Evaluation of the U.S. Nuclear Regulatory Commission's Information Technology Asset Management

OIG-24-E-01

July 3, 2024

All publicly available OIG reports, including this report, are accessible through the OIG's website at: nrcoig.oversight.gov

MEMORANDUM

DATE: July 3, 2024

TO: Raymond V. Furstenau
Acting Executive Director for Operations

FROM: Hruta Virkar, CPA ***/RA/***
Assistant Inspector General for Audits & Evaluations

SUBJECT: EVALUATION OF THE U.S. NUCLEAR REGULATORY COMMISSION'S INFORMATION TECHNOLOGY ASSET MANAGEMENT (OIG-24-E-01)

Attached is the Office of the Inspector General's (OIG) evaluation report titled: *Evaluation of the U.S. Nuclear Regulatory Commission's Information Technology Asset Management.*

The report presents the results of the subject evaluation. Following the May 29, 2024, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions or comments about our report, please contact me at 301.415.1982 or Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: J. Martin, Acting ADO
M. Meyer, DADO
J. Jolicoeur, OEDO

Results in Brief

Evaluation of the U.S. Nuclear Regulatory Commission's Information Technology Asset Management

OIG-24-E-01
July 3,2024

Why We Did This Review

In December 2023, the Audits & Evaluations Division within the Office of the Inspector General (OIG) was referred a hotline complaint that stated (1) U.S. Nuclear Regulatory Commission (NRC) information technology (IT) assets were not returned upon employee separation from the NRC; (2) IT assets are not located in the locations that are shown in the Configuration Management Database located in the Information Technology Service Management (ITSM) toolset; (3) new IT assets are not being logged into the appropriate database; and, (4) decommissioning procedures were not followed for IT assets.

The evaluation objective was to determine the facts and circumstances regarding allegations of information technology asset mismanagement.

What We Found

The Office of the Inspector General (OIG) determined that U.S. Nuclear Regulatory Commission (NRC) information technology (IT) assets were not managed effectively throughout aspects of the IT lifecycle management process.

The OIG substantiated four allegations. The OIG found that some NRC assets were not returned upon employee separation from the NRC. Specifically, three employees separated from the NRC without returning four laptops. Additionally, NRC IT assets are not located in the locations that are shown in the configuration management database. The OIG found that 666 of 980 items were not in the locations assigned within the ITSM toolset. Further, new IT assets were not logged into the appropriate database for a period of 3 months. The OIG also found that NRC decommissioning procedures were not followed for IT assets.

What We Recommend

This report makes six recommendations to improve the NRC's information technology asset management program.

TABLE OF CONTENTS

APPENDIX

ABBREVIATIONS AND ACRONYMS

CMDB	Configuration Management Database
EDO	Executive Director for Operations
EUC	End-User Computing Services
IT	Information Technology
ITAM	Information Technology Asset Management
ITSM	Information Technology Service Management
NRC	U.S. Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
SIT	Systems Integration Task

I. BACKGROUND

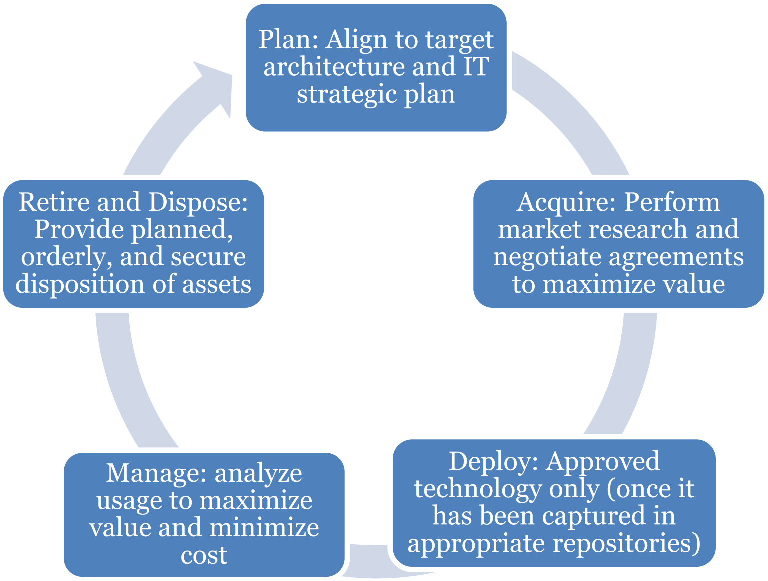
Information Technology Asset Management

Effective information technology asset management (ITAM) is essential for maintaining the integrity, security, and efficiency of the U.S. Nuclear Regulatory Commission's (NRC's) information technology (IT) infrastructure. ITAM comprises practices and strategies for overseeing, managing, and optimizing NRC-owned IT systems, hardware, software, and processes. The NRC has established an ITAM program to implement a systematic process that joins contractual, financial, inventory, and IT governance functions to support the management of IT assets throughout their lifecycles and the strategic decision-making for the IT environment at the NRC. Additionally, the NRC's *Hardware Asset Management (HAM) Playbook, Version 2.2,* describes the processes for the effective management of hardware assets and the reconciliation of asset records.

The IT Asset Lifecycle Stages

The NRC manages IT assets throughout five lifecycle stages (i.e., planning, acquisition, deployment, management, and retirement and disposal) in a centralized IT asset repository that accounts for the presence and purchase of all hardware and software. Figure 1 describes the five IT asset lifecycle stages.

Figure 1: IT Asset Lifecycle Management Process


Plan: Align to target architecture and IT strategic plan
Acquire: Perform market research and negotiate agreements to maximize value
Deploy: Approved technology only (once it has been captured in appropriate repositories)
Manage: analyze usage to maximize value and minimize cost
Retire and Dispose: Provide planned, orderly, and secure disposition of assets

Source: NRC ITAM Policy

The agency migrated the configuration management database (CMDB)[1] information, including IT asset location information, to a new IT service management platform in July 2023.

Property Management and Tagging

The Office of the Chief Information Officer (OCIO) manages the ITSM toolset, maintaining records of all IT assets (i.e., laptops, monitors, printers, computers, and other IT peripherals) as needed, regardless of acquisition cost. The NRC uniquely identifies its IT assets with tags to properly track them in their appropriate systems. The NRC uses blue tags for assets with an acquisition cost of $2,500 or greater and red tags for IT assets with an acquisition cost of less than $2,500.

Asset Oversight

Office of the Chief Information Officer

The OCIO plans, directs, and oversees IT resources to ensure the delivery of IT services that are critical to support the agency's mission, goals, and priorities. Specifically, the Service Fulfillment and Delivery Branch is responsible for establishing, managing, and maintaining agency ITAM, and providing a comprehensive IT asset and CMDB service. The OCIO also oversees the contractors for its ITAM contracts.

ITAM Contracts

Two contractors, a Systems Integration Task (SIT) contractor and an End User Computing Services (EUC) contractor, provide support for the IT asset lifecycle. Both contractors utilize the NRC's CMDB to manage the NRC's IT assets. The SIT contractor enters new assets into the CMDB, while the EUC contractor maintains the current status of the IT asset during its full lifecycle.

The SIT contractor supports the short-term storage of devices prior to re-imaging, distribution of devices, and moving devices between the NRC warehouse and NRC headquarters. The EUC contractor provides deskside support for IT asset deployment, receives assets from the SIT contractor, and is responsible for setting up the asset for the end-user. The EUC contractor also

[1] A CMDB is a centralized file that functions as a comprehensive data warehouse, organizing information about an IT environment. The CMDB clarifies the relationships between hardware, software components, and networks for improved configuration management.

returns IT assets back to the SIT contractor once the user no longer needs the asset for reimaging or decommissioning and disposal.

Office of Administration

The Office of Administration establishes the guidance for the receipt and tagging of newly acquired property and distributes red and blue tags, based on the acquisition cost, to designated property custodians. The Office of Administration is tangentially involved in the IT asset lifecycle management process, receiving newly acquired IT assets at the NRC's warehouse, issuing tags to the OCIO to properly track its assets in the ITSM toolset, and disposing of IT assets at their end of life at the OCIO's request.

Allegation Summary

In December 2023, the Audits & Evaluations Division within the Office of the Inspector General (OIG) was referred a hotline complaint that stated: (1) NRC information technology assets were not returned upon employee separation from the NRC; (2) IT assets are not located in the locations that are shown in the CMDB located in the ITSM toolset; (3) new IT assets are not being logged into the appropriate database; and, (4) decommissioning procedures were not followed for IT assets.

II. OBJECTIVE

The evaluation objective was to determine the facts and circumstances regarding allegations of information technology asset mismanagement.

III. FINDINGS

The OIG determined that the NRC's IT assets were not managed effectively throughout the IT lifecycle management process.

1. NRC Assets Were Not Returned upon Employee Separation from the NRC

The OIG substantiated the allegation that some NRC assets were not returned upon employee separation from the NRC. Specifically, the OIG obtained a list of all employees who separated from NRC headquarters in calendar year 2023. The list showed 133 employee separations in 2023. Of those 133, the OIG found 12 former employees who were still assigned laptops within the CMDB in the ITSM toolset. The OIG sent a list to the NRC to determine the location and status of the assets. Based on the agency's response, the OIG found three employees left NRC employment without returning four laptops. NRC staff stated that one individual possesses two laptops and was sent return boxes for the items, but the individual has not returned the items. NRC staff also stated they were unable to reach the two other separated employees.

The OIG determined that this issue occurred because the NRC's separation process does not include a step to ensure IT assets are returned to the NRC prior to the employee receiving separation clearance. Specifically, NRC form 270, *Separation Clearance,* does not include a step to verify that IT assets under $2,500 are returned. In addition, Management Directive 13.1, *Property Management,* is unclear regarding who is responsible for ensuring the return of items below the $2,500 threshold. The OIG determined that the NRC has not clearly defined who bears responsibility to ensure that IT assets under the $2,500 threshold are returned to the NRC prior to an employee's separation. The former employees' failure to return laptops prevented the NRC from reissuing those laptops or potentially putting them to other use.

Recommendations

The OIG recommends that the Executive Director for Operations (EDO):

1.1. Update NRC form 270, *Separation Clearance,* to include a step to ensure IT assets under the $2,500 threshold are returned prior to employee clearance for separation; and,

1.2. Update MD 13.1, *Property Management,* or develop other guidance, to clearly describe the roles and responsibilities of NRC employees and contractors as they pertain to the handling, storage, issuance, and return of IT assets under the $2,500 threshold.

2. NRC IT Assets Are Not Located in the Locations that Are Shown in the CMDB Located in the ITSM Toolset

The OIG substantiated the allegation that NRC IT assets are not located in the locations shown in the CMDB located in the ITSM toolset. The OIG reviewed the storage locations for IT assets within the ITSM toolset and noted that there were eight storage locations consisting of seven rooms within NRC headquarters and the NRC warehouse. The OIG selected a judgmental sample that included all laptops, desktops, and tablets in all eight locations to verify their existence in the locations listed in the ITSM toolset. The OIG found that 666 of 980 items were not in the location assigned within the ITSM toolset.[2] In addition, the OIG found 149 items physically present in rooms for which the assets were not on the inventory lists.

The OIG determined these issues occurred due to failure to ensure proper contract management oversight. Specifically, the NRC did not ensure that the contractor performed the following requirements:

- Developed and applied stringent inventory measures to ensure accuracy and reduce risk of inventory discrepancies;
- Maintained and operated the NRC's Logistics Management Center, to include, but not limited to, the full lifecycle management of all IT

[2] The OIG substantiated the allegation that the IT assets were not stored in their designated locations; however, the OIG did not determine if the assets were in other NRC locations or assigned to users.

assets, including development of procedures to ensure all assets are accounted for during all stages of lifecycle management;

- Ensured asset management documents remain current and located on a designated, centralized site;
- Populated, reconciled, and maintained all hardware/software IT asset data in the CMDB and ensure accuracy of configuration information; and,
- Performed periodic inventory scans to ensure the accuracy of the CMDB.

NRC staff stated that the accuracy of the CMDB data has been an issue since 2017, when the management of IT assets was transferred from a previous contractor to the NRC. NRC staff stated that the issue was exacerbated by the information migration to the new ITSM toolset. While the OIG acknowledges the challenge that NRC officials noted regarding having unreliable CMDB data since 2017, sufficient steps were not taken to correct the issues from February 2022, when the current contracts governing the lifecycle process were awarded, to July 2023, when the transition to a new ITSM toolset occurred. These issues prevented the NRC from better understanding and managing its IT asset environment, rightsizing the IT inventory, and optimizing inventory purchase decisions and strategies.

Recommendation

The OIG recommends that the EDO:

2.1. Complete an inventory of laptops, desktops, and tablets, and update the information in the CMBD in the current ITSM toolset.

3. New IT Assets Are Not Being Logged into the Appropriate Database

The OIG substantiated the allegation that new IT assets are not being logged into the appropriate database. The OIG conducted a walkthrough of the NRC warehouse to determine if new assets in the warehouse were being tracked in the ITSM toolset. The OIG observed that there were 16 pallets of 24 laptops each (384 total laptops) that had not been tagged. Consequently, they were not entered into the CMDB within the ITSM toolset for a period of 3 months. The OIG noted that over 1,700 red tags were requested for IT assets that arrived within an approximate 1-month period. The OIG found that the

NRC's Office of Administration is responsible for issuing red tags for assets under the $2,500 threshold when requested; however, the office was unable to fulfill the request due to a lack of tags.

The OIG determined that these issues occurred due to the absence of expressly stated roles and responsibilities and clearly defined policies and procedures. Specifically, the governing documents do not clearly define the roles, responsibilities, or process for the acquisition of IT assets, nor do they expressly state the process for obtaining red tags for IT Assets under the $2,500 threshold. These issues prevent the NRC from better understanding and managing its IT asset environment.

Recommendation

The OIG recommends that the EDO:

3.1 Update MD 13.1, *Property Management,* and the *Hardware Asset Management Playbook*, or develop other guidance, to expressly state the roles and responsibilities for acquiring assets and requesting red tags for IT assets in a timely manner.

4. NRC Decommissioning Procedures Were Not Followed for IT Assets

The OIG substantiated the allegation that NRC decommissioning procedures were not followed for IT assets. The OIG found that over 1,500 IT assets were stored in headquarters awaiting disposal. Some assets have been stalled in the disposal process since 2022.

The OIG determined that these issues occurred because the EUC contractor's performance-based statement of work does not include a service level requirement that covers the sanitation of hardware. The OIG also determined that the contract documentation was not written in a manner that ensured the contracting officer's representative would or should monitor the contractor to ensure they were performing sanitation services in a timely and sufficient manner. In addition, the OIG reviewed the PC Decommissioning (Wipe) Standard Operating Procedure and noted that the sanitization sticker "received" date does not require it to be filled in. Further, it appears that an extra step, not documented in the standard operating procedures, was inserted into the decommissioning process to verify the sanitation of assets was complete prior to the release of the assets to the Office of Administration.

The additional step made it unclear who was responsible for the assets, causing the assets to accumulate.

These issues led to the NRC paying approximately $37,000, funds which could be put to better use, for an excess of software licenses installed on unused IT hardware due to maintaining assets waiting for disposal. In addition, due to space limitations in NRC headquarters, the contractor was unable to move new IT assets from the warehouse.

Recommendations

The OIG recommends that the EDO:

4.1 Update the affected contract(s) to include a service level requirement for the sanitation of assets; and,

4.2 Update the PC Decommissioning Standard Operating Procedure and the Hardware Asset Management Playbook to reflect all the required steps in the decommissioning and disposal process.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

The OIG recommends that the Executive Director for Operations:

1.1 Update NRC form 270, *Separation Clearance,* to include a step to ensure IT assets under the $2,500 threshold are returned prior to employee clearance for separation;

1.2 Update MD 13.1, *Property Management,* or develop other guidance, to clearly describe the roles and responsibilities of NRC employees and contractors as it pertains to the handling, storage, issuance, and return of IT assets under the $2,500 threshold;

2.1 Complete an inventory of laptops, desktops, and tablets, and update the information in the CMBD in the current ITSM toolset;

3.1 Update MD 13.1, *Property Management,* and the Hardware Asset Management Playbook, or develop other guidance, to expressly state the roles and responsibilities for acquiring assets and requesting red tags for IT assets in a timely manner;

4.1 Update the affected contract(s) to include a service level requirement for the sanitation of assets; and,

4.2 Update the PC Decommissioning Standard Operating Procedure and the Hardware Asset Management Playbook to reflect all the required steps in the decommissioning and disposal process.

V. NRC COMMENTS

The OIG held an exit conference with the agency on May 29, 2024. Before the exit conference, agency management reviewed and provided comments on the discussion draft version of this report, and the OIG discussed these comments with the agency during the conference. Following the conference, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide additional comments. The OIG has incorporated the agency's comments into this report, as appropriate.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The evaluation objective was to determine the facts and circumstances regarding allegations of information technology asset mismanagement.

Scope

This evaluation focused on records and inventory from July 2023 to present, current NRC policies and practices, and the IT asset management lifecycle. We conducted this evaluation at NRC headquarters in Rockville, Maryland from January 2024 to April 2024.

Methodology

The OIG reviewed relevant criteria for this evaluation, including, but not limited to:

- Management Directive 13.1, *Property Management;*
- Information Technology Asset Management Policy;
- Hardware Asset Management (HAM) Playbook;
- NRC Form 270, *Separation Clearance;*
- NRC Form 747, *Equipment Data Sheet*;
- PC Decommissioning Standard Operating Procedure for NRC GLINDA End User Contractors;
- Systems Integration Task contract documents; and,
- End User Computing Services contract documents.

The OIG interviewed contracting officer's representatives, Office of Administration personnel, and Office of the Chief Information Officer personnel. In addition, the OIG conducted physical inventories of the NRC's IT assets using data from the ITSM tool. The OIG also conducted analysis of inventories provided by the contractors.

The OIG conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. The OIG believes that the evidence obtained provides a reasonable basis for our findings and conclusions based on the evaluation objective. Throughout the evaluation, auditors considered the possibility of fraud, waste, and abuse in the program.

The evaluation was conducted by Mike Blair, Team Leader; Diane Parker, Audit Manager; Janelle Davis, Senior Auditor; and, Lawrence Heller, Auditor.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Online:	Hotline Form
Telephone:	1.800.233.3497
TTY/TDD:	7-1-1, or 1.800.201.7165

Address:

U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O12-A12
11555 Rockville Pike
Rockville, Maryland 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email the OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.

NOTICE TO NON-GOVERNMENTAL ORGANIZATIONS AND BUSINESS ENTITIES SPECIFICALLY MENTIONED IN THIS REPORT

Section 5274 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, amended the Inspector General Act of 1978 to require OIGs to notify certain entities of OIG reports. In particular, section 5274 requires that, if an OIG specifically identifies any non-governmental organization (NGO) or business entity (BE) in an audit or other non-investigative report, the OIG must notify the NGO or BE that it has 30 days from the date of the report's publication to review the report and, if it chooses, submit a written response that clarifies or provides additional context for each instance within the report in which the NGO or BE is specifically identified.

If you are an NGO or BE that has been specifically identified in this report and you believe you have not been otherwise notified of the report's availability, please be aware that under section 5274 such an NGO or BE may provide a written response to this report no later than 30 days from the report's publication date. Any response you provide will be appended to the published report as it appears on our public website, assuming your response is within the scope of section 5274. Please note, however, that the OIG may decline to append to the report any response, or portion of a response, that goes beyond the scope of the response provided for by section 5274. Additionally, the OIG will review each response to determine whether it should be redacted in accordance with applicable laws, rules, and policies before we post the response to our public website.

Please send any response via email using this link. Questions regarding the opportunity to respond should also be directed to this same address.