



Office of Inspector General

Information Technology
Asset Inventory Review

**INFORMATION
TECHNOLOGY ASSET
INVENTORY REVIEW**

Report No. MAR-18-03

March 2018

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

CONTENTS

Management Advisory Report

Results in Brief	1
Background	1
Evaluation Results	2
Criteria	3
Recommendations	4

Appendices

Appendix I Objective, Scope, and Methodology	5
Appendix II Management Response	6
Appendix III Report Distribution	8

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
IP	Internet Protocol
IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information

Information Technology Asset Inventory Review

March 20, 2018

The Honorable Colleen Duffy Kiko, 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. IT asset inventory policies and procedures need to be updated, reviewed and approved. Maintenance of inventories not connected to the network (e.g. those items in storage or without an Internet Protocol (IP) address) need to be better managed. Position descriptions also need to be updated to ensure that personnel understand their job responsibilities. Lastly, auditing needs to be deployed to ensure that inventory additions, deletions and updates are managed appropriately.

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

We conducted our fieldwork in December 2017 to March 2018. Appendix I contains a detailed description of our objective, scope, and methodology. Appendix II 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 evaluation 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 that specific tools will be deployed thereby ensuring that all

hardware and software are accounted for. In preparation for the upcoming compliance with CDM, the FLRA contracted with Dembo Jones, P.C. to assess the current asset inventory in terms of its completeness and accuracy.

Evaluation Results

Our evaluation determined the FLRA's property management systems, policies, and processes are now strong. This year's review resulted in the five findings below:

#	Deficiency	Risk	Risk Ranking
1	Inventory procedures are not formally reviewed and updated. For example, the current inventory procedures don't currently address misclassified and/or inaccurate inventory. The inventory procedures also don't address asset transfers between employees.	Without reviewing and updating inventory procedures, there is the risk that the current policies will contain outdated or obsolete requirements, thereby leading to inventory listings being inaccurate and/or incomplete.	Medium
2	The current inventory procedures pertain only to assets in excess of \$3,500.	Many inventory assets are less than \$3,500 and there is the risk that equipment may have Personally Identifiable Information (PII) and become unaccounted for.	Medium
3	There are no periodic reviews of the audit logs detailing when inventory is added, removed or updated.	Without reviews of audit logs, there is no detective or corrective controls in place to identify when there are additions, deletions or modifications of inventory.	High
4	FLRA doesn't maintain a formal listing of excessed equipment or how the equipment was sanitized.	Without the appropriate documentation of when and how the inventory was excessed, there is the risk that PII will still be residing on the inventory, thereby exposing the agency to unforeseen risks.	Medium
5	The current inventory only includes those endpoints that are connected to the network and have an IP address only. Endpoints without an IP address or not connected to the network are not currently being tracked and maintained.	Inventory items without an IP address or not connected to the network may contain PII and if compromised will lead to a privacy violation for the agency.	Medium

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 (FISMA) (44 U.S.C. 3551-3558) 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: Protection of Sensitive Agency Information (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 Personal Identity Verification access systems⁴;
- 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 Civilian Government (October 30, 2015)⁷.

Recommendations

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

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>

We recommend the Director of Information Technology:

1. Review all inventory policies and procedures annually, and updates should be made if it is deemed appropriate.
2. Update inventory procedures to include all assets, which contain PII.
3. Review audit logs monthly and reconcile against all changes to inventory and the staff member who made the change.
4. Ensure that as inventory is excessed, the date of excess and method of sanitization are documented to ensure that PII is removed from the inventory appropriately.
5. Ensure all IT assets are accounted for and protected, whether or not they are connected to the network and/or contain an IP address.

Management's Response

FLRA management acknowledged all five findings and intends to take the corrective actions.

OIG Comment

Management's response meets the intent of our recommendations.

A handwritten signature in black ink that reads "Dembo Jones, P.C." with a period at the end.

Dembo Jones, P.C.

Rockville, Maryland
March 20, 2018

Appendix I: Objective, Scope, and Methodology

Our objective was to perform an IT asset inventory review. We initiated our review in December 2017 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

March 19, 2018

MEMORANDUM

TO: Dana Rooney
Inspector General

FROM: William Tosick 
Executive Director

SUBJECT: Response to the Inspector General's Management Letter Regarding the Fiscal Year 2018 audit of the Federal Labor Relations Authority (FLRA) Information Technology (IT) Asset Inventory

The purpose of this memorandum is to address the findings raised in the management letter pertaining to FLRA's Information Technology (IT) Asset Inventory. The findings are addressed separately below. As always, I look forward to working with your office as we continue to improve our operations and take steps to fully address the five open findings set forth below.

Finding: Inventory procedures are not formally reviewed and updated

Inventory procedures are not formally reviewed and updated. For example, the current inventory procedures don't currently address misclassified and/or inaccurate inventory. The inventory procedures also don't address asset transfers between employees.

Without reviewing and updating inventory procedures, there is the risk that the current policies will contain outdated or obsolete requirements, thereby leading to inventory listings being inaccurate and/or incomplete.

Management Response: FLRA Management acknowledges the finding and intends to take the corrective actions set forth below.

Corrective Action: FLRA will update their inventory procedures to address any outdated or obsolete requirements, addressing updating misclassified and/or inaccurate inventory, and tracking asset transfers between employees. Procedures will also include annual reviews with ad-hoc reviews when changes may warrant.

Finding: The current inventory procedures pertain only to assets in excess of \$3,500.

Many inventory assets are less than \$3,500 and there is the risk that equipment may have personally identifiable information (PII) and become unaccounted for.

Management Response: FLRA Management acknowledges the finding and intends to take the corrective actions set forth below.

Corrective Action: FLRA is currently tracking items valued less than \$3,500. Procedures will be updated to reflect the current process. This will be done as part of the inventory procedure review/update.

Finding: There are no periodic reviews of the audit logs detailing when inventory is added, removed or updated.

Without reviews of audit logs, there are no detective or corrective controls in place to identify when there are additions, deletions or modifications of inventory.

Management Response: FLRA Management acknowledges the finding and intends to take the corrective actions set forth below.

Corrective Action: As part of the inventory procedure review/update, processes will be added to review audit logs and provide corrective controls.

Finding: FLRA doesn't maintain a formal listing of excessed equipment or how the equipment was sanitized

Without the appropriate documentation of when and how the inventory was excessed, there is the risk that PII will still be residing on the inventory, thereby exposing the agency to unforeseen risks.

Management Response: FLRA Management acknowledges the finding and intends to take the corrective actions set forth below.

Corrective Action: FLRA currently maintains excess documentation. FLRA will formalize the existing process tracking all equipment excessed and if/how PII was sanitized. This will also be included with the updated inventory procedures.

Finding: The current inventory only includes those endpoints that are connected to the network and have an IP address only. Endpoints without an IP address or not connected to the network are not currently being tracked and maintained.

Inventory items without an IP address or not connected to the network may contain Personally Identifiable Information (PII) and if compromised will lead to a privacy violation for the agency.

Management Response: FLRA Management acknowledges the finding and intends to take the corrective actions set forth below.

Corrective Action: FLRA is working with DHS to implement Continuous Diagnostics Mitigation (CDM) and the tools necessary to track items without IP addresses.

Should you have any questions or concerns, then please do not hesitate to contact me.

2

Appendix III: Report Distribution

Federal Labor Relations Authority

The Honorable Ernest DuBester, Member

The Honorable James Abbott, Member

William Tosick, Executive Director

Michael Jeffries, Director, Information Technology

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](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