MEMORANDUM

DATE: May 23, 2023

TO: Daniel H. Dorman
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 (OIG-21-A-05)

REFERENCE: CHIEF INFORMATION OFFICER MEMORANDUM DATED APRIL 4, 2023

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated April 4, 2023. Based on this response, recommendations 2(c)-2(e), 5, 6, 8, and 10-13 remain in open and resolved status. Recommendations 2(a), 4, and 7 are now closed. Recommendations 1, 2(b), 2(f), 3, and 9 were previously closed. Please provide an updated status of the open and resolved recommendations by November 30, 2023.

If you have any questions or concerns, please call me at 301.415.1982 or Terri Cooper, Team Leader, at 301.415.5965.

Attachment:
As stated

cc: M. Bailey, OEDO
J. Jolicoeur, OEDO
M. Meyer, OEDO
RidsEdoMailCenter Resource
OIG Liaison Resource
EDO_ACS Distribution

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 2(a):	Assess enterprise, business process, and information system level risks.
Agency Response Dated April 4, 2023:	The U.S. Nuclear Regulatory Commission (NRC) completed its assessment of its risks at the enterprise, business process, and information system levels. This assessment was executed in conjunction with the NRC's recent conversion from a three-tier to a five-tier risk model. Target Completion Date: Completed
OIG Analysis:	The OIG reviewed the NRC's Information Security Architecture (ISA) and determined the NRC has assessed enterprise, business process, and information system risk. This recommendation is therefore closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 2(c):	If necessary, update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
Agency Response Dated April 4, 2023:	The NRC has transitioned all of its information systems to National Institute of Standards and Technology SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," issued September 2020, except for Office of Nuclear Security and Incident Response Federal Information Security Modernization Act of 2014 (FISMA) systems. The transition of these systems to Revision 5 is expected to be funded in the third quarter (Q3) of fiscal year (FY) 2023. Therefore, the NRC is requesting a new Target Completion date of FY2024, Q1. Target Completion Date: FY 2024, Q1
OIG Analysis:	The proposed action meets the intent of the recommendation. The OIG will close the recommendation when the NRC updates enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions, if necessary.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 2(d):	Conduct an organization wide security and privacy risk assessment and implement a process to capture lessons learned and update risk management policies, procedures, and strategies.
Agency Response Dated April 4, 2023:	The NRC recently implemented a 3-year cycle for the risk assessment of its information security architecture, which includes both security and privacy. Year 1 of the assessment cycle focuses on the Identify Function. Year 2 focuses on the Protect and Detect Functions. Year 3 focuses on the Respond and Recover Functions. The NRC is currently in year 2 of the cycle and expects to complete year 3 by the fourth quarter (Q4) of FY 2024. Throughout the 3-year risk assessment cycle, the NRC will follow its process to capture lessons learned and, where needed, update its risk management policies, procedures, and strategies. Target Completion Date: FY 2024, Q4
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC conducts an organization-wide security and privacy risk assessment and implements a process to capture lessons learned and update risk management policies, procedures, and strategies.
Status:	Open: Resolved.

Recommendation 2(e):	Consistently assess the critically of POA&Ms to support why a POA&M is or is not of a high or moderate impact to the Confidentiality, Integrity and Availability (CIA) of the information system, data, and mission.
Agency Response Dated April 4, 2023:	The NRC consistently assesses the criticality of Plans of Action and Milestones (POA&Ms) by ensuring that information systems security officers and assessors adhere to CSO-PROS-2030, "NRC Risk Management Framework (RMF) Process," specifically step 5. CSO-PROS-2030 further prescribes that assessors follow CSO-PROS-2102, "System Cybersecurity Assessment Process," when performing security assessments. Additionally, CSO-STD-0020, "System Security and Privacy Controls Standard," prescribes the organizationally defined frequency by which all such testing is performed. Finally, the Risk and Continuous Authorization Tracking System (RCATS) employs a POA&M management component that requires all POA&Ms to be assigned a criticality (severity) at the time of creation. To date, 13 out of 15 FISMA systems have been migrated to RCATS. The NRC expects to migrate the remaining two systems to RCATS by FY 2023, Q3. Target Completion Date: The NRC recommends closure of this item.
OIG Analysis:	The NRC and OIG met to discuss this recommendation and the action necessary for closure. The OIG will close this recommendation when the NRC consistently assesses the criticality of POA&Ms.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 4:	Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all the NRC systems (findings noted in bullets 1, 3, and 4 above) by continuing efforts to implement these capabilities using the Splunk QAudit, Sailpoint, and Cyberark automated tools.
Agency Response Dated April 4, 2023:	The NRC implemented a workflow-based privileged account review process in October 2021 within its Enterprise Identity Hub platform. In part because of the efficiency and ease of use of the tool, the NRC was able to increase the review frequency from annual to biannual. The NRC's Splunk QAudit provides centralized audit log monitoring. PIV login and other strong authentication are managed by the NRC's Identity, Credential, and Access Management (ICAM) program using a combination of identity platforms, including Microsoft Active Directory, ICAM Authentication Gateway (based on Microsoft's Active Directory Federation Services software), ICAM Enterprise Identity Hub (based on SailPoint Identity IQ software), and most recently a privileged account management platform (based on CyberArk software). This recommendation was carried over to recommendation 10 in OIG-22-A-04, "Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2021," dated December 20, 2021. On January 11, 2023, the NRC provided the above response to OIG-22-A-04 recommendation 10, which resulted in the closure of that recommendation. Based on the above response, the NRC requests that this recommendation also be closed. Target Completion Date: The NRC recommends closure of this item.

Recommendation 4 (continued):

OIG Analysis:	The OIG met with OCIO to view the centralized system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems. Therefore, this recommendation is now considered closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 5:	Update user system access control procedures to include the requirement for individuals to complete a non-disclosure agreement as part of the clearance waiver process prior to the individual being granted access to the NRC systems and information. Also, incorporate the requirement for contractors and employees to complete non-disclosure agreements as part of the agency's on-boarding procedures prior to these individuals being granted access to the NRC's systems and information.
Agency Response Dated April 4, 2023:	The NRC will update its onboarding procedures to require individuals to complete a nondisclosure agreement before they are granted access to the NRC'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, the NRC is recommending a new target completion date of FY 2024, Q3. Target Completion Date: FY 2024, Q3
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC updates the user system access control procedures.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 6:	Continue efforts to identify individuals having additional responsibilities for PII or activities involving PII and develop role-based privacy training for them to be completed annually.
Agency Response Dated April 4, 2023:	The NRC will conduct an in-depth, independent assessment of the Privacy Program, which will cover roles and training gaps. Using the results of the assessment, the NRC will update and develop annual role-based privacy training to address the identified gaps. The NRC will begin the assessment in Q3 of FY 2023, with completion planned by the first quarter (Q1) of FY 2024. The agency plans to complete the associated training development and implementation by FY 2025, Q1. Target Completion Date: FY 2025, Q1
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC identifies individuals having additional responsibilities for PII or activities involving PII and develops role-based privacy training for them to complete annually.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 7:	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.
Agency Response Dated April 4, 2023:	The creation of a separate, secure system to perform this security awareness and role-based training activity is not deemed cost effective since it would require the duplication of existing hardware, software, and support services and it would redirect staff from other network operations and maintenance tasks that could cause security and operational issues to the main network and reduce the NRC's ability to provide mission-focused services. The NRC estimates that this would increase costs across the Information Technology/Information Management Business Line, including hardware, software, operational maintenance, and NRC staff and contractual support resources, by nearly $1 million annually. In addition, this estimated cost does not include any changes that would be required by the Office of the Chief Human Capital Officer for its training system or resources. Instead, the NRC plans to add streamlined security training that does not contain sensitive information to its onboarding process, which occurs before employees gain access to the NRC network. The NRC will also strengthen its post-onboarding process to ensure that new employees complete all required security awareness and role-based training within the required timeframe. These changes, with the personnel security processing that occurs prior to onboarding make this a low risk to NRC systems. Based on this analysis, the NRC requests that this recommendation be closed. Target Completion Date: The NRC recommends closure of this item.

Recommendation 7 (continued):

OIG Analysis:	The OIG reviewed the streamlined training, and that the NRC provides the training before access to the NRC network is given. This recommendation is therefore closed.
Status:	Closed.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 8:	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 April 4, 2023:	The Office of the Chief Information Officer (OCIO) will analyze the agency's security awareness and role-based training records to better inform its response to this recommendation. OCIO staff will also consult with stakeholders such as the Office of the Chief Human Capital Officer and the National Treasury Employees Union to develop a specific, risk-based solution to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role based security training. To perform this analysis and develop a solution the NRC requests a new Target Completion Date of Q2 FY2024. Target Completion Date: FY 2024, Q2
OIG Analysis:	The proposed action meets the intent of the recommendation. The OIG will close the recommendation when the NRC provides documentation of the meetings with OCIO, OCHCO, NTEU and other stakeholders, and provides detailed documentation on why or why not the agency can 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.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 10:	Conduct an organizational level 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 April 4, 2023:	The NRC will 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. Target Completion Date: FY 2023, Q4
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation after the NRC conducts an organizational level BIA and updates its contingency planning policies and procedures accordingly.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 11:	For low availability categorized systems complete an initial BIA and update the BIA whenever a major change occurs to the system or mission that it supports. Address any necessary updates to the system contingency plan based on the completion of or updates to the system level BIA.
Agency Response Dated April 4, 2023:	For low-availability categorized systems, the NRC will complete an initial BIA and update the BIA whenever a major change occurs in the system or mission that it supports. The NRC will also address any necessary updates to the system contingency plan based on the completion of or updates to the system-level BIA. The NRC will also update its associated processes to incorporate these actions into its cybersecurity program. Target Completion Date: FY 2023, Q4
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation after the NRC addresses any necessary updates to the system contingency plan based on the completion of or updates to the system level BIA.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 12:	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 April 4, 2023:	The NRC will seek clarification from the Office of the Inspector General (OIG) of the requirements for this recommendation and establish an associated target completion date. Target Completion Date: To be determined.
OIG Analysis:	The NRC and OIG are working to come to an agreement on a sufficient way to complete this recommendation. The OIG will close the recommendation after the NRC integrates metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans to deliver persistent situational awareness across the organization.
Status:	Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020
Status of Recommendations
(OIG-21-A-05)

Recommendation 13:	Implement automated mechanisms to test system contingency plans, then update and implement procedures to coordinate contingency plan testing with ICT supply chain providers and implement an automated mechanism to test system contingency plans.
Agency Response Dated April 4, 2023:	The NRC will seek clarification of the requirements for this recommendation from the OIG and establish an associated target completion date. Target Completion Date: To be determined.
OIG Analysis:	The NRC and OIG are working to come to an agreement on a sufficient way to complete this recommendation. The OIG will close the recommendation when the agency provides documentation of the cost-benefit analysis and detailed information on the decision as to why or why not the agency will implement automated mechanisms to test system contingency plans, then update and implement procedures to coordinate contingency plan testing with ICT supply chain providers and implement an automated mechanism to test system contingency plans.
Status:	Open: Resolved.