Office of Inspector General

Information Technology Asset Inventory Review

INFORMATION TECHNOLOGY ASSET INVENTORY REVIEW

Report No. MAR-21-06

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

CONTENTS

Management Advisory Report

Appendices

Abbreviations

CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FLRA	Federal Labor Relations Authority
HSPD	Homeland Security Presidential Directive
IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information

DEMBO·JONES
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Information Technology Asset Inventory Review
July 8, 2021

The Honorable Ernest DuBester, Chairman

This report presents the results of our review of the Federal Labor Relations Authority (FLRA) Information Technology (IT) Asset Inventory. We contracted with the FLRA Office of Inspector General (OIG) to perform the IT asset inventory review.

Results in Brief

Overall, the FLRA's policies, records and controls over IT asset inventories are strong, however improvements need to be made. Several laptops were unassigned in terms of which employee is responsible (assigned) for the respective equipment.

In a written response, FLRA management acknowledged our finding and intends to take the corrective action. Overall, we found that management's response meets the intent of our recommendation.

We conducted our fieldwork in April and May of 2021. Appendix I contains a detailed description of our objective, scope, and methodology. Appendix 2 provides management's response to the OIG recommendations.

Background

Dembo Jones, P.C., on behalf of the FLRA, OIG, conducted an independent IT Asset inventory review of the FLRA's IT equipment (e.g. desktops, laptops, servers, printers, monitors, routers, switches and firewalls).

All agencies within the executive branch of Government will be required to comply with the Department of Homeland Security's (DHS) new mandate as it relates to Continuous Diagnostics and Mitigation (CDM). The requirements of CDM stipulate those specific tools will be deployed thereby ensuring that all hardware and software are accounted for. FLRA contracted with our firm to assess the current asset inventory in terms of its completeness and accuracy.

Evaluation Results

Our evaluation determined FLRA has made great strides in improving their inventory practices. The IT asset inventory policies and procedures have been reviewed, updated, and approved. Position descriptions were updated to ensure that personnel understand their job responsibilities. This year's review resulted in one finding below:

#	Deficiency	Risk	Risk Ranking
1	Several laptops were unassigned in terms of who is responsible for the respective equipment.	Without appropriate assignments to all IT inventory items, there is the risk that inventory can be misclassified and/or assigned to the wrong person. This may also lead to lost/stolen IT equipment, as it is not currently being managed in terms of which employee is responsible (assigned) for that equipment such as laptops.	Low

Criteria

CDM is consistent with and promotes carrying out these responsibilities. The statutory authority for CDM is as follows:

- Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551-3558) (FISMA) directs the Secretary of DHS, in consultation with the Director of Office of Management and Budget (OMB), to administer the implementation of agency information security policies and practices for information systems

- FISMA further authorizes DHS to, upon request by an agency, deploy, operate, and maintain technologies to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement. This specifically authorizes the CDM program.

Relevant policy directives that relate to CDM include, but are not limited to the following:

- OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003)[1];
- OMB Memorandum M-06-16: Protecton of Sensitive Agency Information

[1] Found at, https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/US_OMB/O030703F.pdf

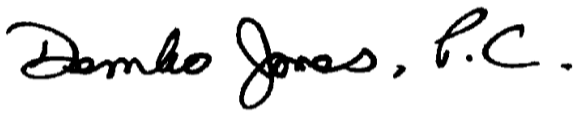
(June 23, 2006)[2];

- OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)[3];
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) – 12, Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011). The CDM Program will support visibility into agency HSPD-12 implementation of PIV access systems[4];
- OMB Memorandum M-14-03, Enhancing the Security of Federal Information and information Systems, (November 18, 2013)[5];
- OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices (October 3, 2014)[6]; and
- OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan for the Federal Civiliam Government (October 30, 2015)[7].

Recommendation

We recommend the Director of Information Resources:

1. All IT inventory items such as laptops, should be assigned to personnel within the agency.



Dembo Jones, P.C.

North Bethesda, Maryland
July 8, 2021

[2] Found at, http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-06-16.pdf
[3] Found at, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
[4] Found at, http://www.cac.mil/Portals/53/Documents/m-11-11.pdf
[5] Found at, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2014/m-14-03.pdf
[6] Found at, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-01.pdf
[7] Found at, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Appendix I: Objective, Scope, and Methodology

Our objective was to perform an IT asset inventory audit. We initiated our audit in April 2021 and performed the following steps in order to obtain an understanding and document a summary of the FLRA's IT asset inventory policies and procedures:

- Met with the Chief Information Officer and the Security Officer and documented the policies and procedures they use to order, track and dispose of IT assets;
- Reviewed all inventory policies and procedures.
- Performed a walkthrough from a sample of IT assets from the inventory listing to the IT assets located throughout the agency;
- Assessed overall access, authentication and password complexity to the software application used for maintaining IT assets;
- Reviewed position descriptions of selected personnel; and
- Assessed audit logs and the subsequent review to ensure that changes to inventory are complete and accurate.

Appendix II: Management Response

UNITED STATES OF AMERICA
FEDERAL LABOR RELATIONS AUTHORITY

2 July, 2021

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: Michael Jeffries
Executive Director

SUBJECT: Management Response to FY2021 Draft Report on the FLRA's IT Asset Inventory Program

FLRA sincerely appreciates the Inspector General's comprehensive look into the inventory practices within our Agency and the opportunity to review and provide comments on the draft report. In recent years, IRMD actively sought ways to improve the tools with which they monitor the lifecycle of all IT hardware/assets. These strides were reflected in the results of our prior audit. Most recently, though, IRMD has also updated the policies and procedures that govern the specific ways in which they use those tools and the ways in which they interact with other Agency components (e.g. ASD) in order to create a more foolproof and comprehensive system. FLRA is pleased that all previous findings reviewed remain closed and the asset inventory program is in outstanding operational status.

The report does contain one new finding, requiring FLRA to assign all unused equipment to an individual. FLRA recognizes that this finding aligns with OMB guidance, however FLRA does not feel this presents a significantly elevated security threat or that it elevates the possibility of loss or theft. Currently, *all* assets are tracked in the Agency's property inventory, and items without specific personnel assignment are assigned to the Information Resources Management Division, IRMD. These assets are physically secured and are controlled and dispensed by IRMD staff. FLRA agrees that, to more closely align with OMB guidance and to respond explicitly to the IG concern, IRMD will begin assigning all assets (to include the laptops identified) to individuals in the IT asset tracking system – and will modify Agency policies and procedures to reflect the update.

FLRA maintains an active commitment to keeping FLRA's IT assets safe and secure. Thank you to the Inspector General for their continued support and efforts to help FLRA ensure its programs are securely and cost effectively implemented.

Appendix III: Report Distribution

Federal Labor Relations Authority

Ernest DuBester, Chairman
Colleen Duffy Kiko, Member
James T. Abbott, Member
Michael Jeffries, Executive Director
Dave Fontaine, Director Information Resources

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

Information Technology Asset Inventory Review