



Office of Inspector General

FOLLOW-UP ON THE EVALUATION OF THE
FEDERAL LABOR RELATIONS AUTHORITY'S
COMPLIANCE WITH THE PRIVACY ACT
MANDATORY ANNUAL TRAINING REQUIREMENT
FOR FISCAL YEAR 2023

**FOLLOW-UP ON THE
EVALUATION OF THE
FEDERAL LABOR
RELATIONS AUTHORITY'S
COMPLIANCE WITH THE
PRIVACY ACT MANDATORY
ANNUAL TRAINING
REQUIREMENT FOR FISCAL
YEAR 2023**

**Report No. MAR-25-08
July 2025**

Federal Labor Relations Authority
1400 K Street, N.W., 3rd Floor, Washington, D.C. 20424

Table of Contents

Management Advisory Review

Results in Brief	1
Background	1
Results in Detail	3
Conclusion	3

Appendices

Appendix 1: Objective, Scope, and Methodology	4
Appendix 2: Report Distribution	5

Acronyms

FY	Fiscal Year
FLRA	Federal Labor Relations Authority
IT	Information Technology
MAR	Management Advisory Review
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SAOP	Senior Agency Official for Privacy
U.S.C.	United States Code

Follow-Up on the Evaluation of the Federal Labor Relations Authority's Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023

Report No. MAR-25-08

July 9, 2025

The Honorable Colleen Duffy Kiko
Chairman

This report presents the results of our follow-up review to the Office of Inspector General (OIG) report, *Evaluation of the Federal Labor Relations Authority's Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023*, Report No. MAR-25-01. We issued Report MAR-25-01 on October 7, 2024, and made three recommendations that the Federal Labor Relations Authority (FLRA) management concurred with. For this follow-up report, our work was limited to reviewing, as of June 10, 2025, the actions taken to implement these three recommendations.

Results in Brief

The FLRA OIG conducted a follow-up review of the report titled, *Evaluation of the Federal Labor Relations Authority's Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023*, Report No. MAR-25-01. We determined that the FLRA has taken sufficient action to implement the three recommendations made in that report. Therefore, we are closing out these recommendations and this report. The background and details are as follows.

Background

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, prescribes how Federal agency records containing individually identifiable information are to be maintained, who may access such information, how that information may be accessed, and when the Government may use or disclose the information. The general rule under the Privacy Act is that an agency cannot disclose a record contained in a system of records unless the individual to whom the record pertains gives prior written consent to the disclosure.¹ There are 12 exceptions to this general rule.²

The Privacy Act also requires Federal agencies to instruct their employees on the law and the rules and procedures established by the agency with regards to the agency's implementation of the law.³ The Office of Management and Budget (OMB) provided guidance issued on July 9, 1975, Privacy Act Implementation, Guidelines and Responsibilities, 40 Fed. Reg. 28948, which

¹ 5 U.S.C. § 552a(b).

² *Id.*

³ *Id.* § 552a(e)(9) (“Each agency that maintains a system of records shall ... establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance; ...”).

stated the need for Federal agencies to provide training to their employees.⁴ OMB provided further instruction on the Privacy Act in OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016), which states: “Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII [Personally Identifiable Information] for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.”⁵ Further, OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016): states:

Agencies shall design their privacy control selection process to include privacy controls that allow the agency to ensure compliance with applicable requirements in the Privacy Act and related OMB guidance. At a minimum, the controls selected for an information system that contains information in a system of records shall address the following elements:

...

Privacy Training. Agencies shall ensure that the agency’s training practices are sufficient and that agency personnel understand the requirements of the Privacy Act, OMB guidance, the agency’s implementing regulations and policies, and any job-specific requirements.⁶

FLRA’s Policy No. 1312, *Protection of Personally Identifiable Information*, was issued on November 3, 2010.⁷ It sets formal policy regarding the protection of PII and requires annual training by all FLRA employees, contractors, and others with access to FLRA Information Technology (IT) systems or records.^{8,9} The policy also defines roles and responsibilities for employees and other key officials such as the Senior Agency Official for Privacy (SAOP). The FLRA Solicitor is the FLRA’s SAOP. It is important to note that the scope of our review was limited to reviewing FLRA employee compliance with the mandatory training requirement and did not include whether the SAOP properly identified any and all FLRA contractor employees who must take the training.

Original Report

On October 7, 2024, the OIG issued a report (MAR-25-01) to the FLRA Chairman titled, *Evaluation of the Federal Labor Relations Authority’s Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023*. The objective of this review was

⁴ 40 Fed. Reg. at 28965-66, 28970.

⁵ OMB Circular A-130, Appendix II, § 3.b.

⁶ OMB Circular A-108, § 12.f.

⁷ On June 10, 2025, FLRA issued a revised version of this policy in response to OIG’s initial report.

⁸ See Policy No. 1312, § 1312.4.k.(3) (requiring “FLRA Users,” those with access to FLRA IT systems or records, to “[c]omplete annual agency-wide PII training and, as appropriate, office or job specific training”); § 1312.4.j.(1) (requiring supervisors to “[e]nsure that employees within their organization complete any required agency-wide PII training, including the required annual Information Systems Security Awareness Training.”).

⁹ FLRA Policy No. 1312 defines “FLRA User” as: “employee, contractor, intern, volunteer, detailee, or other individual performing work for FLRA with access to FLRA IT systems, FLRA’s operational records, or FLRA’s accessioned records and donated historical materials that contain PII.” FLRA Policy No. 1312, § 1312.3.f.

to determine whether all FLRA employees took the mandatory annual privacy training that took place on September 27, 2023 for Fiscal Year (FY) 2023. FLRA employees and users had the option of watching the training live or subsequently watching a recording of the live training event. Our review determined that FLRA's SAOP had not effectively monitored the completion of annual privacy training for FY 2023 to ensure 100 percent compliance by FLRA employees. This was in part due to not having a complete employee roster. Also, the follow-up that was conducted by the Office of the Solicitor with employees who had not taken the training did not include any notification to the employees' supervisors so that the supervisors could take appropriate action to ensure their employees took the mandatory privacy training. We also found that FLRA's policy regarding the protection of PII was 14 years old (predating revisions to the OMB Circulars referenced in this report).

We made three recommendations to the SAOP as follows:

1. Develop and implement a process to monitor the completion of mandatory annual privacy training including the notification of supervisors.
2. Obtain an up-to-date and accurate FLRA users roster for tracking compliance.
3. Review FLRA's Policy No. 1312, *Protection of Personally Identifiable Information*, to ensure it is up-to-date with current OMB guidance and update if necessary.

Results in Detail

Our follow-up review determined that the SAOP instituted procedures to properly monitor the completion of the mandatory annual privacy training by FLRA users. This also included ensuring the Office of the Solicitor has a current employee roster of FLRA employees and other users. The SAOP provided documentation that demonstrated steps taken by FLRA for the monitoring of the FY 2024 mandatory annual privacy training. FLRA continued follow-up and monitoring FLRA users until it achieved 100 percent compliance with the FY 2024 privacy training.

The SAOP also conducted a review of FLRA Policy No. 1312, *Protection of Personally Identifiable Information*. Necessary updates as determined by the SAOP were made to the policy to ensure it was up-to-date with all statutory, regulatory, and OMB requirements. This policy was approved by FLRA leadership and became effective June 10, 2025.

Conclusion

We determined that the FLRA has taken appropriate action to close-out the three open recommendations. This is the follow-up and close-out report for OIG Report MAR-25-01.

Appendix 1: Objective, Scope, and Methodology

This follow-up review of the *Evaluation of the Federal Labor Relations Authority's Compliance with the Privacy Act Mandatory Annual Training Requirement for Fiscal Year 2023*, Report No. MAR-25-01, was conducted to review the status of the implementation of the open recommendations. We made three recommendations in our original report.

The objective of this review was limited to determine whether the FLRA acceptably resolved and implemented the three open recommendations in report MAR-25-01. Our review was limited to reviewing the finalized policy and did not include any testing as to the effectiveness of the policy.

We engaged the SAOP and obtained necessary documentation. The information requested was examined, along with management feedback, in order to analyze and draw conclusions. Our conclusions were based on this analysis. A preliminary version of the report was shared with management for their awareness.

Appendix 2: Report Distribution

FLRA

The Honorable Anne M. Wagner, Member
Solicitor
Executive Director
Chief Information Officer

Contacting the Office of Inspector General

If you know of fraud, waste, or misconduct
relating to an FLRA program, contract, or
employee, you may report it to the FLRA OIG

Hotline:

HOTLINE (877) 740-8278

[HTTP://WWW.FLRA.GOV/OIG-Hotline](http://www.flra.gov/OIG-Hotline)

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

WRITE: 1400 K Street, N.W., 3rd Floor
Washington, D.C. 20424

When reporting information, you may choose to be confidential, which means the FLRA OIG will not disclose your identity without your consent, unless the Inspector General determines that such a disclosure is unavoidable during the course of an investigation. You may instead choose to be anonymous. Anonymous reports may limit our ability to process the information you provide as we would not be able to contact you for additional information or clarification. To learn more about the FLRA OIG, visit our website at: www.flra.gov/components-offices/offices/office-inspector-general



Office of Inspector General

FOLLOW-UP ON THE EVALUATION OF THE
FEDERAL LABOR RELATIONS AUTHORITY'S
COMPLIANCE WITH THE PRIVACY ACT
MANDATORY ANNUAL TRAINING REQUIREMENT
FOR FISCAL YEAR 2023