



MEMORANDUM

DATE: March 13, 2024

TO: Raymond V. Furstenau
Acting Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023, REGION I: KING OF PRUSSIA, PENNSYLVANIA (OIG-24-A-03)

REFERENCE: CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM DATED FEBRUARY 16, 2024.

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations as discussed in the agency's response dated February 9, 2024. Based on this response, recommendations 2 and 4 are closed. Based on this response, recommendations 1 and 3 remain open and resolved. Please provide an updated status of the open, resolved recommendations by July 19, 2024.

If you have any questions or concerns, please call me at 301.415.1982 or Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: J. Martin, Acting ADO
T. Govan, DADO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO ACS Distribution

**AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
REGION I: KING OF PRUSSIA, PENNSYLVANIA
Status of Recommendations
(OIG-24-A-03)**

Recommendation 1:

We recommend NRC management implement a process to validate that all new users complete their initial security training requirements and acknowledgement of rules of behavior within the defined timeframes NRC has established.

Agency Response Dated
February 9, 2024:

The U.S. Nuclear Regulatory Commission (NRC) is in the process of completing an enterprise-wide change that will ensure all new users have electronic access to the required training upon onboarding. In the interim, Region I will provide new users with a copy of the applicable training material and the Rules of Behavior and will instruct the individuals to read and acknowledge the material within 7 days. Upon receipt of acknowledgement, Region I will send confirmation to Talent Management System (TMS) Resource Support and request that the individuals be marked as having completed the required cybersecurity training. Region I will further instruct each new user, upon onboarding, to complete the remaining required training within 7 days of being granted access to the TMS.

Additionally, Region I will regularly remind staff of the importance of reviewing existing management directives and other guidance documents to ensure an explicit understanding of, and compliance with, such policies.

Region I has shared the lessons learned from this audit with other regional offices and the Technical Training Center (TTC) for their awareness and appropriate action.

Target Completion Date: Fiscal Year (FY) 2024,
Third Quarter (Q) 3

**AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
REGION I: KING OF PRUSSIA, PENNSYLVANIA
Status of Recommendations
(OIG-24-A-03)**

Recommendation 1 (continued):

OIG Analysis: The OIG will close this recommendation after confirming that NRC management has implemented a process to validate that all new users complete their initial security training requirements and acknowledgement of rules of behavior within the defined timeframes that the NRC has established.

Status: Open: Resolved.

**AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
REGION I: KING OF PRUSSIA, PENNSYLVANIA
Status of Recommendations
(OIG-24-A-03)**

Recommendation 2: We recommend NRC management define and implement a process to notify appropriate members of personnel security of separations at the Region I facility.

Agency Response Dated
February 9, 2024:

The processes for managing network account access are centralized in the Office of the Chief Information Officer (OCIO), and individual offices and regions do not have the authorization or ability to disable network accounts. However, in parallel with the agency's out-processing notification process initiated through Form 270 by the Office of the Chief Human Capital Officer, Region I will notify the agency's IT systems account managers when accounts are no longer required, terminated, or transferred and when system usage or need-to-know changes for an individual.

Management has shared the lessons learned from this audit with other regional offices and the TTC for their awareness and appropriate action.

Target Completion Date: The NRC recommends closure of this item.

OIG Analysis:

The OIG reviewed the evidence and confirmed that the NRC management has defined and implemented a process to notify appropriate members of personnel security of separations at the Region I facility by initiating the notification process through form 270 by the Office of the Chief Human Capital Officer. The OIG has also reviewed the evidence that demonstrates that the management has shared the lessons learned from this audit with other regional offices and the TTC for their awareness and appropriate action. Hence, this recommendation is closed.

Status: Closed.

**AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
REGION I: KING OF PRUSSIA, PENNSYLVANIA
Status of Recommendations
(OIG-24-A-03)**

Recommendation 3: We recommend NRC management define and implement a process to conduct reviews and removal of unnecessary badged access for its Regions.

Agency Response Dated
February 9, 2024:

Region I will regularly review the badge access list detailing authorized facility access by individuals and will remove individuals from the facility access list when their access is no longer required (using the regional action item tracking system to monitor review dates). In addition, the Office of Administration, Security Management and Operations Branch, and OCIO will define and implement a review process to remove unnecessary badged access, with input from regional offices and the TTC, as appropriate.

In accordance with agency policy, Region I deactivates and also requires NRC employees to return their identification badges upon leaving agency employment.

Region I has shared the lessons learned from this audit with other regional offices and the TTC for their awareness and appropriate action.

Target Completion Date: FY 2024, Q 4

OIG Analysis: The OIG will close this recommendation after confirming that NRC management has defined and implemented a process to conduct reviews and removal of unnecessary badged access for its Regions.

Status: Open: Resolved.

**AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S
IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY
MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2023
REGION I: KING OF PRUSSIA, PENNSYLVANIA
Status of Recommendations
(OIG-24-A-03)**

Recommendation 4: We recommend NRC management remediate identified vulnerabilities in accordance with NRC's defined timeframes and document risk acceptances with mitigating controls for vulnerabilities that cannot be remediated within the defined timeframes.

Agency Response Dated
February 9, 2024:

Region I has reviewed and remediated where feasible the identified critical and high vulnerabilities. For critical and high vulnerabilities that could not be remediated, Region I has completed all required documentation. In the future, Region I will continue to work with the agency's cybersecurity team and create regional action items to track completion of remediation and documentation of all critical and high vulnerabilities through to completion.

Region I has shared the lessons learned from this audit with other regional offices and the TTC for their awareness and appropriate action.

Target Completion Date: The NRC recommends closure of this item.

OIG Analysis:

The OIG reviewed the evidence and confirmed that the NRC management has remediated identified vulnerabilities in accordance with NRC's defined timeframes and documented risk acceptances with mitigating controls for vulnerabilities that cannot be remediated within the defined timeframes. The OIG also confirmed that Region I has shared the lessons learned from this audit with other regional offices and the TTC for their awareness and appropriate action. Based on the evidence provided, the OIG closes this recommendation.

Status:

Closed.