May 4, 2022

MEMORANDUM TO: Daniel H. Dorman
Executive Director for Operations

David J. Nelson
Chief Information Officer

FROM: Eric Rivera ***/RA/***
Acting 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 6, 2022

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated April 6, 2022. Based on this response, recommendations 2(a), 2(c)-(e), and 4–13 remain in open and resolved status. Recommendations 1, 2(b), and 3 were previously closed. Please provide an update on the status of these resolved recommendations by October 14, 2022. If you have questions or concerns, please call me at (301) 415-5915 or Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

cc: J. Jolicoeur, OEDO
S. Miotla, 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

OIG-21-A-05

Status of Recommendations

Recommendation 2(a):	Assess enterprise, business process, and information system level risks.
Agency Response dated April 6, 2022:	Conversion of the NRC from a three-tier risk model to a five-tier risk model is underway and being piloted on the Information Technology Infrastructure. This will further align the NRC's practices with those of the National Institute of Standards and Technology (NIST) and with other Federal mandates such as the Federal Information Technology Acquisition Reform Act. The NRC has a planned completion date of the fourth quarter (Q4) of fiscal year (FY) 2022 for this action. Target Completion Date: Q4 FY 2022 Point of Contact: Bill Dabbs, OCIO/GEMSD/CSB
OIG Analysis:	The proposed action meets the intent of the recommendation. The OIG will close the recommendation when the NRC completes its assessment of enterprise, business process, and information system level risks.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

OIG-21-A-05

Status of Recommendations

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 6, 2022:	This action was dependent on completion of the ISA. With the ISA complete, the NRC has revised the completion date to the third quarter (Q3) of FY 2022. **Target Completion Date:** Q3 FY 2022 **Point of Contact:** Garo Nalabandian, OCIO/GEMSD/CSB
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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	The NRC plans to conduct an assessment of the agency's ISA over a 3-year period. The Phase 1 assessment is focused on the Identify Function, is expected to be completed Q3 FY22; this assessment is currently on schedule. The Phase 2 assessment focused on the Protect and Detect Functions, is planned and expected to be completed Q3 FY22. The Phase 3 assessment focused on the Respond and Recover Functions, is planned expected to be completed Q4 FY22. **Target Completion Date:** Q3 FY 2022 **Points of Contact:** Bill Dabbs, OCIO/GEMSD/CSB Sally Hardy, OCIO/GEMSD/CSB
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.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

OIG-21-A-05

Status of Recommendations

Recommendation 2(e):	Consistently assess the criticality 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 6, 2022:	OCIO will assess the criticality of system plans of action and milestones (POA&Ms) and the risk to the associated systems, data, and mission functions. **Target Completion Date:** Q4 FY 2022 **Point of Contact:** Bill Bauer, OCIO/GEMSD/CSB
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation after 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

OIG-21-A-05

Status of Recommendations

Recommendation 2(f):	Assess the NRC supply chain risk and fully define performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.
Agency Response dated April 6, 2022:	The NRC has defined an acquisition process, CSO-PROS-0005, "Information and Communications Technology Acquisition Process," dated March 18, 2021, available on the internal Cybersecurity Organization (CSO) SharePoint site, to identify contract requirements for the supply chain. Additionally, the NRC is developing a supplemental Supply Chain Risk Assessment process that will provide a basis for measuring and monitoring metrics to assess risks associated with contractor systems and services. The agency plans to complete this action by the third quarter (Q3) of FY 2022. **Target Completion Date:** Q3 FY 2022 **Points of Contact:** Kathy Lyons-Burke, OCIO/FO Garo Nalabandian, OCIO/GEMSD/CSB
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC assesses the supply chain risk and fully defines performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

OIG-21-A-05

Status of Recommendations

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 automated tools.
Agency Response dated April 6, 2022:	The NRC will identify a means to centralize the review of privileged and nonprivileged user access, audit log activity monitoring, and manage PIV or IAL 3/AAL 3 credential access to all NRC systems by continuing efforts to implement these capabilities using the automated tools. The agency plans to complete this action by Q3 FY 2022. **Target Completion Date:** Q3 FY 2022 **Points of Contact:** Michael Williams, OCIO/SDOD/NSOB David Offutt, OCIO/SDOD/NSOB
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC centralizes the review of privileged and nonprivileged user access, audit log activity monitoring, and the management of PIV or IAL 3/AAL 3 credential access to all the NRC systems.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

OIG-21-A-05

Status of Recommendations

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 6, 2022:	The NRC is evaluating ownership of this function and the need for an associated process update. Once ownership is established, the agency will review the corresponding process to incorporate any additional requirements for granting system access. **Target Completion Date:** Q4 FY 2022 **Point of Contact:** Garo Nalabandian, OCIO/GEMSD/CSB
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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	The NRC will continue to identify individuals with responsibilities or activities involving personally identifiable information (PII) and develop or identify the appropriate training based on Federal Government standards. **Target Completion Date:** Q3 FY 2022 **Point of Contact:** Sally Hardy, OCIO/GEMSD/CSB
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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	The NRC will perform a cost-benefit analysis of the cost of implementing a technical capability versus the risk of maintaining the current process. **Target Completion Date:** Q3 FY 2022 **Point of Contact:** Michael Mangefrida, CIO/GEMSD/CSB
OIG Analysis:	The proposed action meets the intent of the recommendation. The OIG will close the recommendation when the NRC provides documentation of the cost-benefit analysis and a detailed explanation as to why or why not the agency will implement the technical capability to restrict or not allow access for new employees and contractors until they have completed appropriate 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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	OCIO will work with the Office of the Chief Human Capital Officer, the National Treasury Employees Union, and other stakeholders to determine whether this would be feasible for the workforce. **Target Completion Date:** Q3 FY 2022 **Point of Contact:** Michael Mangefrida, CIO/GEMSD/CSB
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

OIG-21-A-05

Status of Recommendations

Recommendation 9:	Implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or non-reportable incident to US-CERT.
Agency Response dated April 6, 2022:	The NRC will implement metrics to measure the effectiveness of the process for investigating an event and determining whether it is an incident reportable to the U.S. Computer Emergency Readiness Team (US-CERT). **Target Completion Date:** Q3 FY 2022 **Points of Contact:** Michael Williams, OCIO/SDOD/NSOB David Offutt, OCIO/SDOD/NSOB
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC implements metrics to measure the effectiveness of the process for investigating an event and determining whether it is an incident reportable to the US-CERT.
Status:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020

OIG-21-A-05

Status of Recommendations

Recommendation 10:	Conduct an organizational level BIA [business impact assessment] 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 6, 2022:	OCIO will evaluate contingency planning requirements and associated priorities to determine the impact and related updates to policies and procedures. **Target Completion Date:** Q3 FY 2023 **Point of Contact:** Debra Reyes, OCIO/SDOD/DCTSB
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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	OCIO will evaluate contingency planning requirements and associated priorities to determine the impact and related updates to policies and procedures. **Target Completion Date:** Q3 FY 2023 **Point of Contact:** Debra Reyes, OCIO/SDOD/DCTSB
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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	OCIO will evaluate existing metrics for assessing the effectiveness of system contingency plans against related plans. Once assessed, the staff will review and update the corresponding plans accordingly. **Target Completion Date:** Q4 FY 2023 **Point of Contact:** Debra Reyes, OCIO/SDOD/DCTSB
OIG Analysis:	The proposed actions meet the intent of the 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

OIG-21-A-05

Status of Recommendations

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 6, 2022:	The NRC will perform a cost-benefit analysis of the cost of implementing a technical capability versus the risk of maintaining or supplementing the current process. **Target Completion Date:** Q4 FY 2023 **Point of Contact:** Debra Reyes, OCIO/SDOD/DCTSB
OIG Analysis:	The proposed actions meet the intent of the 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.