

SUBJECT: Management Response to Draft Report Evaluation of the Federal Labor Relations Authority Fiscal Year 2015 Privacy Program Report No. AR-15-04

Thank you for the opportunity to review and provide comments on the May 13, 2015 draft evaluation of the FLRA's Privacy Program. Please accept this memorandum as a management's response to the draft.

To begin, we are pleased to learn that the auditors identified only 4 issues in an exhaustive evaluation of 27 different testing areas of privacy protection, many of which had numerous subparts. We would greatly value the inclusion of these successes in the final draft.

Below, we provide responses to each of the four findings in the draft report. We appreciate your consideration in finalizing the report.

Finding No. 1 – IT and Privacy Coordination

1. *The IT Department and the Office of Privacy contained different inventories of the systems residing at the FLRA for some of the systems noted above. The privacy requirements should be known to the IT Department since it is within their responsibility to manage security over privacy related data on IT systems.*
   i. *FOIAOnline, WebTA and the various paper-based systems were not contained within the IT system inventory.*
   ii. *The GSS network was not contained within the Privacy system inventory.*

2. *All systems housing PII should be assessed to determine if a privacy impact assessment (PIA) is warranted. The PIA will help to ensure that controls are deployed on those systems that are commensurate with the PII residing on those systems. There are 11 systems, for which there has not been a determination made on which systems require a*

PIA, and whether the PIAs need to be placed on the FLRA website. For example, the GSS network didn't have a PIA completed.

Respectfully, the draft report's observation in paragraph 2 above that the FLRA has not made a PIA determination on 11 systems may not be entirely accurate.

- The 2014 FLRA Systems Inventory, which was provided to the auditors and is attached, evaluated whether a PIA is necessary for all of the Third Party systems listed on page 4 of the draft report. We will reexamine those determinations, however, to ensure their accuracy.

- As to the Case Management e-Filing system system, the Agency completed its PIA and posted it on its website as of February 10, 2015.

- As to the FOIAOnline System, no FLRA PIA was necessary under OMB Memo M-03-22, at ¶ II(B)(b)(7) (Sep. 26, 2003), because the PIA was completed by the EPA.

- Finally, as to the paper-based systems identified on page 4 of the draft report, it is unclear whether PIAs are necessary, as OMB Memo M-03-22, at ¶ II(B)(a)(1)-(2) ("When to conduct a PIA"), only requires PIAs of "IT Systems" or "electronic collections" of PII. That said, we will consider whether any paper based systems, most of which are covered by Systems of Records Notices that discuss the privacy implications of the PII they contain, should also have a PIA.

We are committed to issuing a PIA for the GSS Network, as noted below.

The draft report also recommends annual meetings between the CIO and SAOP to discuss the requirements for protecting PII in the system. Although the CIO and SAOP have met regularly on an ad hoc basis to discuss privacy matters, particularly surrounding the annual FISMA audit, we have implemented this recommendation and scheduled quarterly meetings to discuss privacy matters and PIA requirements. In light of our implementation of this recommendation, we respectfully request that the final report close this component of Finding No. 1.

Finding No. 2 – System of Records Notices and Routine Use Review

3. *"Routine Uses" are not described for all FLRA systems, with the exception of the paper-based systems.*
4. *Currently, there is 1 system (i.e. GSS network) without a published SORN, even though it is a requirement that these systems should have an associated SORN that is published, thereby communicating to the public at large, regarding the data collected.*

Finding No. 2 focuses on the Privacy Act's requirement that the Agency issue System of Records Notices and review those notices' routine uses on a regular basis. The draft currently suggests in findings 3 and 4 above that routine uses should be described for "all FLRA systems" and that the Agency has failed to publish a System of Records Notice for the GSS Network. Respectfully,

however, these findings fail to recognize a prerequisite for both routine uses and SORNs: that the Agency determine that the relevant systems are indeed "Systems of Records" under the Privacy Act—e.g., that we use those systems to access personally-identifiable information by an individual attribute such as name or SSN. OMB Memo 99-05, which the draft report cites, only applies to systems covered by the Privacy Act.

Many of the systems in the Agency's systems inventory are not Systems of Records under the Privacy Act (e.g., the Case Management e-Filing system, which accesses records by case number) or are covered by other agencies' SORNs (e.g., FPPS, WebTA, eOPF are all personnel records covered by OPM's records notice OPM/GOVT–1). Thus, we respectfully request that the draft report be modified to reflect that not all systems may require a routine use review or SORN because the Agency has made a determination that several of these systems are not covered by the Privacy Act or are under the control of another agency. We are committed to reviewing whether the Privacy Act applies to any remaining systems, including the GSS Network.

Finding No. 3 – Privacy Impact Assessments

5. *PIAs are required to be updated every 3 years (or earlier if the system had a significant change). PIAs are also required for new systems. A PIA has not been performed on 1 system:*
    a. *GSS Network.*

In September 2012, the SAOP and the CIO discussed whether a PIA was necessary for the GSS Network. At that time, they decided that no PIA was necessary because the GSS Network – as the overarching network infrastructure supporting the Agency's applications – was only a foundation for the information systems, not an information system itself. Although it is debatable whether a PIA is necessary for the GSS Network, we will develop a PIA for the GSS Network within 60 days of the final report.

Finding No. 4 – Website Updates

6. *The FLRA website didn't contain the following:*
    i. *Notification of the authority, purpose and use of the collection of information.*
    ii. *Notification of whether providing information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.*
    iii. *Machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences.*

The draft report identified that the FLRA's current website privacy policy did not reflect the FLRA's actual information collection practices. Contrary to language in the privacy policy, the FLRA does not collect any personally identifiable information, except through individuals' voluntary submission via efiling portals or email inquiries. On June 4, 2015, the FLRA updated the policy to reflect its current practices, which correct any deficiencies identified in Finding No. 4. The updated policy may be reviewed here.

The FLRA does not utilize machine-readable technology to alert users automatically about whether site privacy practices match their personal privacy preferences because the FLRA's website collects no information that would interfere with the personal privacy preferences a user would configure in his or her browser.

We respectfully request that the final report close this finding because of the Agency's successful resolution of the draft report's concerns.

Contacting the Office of Inspector General

If you believe an activity is wasteful, fraudulent, or abusive of Federal funds, contact the:

HOTLINE (800)331-3572

http://www.flra.gov/oig-hotline

email: oigmail@flra.gov
call: (202)218-7970 Fax: (202)208-4535
write to: 1400 K Street, N.W. Suite 250, Washington, D.C. 20424

The complainant may remain confidential; allow their name to be used; or anonymous. If the complainant chooses to remain anonymous, FLRA OIG cannot obtain additional information on the allegation, and also cannot inform the complainant as to what action FLRA OIG has taken on the complaint. Confidential status allows further communication between FLRA OIG and the complainant after the original complaint is received. The identity of complainants is protected under the provisions of the Whistleblower Protection Act of 1989 and the Inspector General Act of 1978. To learn more about the FLRA OIG, visit our Website at http://www.flra.gov/oig

Office of Inspector General

Privacy Program