



Office of Inspector General

# Privacy Program

## AUDIT OF THE FEDERAL LABOR RELATIONS AUTHORITY FY 2016 PRIVACY PROGRAM

FISCAL YEAR 2016

REPORT NO. AR-16-04

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



**OFFICE OF INSPECTOR GENERAL**  
Federal Labor Relations Authority

---

**TABLE OF CONTENTS**

OBJECTIVE ..... 2

BACKGROUND ..... 2

EXECUTIVE SUMMARY ..... 3

SUMMARY OF RESULTS ..... 3

STATUS OF PRIOR YEAR FINDINGS ..... 4

**APPENDIX A: Management Comments to the Draft Report**

## OBJECTIVE

The objective was to perform a privacy and data protection review and to follow-up on the Review of the Federal Labor Relations Authority Privacy and Data Security Policies, Procedures, and Practices for Fiscal Year 2015 Report No. AR-15-04. The purpose of our review was to perform the following:

- Conduct a review of the Federal Labor Relations Authority's (FLRA) privacy and data security policies, procedures, and practices in accordance with regulations;
- Review FLRA's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form;
- Review FLRA'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 FLRA employees and the public;
- Perform an analysis of FLRA'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; and
- Issue recommendations for improvements or enhancements to management of information in identifiable form, and the privacy and data protection procedures of the agency.

## BACKGROUND

Dembo, Jones, Healy, Pennington & Marshall, P.C., on behalf of the 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 2016 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.
- Personal information may be able to be used only 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 no new findings and we determined that the FLRA successfully implemented 5 out of 6 of our prior year recommendations. The FLRA hired an external Privacy expert, who provided training to staff on Privacy related matters. Additionally, FLRA also wrote, approved, and posted updated Privacy Impact Assessments. Lastly, the FLRA's website had significant updates, whereby it currently complies with Privacy related requirements.

## STATUS OF PRIOR YEAR FINDINGS

#	POA&M Year / Number	POA&M (Recommendations)	Open / Closed
1	2015 Finding # 1 Recommendation # 1	<p>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:</p> <ul style="list-style-type: none"> <li>a. Complete inventory of systems and the type of data residing on those systems.</li> <li>b. The safeguarding of data on those systems.</li> <li>c. The management of the systems. For example, are the systems managed by a third party or managed in-house by the FLRA?</li> <li>d. Electronic versus paper-based systems.</li> <li>e. The types of controls deployed and whether or not this is commensurate with the data residing on the systems.</li> <li>f. PIAs for each system.</li> <li>g. System of Records Notices (SORNs) and routing uses for each system.</li> </ul>	Closed
2	2015 Finding # 1 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.	Closed
3	2015 Finding # 2 Recommendation # 3	The Senior Agency Official for Privacy (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.	Open
4	2015 Finding # 2 Recommendation # 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.	Closed
5	2015 Finding # 3 Recommendation # 5	IT should complete a new PIA for the GSS network. The PIAs should be approved and reviewed by the SAOP.	Closed
6	2015 Finding # 4 Recommendation # 6	IT and Privacy should meet to discuss the various website requirements and then update the website accordingly.	Closed

## **APPENDIX A:**

### **Management Comments to the Draft Report**




UNITED STATES OF AMERICA  
**FEDERAL LABOR RELATIONS AUTHORITY**

May 18, 2016

**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 Follow-Up Review of the Federal Labor Relations Authority Fiscal Year 2016 Privacy Program Report No. AR-16-04

Thank you for the opportunity to review and provide comments on the April 28, 2016 draft follow-up evaluation of the FLRA's Privacy Program. We are pleased to learn that the auditors concluded that our program is "strong," closed five of last years' findings, and identified no new findings.

The single remaining finding in the draft report concerns 2015 Finding No. 1, Recommendation #3:

*The Senior Agency Official for Privacy (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.*

The Solicitor's Office is finalizing a global update of the Agency's System of Records Notices (SORNs). As part of that update, we will continue to review whether any of the Agency's electronic systems require SORN. We have already concluded that 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 existing or other agencies' SORNs (e.g., FPPS, WebTA, eOPF are all personnel records covered by OPM's records notice OPM/GOVT-1 and FLRA SORNs governing time and attendance records). As part of the process of updating the Agency's SORNs, we will ensure that IT provides its expertise and input. We expect to have the updated SORN in place by January 2017.

We appreciate your consideration in finalizing the report.

# 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](http://www.flra.gov/oig-hotline)**

EMAIL: [OIGMAIL@FLRA.GOV](mailto:OIGMAIL@FLRA.GOV)  
CALL: (202)218-7970 FAX: (202)343-1072  
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