Office of Inspector General

Review of FLRAs Privacy Program for FY 2020

REVIEW OF THE FEDERAL LABOR RELATIONS AUTHORITY PRIVACY AND DATA PROTECTION PROGRAM FOR FY 2020

Report No. MAR-20-06

August 2020

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

Table of Contents

Review Report

Appendixes

Abbreviations

CIO	Chief Information Officer
FLRA	Federal Labor Relations Authority
FY	Fiscal Year
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Review of the FLRA Privacy and Data Protection Program for FY 2020

Report No. MAR-20-06 ***August 5, 2020***

The Honorable Colleen Duffy Kiko, 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) 2020.

The objective was to perform a privacy and data protection review of FLRA's Privacy and Data Security Policies, Procedures and Practices for FY 2020. A detailed description of our objective is below.

Executive Summary

The 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 (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.

There was one new finding in the current year. The new finding related to the Privacy Impact Assessments. There were several Privacy Impact Assessments (PIA) that had not been updated in more than 3 years.

In a written management response, FLRA agreed with our recommendations. Based on the results our review, we determined that a follow-up review is not warranted in 2021.

Objective

The objective was to perform a privacy and data protection review of the FLRA Privacy and Data Security Policies, Procedures, and Practices for FY 2020. The purpose of our review was to perform the following:

- Conduct a review of the FLRA's privacy and data security policies, procedures, and practices in accordance with regulations;

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

- 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 for improvements or enhancements to management 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 computer security laws and regulations. The vulnerabilities discussed in this report should be included in FLRA's FY 2020 report to the OMB.

The Privacy Act of 1974 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 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.

Summary of Results

Overall, the FLRA's Privacy program is strong. This year's Privacy audit resulted one new finding. Additionally, FLRA also posted PIAs for existing systems, as well as posted System of Records Notice and other Privacy related policies on the agency's website. For example, the FLRA's website had significant updates, whereby it currently complies with Privacy related requirements.

Finding

Privacy Impact Assessments

A PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Condition:

PIAs are required to be updated every 3 years (or earlier if the system had a significant change). PIAs are also required for new systems. Several systems had old or outdated PIAs, where they hadn't been updated in more than three years.

Criteria:

The OMB has specific requirements regarding when and how a PIA should be conducted. This criteria states the instances when a PIA shall be performed as noted by **OMB Memorandum No. 03-22 section II.B.2:**

The E-Government Act of 2002 requires agencies to conduct a PIA. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:

- Conversions - when converting paper-based records to electronic systems;

- Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
- Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
- Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated;
- New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
- Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
- New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
- Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form;
- Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

Cause:

The Chief Information Officer (CIO) and Privacy Act Officer haven't had the appropriate coordination to identify those systems needing a PIA.

Risk:

With incomplete PIAs, FLRA may not be deploying security controls that are commensurate with the PII that resides on those systems.

Recommendation(s):

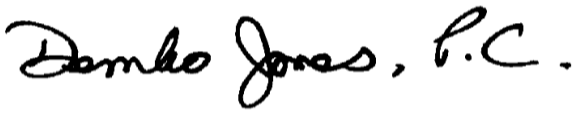
1. The CIO should update the PIAs for those systems with an outdated PIA.

2. The CIO should work with the Privacy Act Officer to determine if there are PIAs needed for those systems that have not had a PIA. Furthermore, the Privacy Act Officer should determine whether the PIAs should be posted on the FLRA's website.

Management Response:

Management agrees with our finding. Based on our finding, management reviewed and updated three FLRA PIAs that needed to be updated. They have also scheduled quarterly privacy meetings to avoid potential vulnerabilities in the FLRA's privacy program.

Dembo Jones, P.C.



North Bethesda, Maryland
August 5, 2020

Appendix 1
Management Response

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

July 31, 2020

MEMORANDUM

TO: Dana Rooney Inspector General

FROM: Noah Peters, Solicitor and Senior Agency Official for Privacy Dave Fontaine, Chief Information Officer

THROUGH: Michael Jeffries
Executive Director

SUBJECT: Management Response to Draft Report Evaluation of the Federal Labor Relations Authority Fiscal Year 2020 Privacy Program Report No. MAR-20-06

Thank you for the opportunity to review and provide comments on the July 2020 draft evaluation of the Privacy Program of the Federal Labor Relations Authority ("FLRA"). Please accept this memorandum as management's response to the draft.

To begin, we are pleased to learn that the auditors concluded that our program is "strong" and identified only one issue in an exhaustive evaluation of different testing areas of privacy protection.

Below, we provide our response to the one finding in the draft report. We appreciate your consideration of this response in finalizing the report.

Finding No. 1 –Privacy Impact Assessments ("PIAs")

1. *PIAs are required to be updated every 3 years (or earlier if the system had a significant change). PIAs are also required for new systems. Several systems had old or outdated PIAs, where they hadn't been updated in more than three years.*

Although designees of the Chief Information Officer ("CIO") and Senior Agency Official for Privacy ("SAOP") have met on an ad hoc basis to discuss privacy matters (particularly surrounding the annual FISMA audit), the FLRA's CIO and SAOP have taken steps, including scheduling quarterly privacy meetings, to correct this finding and to avoid potential vulnerabilities in the FLRA's privacy program.

Subsequent to this finding, the FLRA's CIO and SAOP reviewed and updated three FLRA PIAs that needed to be updated: the FLRA's General Support System Network PIA, the FLRA's E-Gov Travel Services 2, and the FLRA's PRISM PIA (all three updated PIAs are attached hereto as Exhibit A). The FLRA has posted the updated PIAs on its website and those PIAs may be viewed by the public here. The FLRA's CIO and SAOP also have reviewed the FLRA's remaining PIAs and determined that no additional PIAs (or updates) are needed at this time.

In light of our implementation of this recommendation, we respectfully request that the final report close this finding because of the FLRA's successful resolution of the draft report's concerns.

Appendix 2
Report Distribution

Federal Labor Relations Authority

The Honorable Ernest DuBester, Member
The Honorable James Abbott, Member
Michael Jeffries, Executive Director
Noah Peters, Solicitor
David Fontaine, Chief Information Officer

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: (202)218-7970 Fax: (202)343-1072
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

Review of FLRA's Privacy Program for FY 2020