MEMORANDUM

DATE: September 9, 2022

TO: Daniel H. Dorman
Executive Director for Operations

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 2021 (OIG-22-A-04)

REFERENCE: CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM DATED JULY 14, 2022

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated July 14, 2022. Based on this response, recommendations 1 through 8, and 10 through 18, are open and resolved. Recommendation 9 was previously closed. Please provide an updated status of the open and resolved recommendations by January 17, 2023.

If you have any questions or concerns, please call me at (301) 415-5915 or Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

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

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

Recommendation 1:	Reconcile mission priorities and cybersecurity requirements into profiles to inform the prioritization and tailoring of controls (e.g., HVA control overlays) to support the risk-based allocation of resources to protect the NRC's identified Agency level and/or National level HVAs.
Agency Response Dated July 14, 2022:	The U.S. Nuclear Regulatory Commission (NRC) will reconcile mission priorities and cybersecurity requirements to derive profiles to inform the prioritization and tailoring of controls to support the risk-based allocation of resources to protect the NRC's identified agency-and national-level high-value assets (HVAs). Target Completion Date: Fiscal year (FY) 2023, Q2 Point of Contact: Consuella Debnam, OCIO/GEMSD/CSB 301-287-0834 Bill Dabbs, OCIO/GEMSD/CSB (301) 415-0524
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC reconciles mission priorities and cybersecurity requirements to derive profiles to inform the prioritization and tailoring of controls to support risk-based allocation of resources to protect the NRC's identified Agency and National level High Value Assets.
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

OIG-22-A-04

Status of Recommendations

Recommendation 2:	Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity information across organizational units, and (iii) prioritize operational risk response.
Agency Response Dated July 14, 2022:	The NRC will evaluate existing data and metrics to update the Agency's cybersecurity risk register to capture aggregate security risks, normalize cybersecurity risk information across organizational units, and prioritize operational risk response. Target Completion Date: FY 2023, Q1 Point of Contact: Heather Dempsey OCIO/DRMA 301-415-0856
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC evaluates existing data and metrics to update the Agency's cybersecurity risk register to capture aggregate security risks, normalize cybersecurity information across organizational units, and prioritize operational risk response.
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

OIG-22-A-04

Status of Recommendations

Recommendation 3:	Update procedures to include assessing the impacts to the organization's ISA prior to introducing new information systems or major system changes into the Agency's environment.
Agency Response Dated July 14, 2022:	The NRC will assess the information security architecture (ISA) and define appropriate procedures as needed to evaluate impacts from introducing new information systems or major system changes into the Agency's environment. Target Completion Date: FY 2023, Q1 Point of Contact: Bill Dabbs, OCIO/GEMSD/CSB (301) 415-0524 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC updates procedures to include assessing the impacts to the organization's ISA prior to introducing new information systems or major system changes into the Agency's environment.
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

OIG-22-A-04

Status of Recommendations

Recommendation 4:	Develop and implement procedures in the POA&M process to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.
Agency Response Dated July 14, 2022:	The NRC will review the current plan of action and milestones (PO&AM) process to assess additional mechanisms for prioritizing completion and incorporate them as part of documenting a justification and approval for delayed POA&Ms. Target Completion Date: FY 2022, Q4 Point of Contact: Bill Dabbs, OCIO/GEMSD/CSB 301-415-0524 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC develops and implements procedures in the POA&M process to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.
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

OIG-22-A-04

Status of Recommendations

Recommendation 5:	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 July 14, 2022:	The NRC will assess the 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. Target Completion Date: FY 2023, Q3 Point of Contact: Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421 Kathy Lyons-Burke, OCIO (301) 415-6595
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC assesses the NRC 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 THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will assess existing policies and processes and document additional guidance as needed for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third party providers. Target Completion Date: FY 2023, Q3 Point of Contact: Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421 Kathy Lyons-Burke, OCIO (301) 415-6595
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC documents and implements 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:	Open: Resolved.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will assess the feasibility of implementing processes for the 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. Target Completion Date: FY 2023, Q4 Point of Contact: Benjamin Partlow, OCIO/GEMSD/CSB 301-415-2449 Kathy Lyons-Burke, OCIO 301-415-6595
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC implements 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.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will identify, develop, and implement role-based training for supply chain risk management (SCRM), to include the detection of counterfeit system components, targeted to individuals who hold the appropriate roles and responsibilities related to SCRM. Target Completion Date: FY 2023, Q1 Point of Contact: Bill Bauer, OCIO/GEMSD/CSB 301-415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC develops and implements 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

OIG-22-A-04

Status of Recommendations

Recommendation 10:	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 NRC systems (findings noted in bullets a, and c, above) by continuing efforts to implement these capabilities using the Splunk QAudit, SailPoint, and CyberArk automated tools.
Agency Response Dated July 14, 2022:	The NRC completed implementation of a new, workflow-based privileged account review process in October 2021. The agency will identify a means to centralize 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 Splunk QAudit, SailPoint, and CyberArk automated tools. Target Completion Date: December 30, 2022 Point of Contact: Jim Peyton, OCIO/SDOD/NSOB (301) 287-0701
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC identifies a means to centralize 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 automated tools.
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

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The Office of the Chief Information Officer (OCIO) will work with counterparts in the Office of Administration (ADM) to implement a process change to ensure that individual's complete nondisclosure and rules of behavior agreements before being granted system access. Target Completion Date: September 30, 2022 Point of Contact: Jim Peyton, OCIO/SDOD/NSOB (301) 287-0701
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC implements a process change to ensure that individuals complete non-disclosure and rules of behavior prior to being granted system access.
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

OIG-22-A-04

Status of Recommendations

Recommendation 12:	Conduct an independent review or assessment of the NRC privacy program and use the results of these reviews to periodically update the privacy program.
Agency Response Dated July 14, 2022:	The NRC is evaluating current resources to determine support for development of a written assessment. Target Completion Date: FY 2023, Q2 Point of Contact: Sally Hardy, OCIO/GEMSD/CSB (301) 415-5607 Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC conducts an independent review or assessment of the NRC privacy program and uses the results of these reviews to periodically update the privacy program.
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

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will review current capabilities and perform a gap analysis to determine the best and most economical path forward to ensure new NRC employees and contractors have completed the required security awareness and applicable role-based training in the requisite period of time before NRC system access. Target Completion Date: FY 2023, Q1 Point of Contact: Bill Bauer, OCIO/GEMSD/CSB 301-415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC implements 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.

Evaluation Report

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will review current capabilities and perform a gap analysis to determine the best and most economical path forward to ensure NRC employees who have not completed the required security awareness and applicable role-based training have restricted access to NRC systems in such a way as to not disrupt critical Agency services. Target Completion Date: FY 2023, Q1 Point of Contact: Bill Bauer, OCIO/GEMSD/CSB 301-415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC implements 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 THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021

OIG-22-A-04

Status of Recommendations

Recommendation 15:	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 July 14, 2022:	The NRC will implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or nonreportable incident to the U.S. Computer Emergency Readiness Team (US-CERT). Target Completion Date: December 30, 2022 Point of Contact: David Offutt, OCIO/SDOD/NSOB (301) 287-0636 Mike Lidell, OCIO/SDOD/NSOB (301) 287-9265
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC implements metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or nonreportable incident to US-CERT.
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

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	The NRC will conduct an organizational-level business impact assessment (BIA) to determine contingency planning requirements and priorities, including for mission essential functions and HVAs, and update contingency planning policies and procedures accordingly. Target Completion Date: FY 2023, Q3 Point of Contact: Julie Hughes, OCIO/GEMSD/CSB (301) 287-9277 Debra Reyes, OCIO/ITSDOD/DCTSB (301) 287-0681
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC conducts 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.
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

OIG-22-A-04

Status of Recommendations

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 July 14, 2022:	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 2023, Q4 Point of Contact: Julie Hughes, OCIO/GEMSD/CSB (301) 287-9277 Debra Reyes, OCIO/ITSDOD/DCTSB (301) 287-0681
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC integrates 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.
Status:	Open: Resolved.

Status of Recommendations

Recommendation 18:	Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.
Agency Response Dated July 14, 2022:	The NRC will assess the feasibility of implementing procedures to coordinate contingency plan testing with information communication technology (ICT) supply chain providers. Target Completion Date: FY 2023, Q4 Point of Contact: Kathy Lyons-Burke, OCIO (301) 415-6595 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842
OIG Analysis:	The proposed actions meet the intent of the recommendation. The OIG will close this recommendation when the NRC updates and implements procedures to coordinate contingency plan testing with ICT supply chain providers.
Status:	Open: Resolved.