Office of Inspector General

Evaluation of the FLRA's Preparedness Against Cyber Security Attacks

EVALUATION OF THE FLRA'S PREPAREDNESS AGAINST CYBER SECURITY ATTACKS

Report No. MAR-23-04
May 2023

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

CONTENTS

Abbreviations

Dembo Jones	Dembo Jones, P.C.
FLRA	Federal Labor Relations Authority
SOPs	Standard Operating Procedures
SSPP	System Security Privacy Plan

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Evaluation of the FLRA's Preparedness Against Cyber Security Attacks

Report No. MAR-23-04 ***May 3, 2023***

The Honorable Susan Tsui Grundmann
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 cyber security attacks. Dembo Jones' evaluation focused on FLRA's information security as it relates to compliance against National Institute of Standards and Technology Special Publication 800-61, "Computer Security Incident Handling Guide".

Results in Brief

During our Fiscal Year 2023 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.
- Security Awareness training.
- Updated System Security 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.

6116 Executive Blvd • Suite 500
North Bethesda, MD 20852
P 301.770.5100 • F 301.770.5202

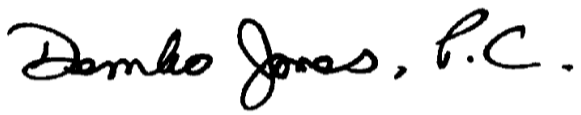
Dembo Jones, P.C.
A Member of Allinial Global
www.dembojones.com

8850 Stanford Blvd • Suite 2000
Columbia, MD 21045
P 410.290.0770 • F 410.290.0774

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 Standard Operating Procedures (SOPs). We conducted our testing through inquiry of FLRA personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Some examples of our inquiries with FLRA management and personnel included, but were not limited to 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
May 3, 2023

Appendix 1

Report Distribution

Federal Labor Relations Authority

Colleen Duffy Kiko, Member
Michael Jeffries, Executive Director
Dave Fontaine, Chief Information Officer
Rebecca Osbourne, Deputy Solicitor

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

email: oigmail@flra.gov
call: (877)740-8278 Fax: (202)208-4535
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

Evaluation of the FLRA's Preparedness Against Cyber Security Attacks