



Office of Inspector General

FLRA Privacy Program
Review FY 2019

REVIEW OF THE FEDERAL
LABOR RELATIONS
AUTHORITY PRIVACY AND
DATA PROTECTION PROGRAM
FOR FY 2019

Report No. MAR-19-04
September 2019

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

Table of Contents

Review Report

Executive Summary	1
Objective	1
Background	2
Summary of Results	3

Appendix

Appendix 1: Report Distribution	4
---------------------------------------	---

Abbreviations

FY	Fiscal Year
FLRA	Federal Labor Relations Authority
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information

Review of the FLRA Privacy and Data Protection Program for FY 2019

Report No. MAR-19-04

September 10, 2019

The Honorable Colleen Duffy Kiko, Chairman

Dembo Jones, P.C. was engaged by the Federal Labor Relations Authority (FLRA) Office of Inspector General (OIG) to perform a Privacy and Data Protection Review for Fiscal Year (FY) 2019.

The objective was to perform a privacy and data protection review of FLRA's Privacy and Data Security Policies, Procedures and Practices for FY 2019. A detailed description of our objective is below.

This year's Privacy review resulted in no new findings. Overall, we determined that the FLRA's Privacy program is strong.

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.

One new finding (which was closed during the current FY) related to the onboarding of new employees and contractors. Employees and contractors were not required to review and indicate that they have in fact understood their privacy roles and responsibilities through receipt of the latest Privacy policies. Prior to issuing this report and within the FY, this deficiency had been remediated successfully.

Objective

The objective was to perform a privacy and data protection review of the FLRA Privacy and Data Security Policies, Procedures, and Practices for FY 2019. The purpose of our review was to perform the following:

- Conduct a review of the (FLRA privacy and data security policies, procedures, and practices in accordance with regulations;

Review of the FLRA Privacy and Data Protection Program for FY 2019 (Report No. MAR-19-04)

-
- 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, 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 FY 2019 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.

Summary of Results

Overall, the FLRA's Privacy program is strong. This year's Privacy audit resulted in no new open findings. 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.

Appendix 1

Report Distribution

Federal Labor Relations Authority

The Honorable Ernest DuBester, Member
The Honorable James Abbott, Member
Michael Jeffries, Executive Director
Rebecca Osbourne, Deputy Solicitor
David Fontaine, Acting Chief Information Officer

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
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>



**FLRA Privacy Program
Review FY 2019**