STATUS OF RECOMMENDATIONS: OIG FINAL AUDIT REPORT OIG-22-A-04, "INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021"

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 January 12, 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 risk-based allocation of resources to protect the NRC's identified Agency and National level High Value Assets.
Target Completion Date:	FY23 Q2
Point of Contact:	Kathryn Harris, OCIO/GEMSD/CSB (301) 287-0515 Bill Dabbs, OCIO/GEMSD/CSB (301) 415-0524
Recommendation 2:	Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity.
Agency Response Dated January 12, 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:	FY23 Q1
Point of Contact:	Alan Sage, OCIO/GEMSD/CSB (301) 415-7060
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.

Enclosure

Agency Response Dated January 12, 2022:	The NRC will assess the ISA and define appropriate procedures as needed to evaluate impacts to introducing new information systems or major system changes into the Agency's environment.
Target Completion Date:	FY23 Q1
Point of Contact:	Bill Dabbs, OCIO/GEMSD/CSB (301) 415-0524 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842
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 January 12, 2022:	The Agency will review the current Plan of Action and Milestones (PO&AM) process to assess additional mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.
Target Completion Date:	FY22 Q4
Point of Contact:	Bill Dabbs, OCIO/GEMSD/CSB (301) 415-0524 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842
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 January 12, 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:	FY23 Q3
Point of Contact:	Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421 Kathy Lyons-Burke, OCIO (301) 415-6595
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 January 12, 2022:	The NRC will assess the existing policies and processes document 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:	FY23 Q3
Point of Contact:	Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421 Kathy Lyons-Burke, OCIO (301) 415-6595
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 January 12, 2022:	The NRC will assess the feasibility of implementing 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.
Target Completion Date:	FY23 Q4
Point of Contact:	Garo Nalabandian, OCIO/GEMSD/CSB (301) 415-8421 Kathy Lyons-Burke, OCIO (301) 415-6595
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 January 12, 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:	FY23 Q1
Point of Contact:	Michael Mangefrida, OCIO/GEMSD/CSB (301) 415-2264

Recommendation 9:	Continue to monitor the remediation of critical and high vulnerabilities and identify a means to assign and track progress of timely remediation of vulnerabilities.
Agency Response Dated January 12, 2022:	This Recommendation 9 is the same as Recommendation 3 from OIG FISMA Audit OIG-21-A-05, which was officially closed by OIG on December 9, 2021. The OIG Memorandum dated December 9, 2021 can be found in the internal Agencywide Documents Access and Management System (ADAMS), Accession No. ML21343A226. Accordingly, this recommendation should be closed.
Target Completion Date:	Complete
Point of Contact:	David Offutt, OCIO/SDOD/NSOB (301) 297-0636
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 January 12, 2022:	Implementation of a new, workflow based privileged account review process was completed in October 2021. The NRC 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:	FY23 Q1
Point of Contact:	Jim Peyton, OCIO/SDOD/NSOB (301) 287-0701
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 January 12, 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 individuals complete non-disclosure and rules of behavior prior to being granted system access.
Target Completion Date:	FY22 Q4

Point of Contact:	Jim Peyton, OCIO/SDOD/NSOB 301) 287-0701
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 January 12, 2022:	The NRC is evaluating current resources to determine support for development of a written assessment.
Target Completion Date:	FY22 Q3
Point of Contact:	Sally Hardy, OCIO/GEMSD/CSB (301) 415-5607 Garo Nalbandian, OCIO/GEMSD/CSB (301) 415-8421
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 January 12, 2022:	The NRC will perform a review of 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 prior to NRC system access.
Target Completion Date:	FY23 Q1
Point of Contact:	Michael Mangefrida, OCIO/GEMSD/CSB (301) 415-2264
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 January 12, 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 system in such a way as to not disrupt critical agency services.

Target Completion Date:	FY23 Q1
Point of Contact:	Michael Mangefrida, OCIO/GEMSD/CSB (301) 415-2264
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 January 12, 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 non-reportable incident to U.S. Computer Emergency Readiness Team (US-CERT).
Target Completion Date:	FY23 Q1
Point of Contact:	David Offutt, OCIO/SDOD/NSOB (301) 287-0636 Mike Lidell, OCIO/SDOD/NSOB (301) 287-9265
Recommendation 16:	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 January 12, 2022:	The NRC will conduct an organizational level Business Impact Analysis 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:	FY23 Q3
Point of Contact:	Julie Hughes, OCIO/GEMSD/CSB (301) 287-9277 Rozier Carter, OCIO/ITSDOD/DCTSB (301) 287-0670
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 January 12, 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:	FY23 Q4
Point of Contact:	Julie Hughes, OCIO/GEMSD/CSB (301) 287-9277 Rozier Carter, OCIO/ITSDOD/DCTSB (301) 287-0670
Recommendation 18:	Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.
Agency Response Dated January 12, 2022:	The NRC will assess the feasibility of implementing procedures to coordinate contingency plan testing with Information Communication Technology supply chain providers.
Target Completion Date:	FY23 Q4
Point of Contact:	Kathy Lyons-Burke, OCIO (301) 415-6595 Bill Bauer, OCIO/GEMSD/CSB (301) 415-5842