Office of Inspector General

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S PREPAREDNESS AGAINST CYBERSECURITY ATTACKS FISCAL YEAR 2025

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S PREPAREDNESS AGAINST CYBERSECURITY ATTACKS FISCAL YEAR 2025

Report No. MAR-25-04
March 2025

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

CONTENTS

Abbreviations

Dembo Jones	Dembo Jones, P.C.
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
SOP	Standard Operating Procedure
SSPP	System Security and Privacy Plan

Evaluation of the FLRA's Preparedness Against Cybersecurity Attacks

Report No. MAR-25-04 ***March 18, 2025***

The Honorable Colleen Duffy Kiko
Chairman

Dembo Jones, P.C. (Dembo Jones), on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent evaluation of the agency's preparedness against cybersecurity attacks. Dembo Jones' evaluation focused on FLRA's information security as it relates to compliance against the National Institute of Standards and Technology's Special Publication 800-61, "Computer Security Incident Handling Guide" (August, 2012).

Results in Brief

During our Fiscal Year (FY) 2025 evaluation, we noted that the FLRA has taken significant steps to improve the information security program. We also noted that the FLRA does take information security weaknesses seriously. This year's testing identified no new findings. Specifically, below are some of those compliance measures that we found at the FLRA:

- Maintenance of a list of security events and incidents for analysis and review of current processes and procedures.
- FLRA has various Policies in place such as:
    - Incident Response Policy (includes means for communicating with the media and sharing of data with other relevant parties).
    - Incident Response Procedures.
    - Incident Response Standard Operating Procedures (SOPs).
- Security Awareness training.
- Updated System Security and Privacy Plan (SSPP).
- Various firewall and other network configuration settings to ensure that attacks are prevented from being exploited on the FLRA network.
- Maintenance of baseline configurations.
- Virus definitions are current and up to date.
- File integrity software is deployed throughout the network.

Scope and Methodology

The scope of our testing focused on the FLRA network General Support System; however, the testing also included other systems in the FLRA system inventory. Our testing also included coverage of the network infrastructure, Policies, Procedures, and SOPs. We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Examples of our inquiries and examination with FLRA management and personnel included, but were not limited to, a review and evaluation of the following:

- SSPP.
- Review of Policies, Procedures (including media and information sharing with other relevant parties), and SOPs.
- Review of network configurations to ascertain if vulnerabilities will be prevented and detected prior to potential exploitation.
- Review of the latest FLRA Risk Assessment.
- Review of standard configurations and the maintenance of baseline configurations.
- Deployment of various products to prevent exploitation.

Dembo Jones, P.C.

North Bethesda, Maryland
March 18, 2025

Appendix
Report Distribution

Federal Labor Relations Authority

Susan Tsui Grundmann, Member
Anne M. Wagner, Member
Michael Jeffries, Executive Director
Dave Fontaine, Chief Information Officer
Thomas Tso, Solicitor

Contacting the Office of Inspector General

IF YOU KNOW ABOUT FRAUD, WASTE, ABUSE, 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

CALL: (877) 740-8278 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/oig

Office of Inspector General

EVALUATION OF THE FEDERAL LABOR RELATIONS AUTHORITY'S PREPAREDNESS AGAINST CYBERSECURITY ATTACKS FISCAL YEAR 2025