MEMORANDUM

DATE: October 11, 2024

TO: Mirela Gavrilas
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021 (OIG-22-A-04)

REFERENCE: CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM DATED AUGUST 23, 2024

Attached is the Office of the Inspector General's (OIG) analysis and status of the recommendations discussed in the agency's response dated August 23, 2024. Recommendations 1-5, 9, 10, 12, and 15 were previously closed and have been removed from the list. Recommendations 14, 16, 17, and 18 were closed in the audit titled *Performance Audit of The U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024* (OIG-24-A-11) issued on September 30, 2024. Based on this response, recommendation 6 is now closed. Recommendations 7, 8, 11, and 13 remain open and resolved. Please provide an updated status of the open, resolved recommendations by April 30, 2025.

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, ADO
M. Meyer, DADO
S. Miotla, DADO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO ACS Distribution

Recommendation 6: Document and implement policies and procedures for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third party providers.

Agency Response Dated
August 22, 2024: The U.S. Nuclear Regulatory Commission (NRC) has implemented policies and procedures for prioritizing externally provided systems and services documented in CSO-PROS-0008, "Process to Assess, Respond, and Monitor ICT Supply Chain Risks," dated August 1, 2023. Specifically, appendix B documents the criteria for prioritizing supply chain risk assessments for information communication technology (ICT) products and services.

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

OIG Analysis: The OIG reviewed the evidence and confirmed that the agency has documented and implemented policies and procedures for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third-party providers.

Status: Closed

Recommendation 7: Implement processes for continuous monitoring and scanning of counterfeit components to include configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

Agency Response Dated August 22, 2024: The tools and technologies required for automated scanning and detection of counterfeit information technology (IT) assets in the NRC's environment are not yet available. However, in April 2021, the NRC developed CSO-PROS-0006, "Counterfeit and Compromised ICT Product Detection Process," to ensure that counterfeit products are detected before they are added to the NRC's environment. In addition, Section 6, "After Acceptance," of CSO-PROS-0006 outlines the requirement for automated scanning and detection and will be updated when the associated tools and technologies are available industrywide. In the rare instances when physical IT components are awaiting repair, those components are maintained and managed in NRC-controlled physical space. The appropriate NRC staff members generally vet any third-party service personnel and replacement parts. The NRC will update CSO-PROS 0006 to include the vetting of third-party service personnel and replacement parts to detect counterfeit parts and other components and prevent them from being added to its environment.

Target Completion Date: FY 2025, first quarter (Q1)

OIG Analysis: The OIG will close this recommendation after confirming that the NRC has implemented processes for continuous monitoring and scanning of counterfeit components to include configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

Status: Open: Resolved

Recommendation 8: Develop and implement role-based training with those who hold supply chain risk management roles and responsibilities to detect counterfeit system components.

Agency Response Dated August 22, 2024: Pursuant to the Supply Chain Security Training Act of 2021 (Public Law 117-145), the General Services Administration is required to develop training for Federal officials with supply chain management responsibilities. The NRC will leverage this training for role holders, which will be implemented by the Office of Management and Budget, when it becomes available. Additionally, in April 2021, the NRC developed CSO-PROS-0006, aimed at those who hold supply chain risk management roles and responsibilities to ensure that counterfeit products are detected before being added to the NRC's environment.

Target Completion Date: FY 2025, Q3

OIG Analysis: The OIG will close this recommendation after confirming that the NRC has developed and implemented role-based training with those who hold supply chain risk management roles and responsibilities to detect counterfeit system components.

Status: Open: Resolved

Evaluation Report
INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(OIG-22-A-04)

Recommendation 11: Update user system access control procedures to include the requirement for individuals to complete a non-disclosure and rules of behavior agreements prior to the individual being granted access to NRC systems and information.

Agency Response Dated August 22, 2024: The NRC will update its onboarding procedures to require individuals to complete a nondisclosure agreement before they are granted access to the agency's systems and information. The clearance waiver process is wholly contained within the NRC's onboarding process and will inherit the updated procedures. The updated procedures will apply to all individuals who will be granted NRC network access after receiving an IT-1, IT-2, L, or Q clearance. Individuals granted building access clearances will not be included because they are not granted access to the NRC network. The nondisclosure agreement will be an updated version of the NRC's Form 176A, "Security Acknowledgment." Because of the estimated time needed to obtain an Office of Management and Budget clearance for these changes to Form 176A.

Target Completion Date: FY 2025, Q3

OIG Analysis: The OIG will close this recommendation after confirming that the NRC has updated user system access control procedures to include the requirement for individuals to complete a non-disclosure and rules of behavior agreements prior to the individual being granted access to NRC systems and information.

Status: Open: Resolved

Recommendation 13: Implement the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training as applicable or implement the technical capability to capture NRC employees and contractor's initial login date so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process in place.

Agency Response Dated
August 22, 2024: The NRC will implement a technical capability to capture NRC employees' and contractor personnel initial login dates or equivalent so that the process currently in place can accurately track and manage the required cybersecurity awareness and role-based training.

Target Completion Date: FY 2025, Q3

OIG Analysis: The OIG will close this recommendation after confirming that the NRC has implemented the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training as applicable or implement the technical capability to capture NRC employees and contractor's initial login date so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process in place.

Status: Open: Resolved

Recommendation 14: Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.

Agency Response Dated
August 22, 2024: The NRC will implement the technical capability or an equivalent method to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.

Target Completion Date: FY 2025, Q3

OIG Analysis: This recommendation is closed based on fieldwork performed during the Performance Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024. Refer to Recommendation Closure memorandum associated with the OIG-24-A-11 report.

Status: Closed

Evaluation Report
INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021
Status of Recommendations
(OIG-22-A-04)

Recommendation 16: Conduct an organizational level business impact assessment (BIA) to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

Agency Response Dated August 22, 2024: The NRC conducted an organizational-level BIA; determined contingency planning requirements and priorities, including for mission-essential functions and high-value assets; and updated contingency planning policies and procedures accordingly.

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

OIG Analysis: This recommendation is closed based on fieldwork performed during the Performance Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024. Refer to Recommendation Closure memorandum associated with the OIG-24-A-11 report.

Status: Closed

Recommendation 17:

Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.

Agency Response Dated August 22, 2024:

The NRC will integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.

Target Completion Date: FY 2025, Q4

OIG Analysis:

This recommendation is closed based on fieldwork performed during the Performance Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024. Refer to Recommendation Closure memorandum associated with the OIG-24-A-11 report.

Status: Closed

Recommendation 18: Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.

Agency Response Dated August 22, 2024: The NRC's current contingency plan testing approach is designed to coordinate contingency plan testing with ICT supply chain providers.

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

OIG Analysis: This recommendation is closed based on fieldwork performed during the Performance Audit of the U.S. Nuclear Regulatory Commission's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024. Refer to Recommendation Closure memorandum associated with the OIG-24-A-11 report.

Status: Closed