



Office of Inspector General

Review of the FLRA's
Privacy and Data Security
Policies, Procedures and
Practices for FY 2024

Review of the
FLRA's Privacy
and Data Security
Policies,
Procedures and
Practices for FY
2024

Report No. MAR-24-06

June 2024

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

Table of Contents

Review Report

Executive Summary	1
Objective	1
Background	2
Findings.....	3
Recommendations.....	4

Appendices

Appendix 1: Management Response	5
Appendix 2: Report Distribution	7

Abbreviations

FLRA	Federal Labor Relations Authority
FY	Fiscal Year
IR	Incident Response
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PM	Program Management
PII	Personally Identifiable Information

Review of the FLRA’s Privacy and Data Security Policies, Procedures, and Practices for FY 2024

Report No. MAR-24-06

June 26, 2024

The Honorable Susan Tsui Grundmann, 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) 2024.

The objective was to perform a privacy and data protection review of FLRA’s Privacy and Data Security Policies, Procedures, and Practices for FY 2024. A detailed description of our objective is below. This year’s Privacy and Data Protection Review resulted in two new findings.

Executive Summary

Dembo Jones, P.C., on behalf of the FLRA, 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, Office of Management and Budget memorandums, Consolidated Appropriations Act of 2005, etc.). The Consolidated Appropriations Act of 2005, codified in relevant part at 42 U.S.C. § 2000ee-2, requires agencies to assign a Chief Privacy Officer who is responsible for identifying and safeguarding personally identifiable information (PII) and requires periodic OIG or OIG-contracted independent third-party review of agency use of PII and of its privacy and data protection policies and procedures.

There were two new findings in the current fiscal year. In a written management response, FLRA agreed with our recommendations. Based on the results of our review, we determined that a review is warranted in FY 2025, to include a follow-up on the FY 2024 report.

Objective

The objective was to perform a privacy and data protection review of the Federal Labor Relations Authority Privacy and Data Security Policies, Procedures, and Practices for FY 2024. 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 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 to management for improvements or enhancements 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, OIG, conducted an independent evaluation of the quality and compliance of the FLRA privacy program with applicable Federal information security laws and regulations.

The Privacy Act of 1974, 5 U.S.C. § 552a, 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 individuals.

The Privacy Act applies to *Federal Government Agencies* and governs their use of a system of records, which is defined as “a group of any records under the control of any 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.”¹

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

- Publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records.
- No agency may disclose personal information to third parties without the consent of the individual (with some exceptions).
- No agency may maintain records on how an individual exercises their First Amendment rights (with some exceptions).
- Federal personal information records are limited only to data that is relevant and necessary.
- Individuals must have access to the records maintained about them by the Federal Government (with some exceptions).
- Individuals must have the opportunity to request correction or amendment to any inaccuracies or incompleteness in their records.

¹ 5 U.S.C. § 552a(a)(5).

Findings

Upon review of the various artifacts, there were (2) deficiencies that were uncovered. There was a total of (44) Privacy controls that were reviewed from National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020). Of those (44) controls, the following had associated deficiencies:

IR-8 (1)

“Include the following in the Incident Response Plan for breaches involving personally identifiable information:

- (a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
- (b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
- (c) Identification of applicable privacy requirements.”

Deficiency

Upon review of the Incident Response Policy and Standard Operating Procedure, we determined that it does not contain the necessary procedures for how to respond to PII breaches, therefore this control is considered "non-compliant."

PM-25

- “a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research;
- b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
- c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
- d. Review and update policies and procedures [*Assignment: organization-defined frequency*].”

Deficiency

Assessor obtained several artifacts for this year's Privacy engagement; however, there were no documents that showed PII is minimized when testing, training, and research is conducted, therefore this control is considered non-compliant.

Recommendation(s):

The Director of the Information Resources Management Division and the Senior Agency Official for Privacy (SAOP) should:

1. Update the Incident Response Policy to include procedures for how to respond to breaches in PII, as follows:
 - a. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
 - b. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
 - c. Identification of applicable privacy requirements.
2. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research and ensure the following:
 - a. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
 - b. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
 - c. Review and update policies and procedures.

Management Response:

Management has agreed with our recommendations. Their response is attached in Appendix 1.



*North Bethesda, Maryland
June 26, 2024*

Appendix 1

Management Response




UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

June 25, 2024

MEMORANDUM

TO: Dana Rooney, Inspector General

FROM: Rebecca J. Osborne, Director of Legislative Affairs and Program Planning

THROUGH: Michael Jeffries, Executive Director 

SUBJECT: Management Response to *Review of the FLRA's Privacy and Data Security Policies, Procedures and Practices for FY 2024* (Report No. MAR-24-06)

Thank you for the opportunity to review and provide comments on the Office of Inspector General's (OIG) report on the Federal Labor Relations Authority's compliance with the Privacy Act and associated information security concerns. The FLRA is committed to making sure that PII, as well as all Government data is handled in a secure and appropriate manner.

RECOMMENDATIONS

The Director of Information Resource Management and the Privacy Act Officer should:

- a. Update the Incident Response Policy to include procedures for how to respond to breaches in PII, as follows:
 - A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
 - An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
 - Identification of applicable privacy requirements.
- b. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research and ensure the following:
 - Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;
 - Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
 - Review and update policies and procedures.

Management Response: FLRA appreciates the Inspector General’s thorough investigation of our compliance with the Privacy Act. Management agrees with the recommendations and will work quickly to implement the proposed changes. The Privacy Office and the Information Resources Management Division will work together to supplement our existing documentation to include specific language as identified in the report.

As always, we appreciate your consideration of these responses and look forward to continuing our efforts to find innovative ways to improve.

CC: Thomas Tso, Solicitor

Appendix 2

Report Distribution

The Honorable Colleen Duffy Kiko,
Member

Michael Jeffries, Executive Director

Dave Fontaine, Director, Information
Resources Management Division

Thomas Tso, Senior Agency Official for Privacy

CONTACTING THE OFFICE OF INSPECTOR GENERAL

IF YOU BELIEVE AN ACTIVITY IS WASTEFUL,
FRAUDULENT, OR ABUSIVE OF FEDERAL FUNDS,
CONTACT THE:

HOTLINE (877)740-8278

https://www.flra.gov/OIG-FILE_A_COMPLAINT

EMAIL: OIGMAIL@FLRA.GOV

CALL: (771)444-5712 FAX: (202)208-4535

WRITE TO: 1400 K Street, N.W. 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

Review FLRA's Privacy and Data
Security Policies, Procedures and
Practices for FY 2024