DEMBO·JONES

CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

May 2017 **Federal Labor Relations Authority (FLRA)**
Office of Inspector General

Independent Accountants' Report on

Evaluation of the FLRA Privacy and Data Protection

CONTENTS

Evaluation Report

Appendices

Abbreviations

CIGIE	Council of the Inspectors General on Integrity and Efficiency
FLRA	Federal Labor Relations Authority
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
U.S.	United States

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Evaluation Report

The Federal Labor Relations Authority
Office of Inspector General

May 9, 2017

The Honorable Patrick Pizzella
Acting Chairman
Federal Labor Relations Authority

Dear Mr. Pizzella:

This report presents the results of our evaluation of the Federal Labor Relations Authority (FLRA) privacy and data protection program and follow-up on the prior year Audit of the Federal Labor Relations Authority Fiscal Year 2016 Privacy Program Report No. AR-16-04. We contracted with the FLRA Office of Inspector General (OIG) to perform the privacy and data protection evaluation.

We performed a Privacy and Data Protection evaluation in accordance with privacy and data protection related laws and guidance (e.g. Privacy Act of 1974, Office of Management and Budget (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.

Our evaluation identified a new finding (which was closed during the current fiscal year) 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 fiscal year, this deficiency had been remediated successfully.

Results in Brief

Overall, the FLRA's Privacy program is strong. Out of 73 different testing areas, this year's Privacy audit resulted in one new finding, and however, as of the end of the fiscal year this finding was closed. The prior year showed an open finding and that was also closed as part of testing this year. The FLRA hired an external

Privacy expert, who provided training to staff on Privacy related matters. 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.

We conducted our fieldwork in March and April 2017. Appendix I contains a detailed description of our objective, scope, and methodology.

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 computer security laws and regulations. The vulnerabilities discussed in this report should be included in FLRA's Fiscal Year 2017 report to OMB.

The Privacy Act of 1974 regulates the use of personal information by the United States (U.S.) 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.

Evaluation Results

We performed our evaluation using the Council of the Inspector General on Integrity and Efficiency Quality Standards for Inspection and Evaluation issued January 2012. Our evaluation determined the FLRA's Privacy Program is strong. This year's evaluation resulted in one finding, however, FLRA management took action to close this finding within the fiscal year.

We also performed a follow-up on one prior year finding that was also closed. For details on the status of current and prior year findings (See Appendix II).

Dembo Jones, P.C.

Rockville, Maryland
May 9, 2017

Appendix I: Objective, Scope, and Methodology

Our objective was to perform a privacy and data protection evaluation and to follow-up on the review of the Federal Labor Relations Authority Fiscal Year 2016 Privacy Program Report No. AR-16-04. We initiated our review in March 2017 and performed the following:

- Conducted an evaluation of the Federal Labor Relations Authority's (FLRA) privacy and data security policies, procedures, and practices in accordance with regulations;
- Reviewed FLRA's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form;
- Reviewed 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;
- Performed an analysis of FLRA's intranet, network, and websites for privacy vulnerabilities (through review of source documents):
    - Noncompliance with stated practices, procedures, and policy; and
    - Risks of inadvertent release of information in an identifiable form from the website of the agency; and
- Issued recommendations for improvements or enhancements to management of information in identifiable form, and the privacy and data protection procedures of the agency.

Appendix II: Status of Current and Prior Year Findings

#	POA&M Year / Number	POA&M (Recommendations)	Open / Closed
1	2017	As part of the Privacy review during the current fiscal year, it was revealed that new employees and contractors were not required to acknowledge that they read, understood and agreed to the respective agency Privacy policies, procedures and Rules of Behavior. Subsequent to the identification of this deficiency, it was remediated immediately and therefore it is documented in this report for information purposes only. However the finding is closed.	Closed
2	2015 Finding # 2 Recommendation # 3	The Senior Agency Official for Privacy and IT should review all routine uses for all systems and coordinate this review. If any of those routine uses are no longer appropriate, IT should work with the Privacy Act Officer to delete those routine uses from the Systems of Records Notices and update accordingly on the agency's website.	Closed

Appendix III: Report Distribution

Federal Labor Relations Authority

The Honorable Ernest DuBester, Member
Michael Jeffries, Acting Executive Director
Fred Jacob, Solicitor
David Fontaine, Acting Chief Information Officer