INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 1:	Develop and document procedures for ensuring publicly accessible Web applications are assigned a system owner with responsibility for ensuring adequate security measures are in place for those applications.
Agency Response Dated July 1, 2016:	The NRC plans to update and implement the OIG recommended procedures by early Q2 FY 2017. The plan includes the verification of system owners for each publicly accessible Web application whose parent systems are currently registered in the NRC System Inventory; identification of additional applications for inclusion in the NRC System Inventory; revision of current process documents to require system owners to keep System Inventory data current and understand their roles and responsibilities for ensuring adequate security measures are in place for their applications; and communication of the revised process to all system owners. **Target Completion Date:** Q2 FY 2017
Agency Response Dated March 31, 2017:	This activity was delayed due to the OCIO reorganization activities. To date, system owners have been identified for publicly accessible web applications via parent systems, and roles and responsibilities are being communicated to system owners. The system inventory is being updated to reflect ownership assignments, and system child/parent relationships. The Change Control Board (CCB) procedure will be revised to validate that a system owner has been named before a system change can be implemented. This process will be mandatory for all system changes for new and existing systems. **Revised Target Completion Date:** Q3 FY 2017
Agency Response Dated September 29, 2017:	The Change Control Board (CCB) procedure has been revised to validate that a system owner has been named before a system change can be implemented. This process is mandatory for all system changes for new and existing systems. **Target Completion Date:** Completed The NRC requests that Recommendation 1 be closed. **Point of Contacts:** Allen Sullivan, 240-415-8950 Bill Dabbs, 301-415-0524

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 2:	Develop and document procedures for ensuring publicly accessible Web applications are incorporated into an approved system authorization boundary and for clearly identifying those applications in system authorization documentation.
Agency Response Dated July 1, 2016:	The NRC plans to update and implement the OIG recommended procedures no later than the end of Q2 FY 2017, as part of the effort described in our response to OIG recommendation 1. The plan includes that publicly accessible Web applications are incorporated into an approved system authorization boundary; revision of current process documents to ensure these applications are identifiable in system authorization documentation; and communication of the revised process to system owners. **Target Completion Date:** Q2 FY 2017
Agency Response Dated March 31, 2017:	This activity was delayed due to the OCIO reorganization activities. To date, system boundaries and system owners have been identified for publicly accessible web applications via parent systems, and roles and responsibilities are being communicated to system owners. The system inventory is being updated to reflect ownership assignments, and system child/parent relationships. The Change Control Board (CCB) procedure will be revised to validate that a system has been incorporated into a system boundary before a system change can be implemented. This process will be mandatory for all system changes for new and existing systems. **Revised Target Completion Date:** Q3 FY 2017
Agency Response Dated September 29, 2017:	The system inventory has been updated to reflect ownership assignments, and system child/parent relationships. The Change Control Board (CCB) procedure has been revised to validate that a system has been incorporated into a system boundary before a system change can be implemented. This process is mandatory for all system changes for new and existing systems. **Target Completion Date:** Completed The NRC requests that Recommendation 2 be closed. **Point of Contacts:** Allen Sullivan, 240-415-8950 Bill Dabbs, 301-415-0524

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 4:	Develop a plan and schedule to identify, review, and update all NRC cyber security standards that have not been updated in the past 12 months.
Agency Response Dated July 1, 2016:	The NRC will develop a plan and schedule to review and update all cyber security standards as needed. **Target Completion Date:** Q1 FY 2017
Agency Response Dated March 31, 2017:	The NRC has completed an inventory of cyber security standards. All vendor specific technical standards were removed from the standards repository. The agency has decided the costs of maintaining standards for specific software and technologies is prohibitive. Moving forward the agency will use public standards developed by the Center for Internet Security (CIS) and Defense Information System Agency (DISA). Due to reductions in the agency's corporate support budget, the review and update of existing standards has slowed considerably and additional time is needed to review and update all impacted documents. **Revised Target Completion Date:** Q2 FY 2018
Agency Response Dated September 29, 2017:	The agency continues to move toward the use of public standards developed by the Center for Internet Security (CIS) and Defense Information System Agency (DISA). The review of existing standards has resulted in a number of standards being eliminated. The NRC is on track to meet the target completion date. **Target Completion Date:** Q2 FY 2018
Agency Response Dated March 31, 2018:	The schedule to review and update standards has been completed. By Q4 2019 all standards will have been reviewed, updated or retired. **Revised Target Completion Date:** Q4 FY 2019
	Point of Contacts: Allen Sullivan, 240-415-8950 Bill Dabbs, 301-415-0524

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 5:	Develop a plan and schedule for evaluating the vulnerabilities identified, determining the appropriate action to address the vulnerability (e.g., mitigation, deviation, risk acceptance), and implementing the remedial actions.
Agency Response Dated July 1, 2016:	The NRC will add all identified vulnerabilities to the appropriate Plan of Action & Milestone (POA&M) plans for ADAMS, BASS, ISMP, ITI, MOMCE, OCIMS, RICS, STAQS and VIDEO. The vulnerabilities will be managed and prioritized along with existing POA&M items. **Target Completion Date:** Q4 FY 2016
Agency Response Dated March 31, 2017:	The NRC needs additional time to address the risks identified in this audit and to implement additional policies on the scanner appliances that address web-centric vulnerabilities. This will help ensure that the agency focuses on the most significant risks with the available resources. The NRC will add all identified vulnerabilities to the appropriate Plan of Action & Milestone (POA&M) plans and the vulnerabilities will be managed and prioritized along with existing POA&M items. Although the completion of this recommendation is outstanding, the NRC is implementing additional vulnerability scanning. Specifically, in support of DHS's Continuous Diagnostic and Mitigation (CDM) program, the NRC recently implemented and is currently tuning a vulnerability scanning solution. Also, the NRC has regular security meetings focusing on addressing the most exploitable risks identified by the scanners across the enterprise. **Revised Target Completion Date:** Q3 FY 2017

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Agency Response Dated September 29, 2017:	The NRC has evaluated the vulnerabilities identified from the audit and created a program level plan of action and milestone (POA&M), POA&M ID 17-15, to address the vulnerabilities from the audit. Please refer to the POA&M details (ML17264B085) for the schedule and actions to be taken to address the vulnerabilities (vulnerability list ML17264A858). Validation of remediated vulnerabilities will be conducted with an Open Web Application Security Project (OWASP) scanning tool. The OWASP scanning tool is planned for implementation by FY18 Q3. The NRC requests that Recommendation 5 be closed. **Target Completion Date:** Completed **Point of Contacts:** Michael Williams, 301-287-0660 David Offutt, 301-287-0636

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 6:	Complete the appropriate NRC RMF authorization activities for the NRC Webcast Portal.
Agency Response Dated July 1, 2016:	The appropriate NRC RMF authorization activities for the NRC Webcast Portal are scheduled for completion in FY 2017. **Target Completion Date:** Q1 FY 2017
Agency Response Dated March 31, 2017:	The NRC RMF authorization for the NRC Webcast Portal was initiated. However, it was put on hold because the current contract is ending. ADM intends to award a new contract to a FEDRamp authorized service provider. The scope of the contract will include ensuring FISMA compliance. In addition, ADM has obligated funds to ensure that FISMA activities will be performed. **Revised Target Completion Date:** Q4 FY 2017
Agency Response Dated September 29, 2017:	The NRC Webcast Portal has been authorized through March 31, 2019. ADM intends to award a new contract to a FEDRamp authorized service provider by the second quarter of 2019. The scope of the contract will include ensuring FISMA compliance. In addition, ADM has obligated funds to ensure that FISMA activities will be performed.
Agency Response Dated April 10, 2018:	The NRC Webcast Portal has been authorized through March 31, 2019. ADM has awarded a new contract to the VBrick Cloud Solution hosted by Amazon Web Services (AWS), a FEDRamp authorized service provider. The scope of the contract will include ensuring FISMA compliance. Currently, ADM is working with OASIS Systems to develop the security assessment package for this new web service. **Revised Target Completion Date:** Q1 FY 2019 **Point of Contacts:** Diem Le, 301-415-7114 Allen Sullivan, 240-415-8950

INDEPENDENT EVALUATION OF THE SECURITY OF NRC'S PUBLICLY ACCESSIBLE WEB APPLICATIONS

OIG-16-A-15

Status of Recommendation

Recommendation 7:	Update CSO-PROS-2101 to include procedures for updating DNS entries and other resources allocated to new systems in addition to the inventory.
Agency Response Dated July 1, 2016:	The NRC will work with the appropriate NRC FISMA System Owners to integrate the procedures for decommissioning IT systems into existing Capital Planning and Investment Control governance processes to ensure all decommissioning instances are captured, DNS entries are updated, and system inventories are updated. When these efforts are completed, CSO-PROS-2101 will be rescinded. **Target Completion Date:** Q3 FY 2017
Agency Response Dated March 31, 2017:	The NRC engaged with system owners to ensure that all appropriate decommissioning activities are occurring on schedule. These procedures, including DNS and system inventory processes are being updated to include these steps, and CSO-PROC-2101 will be rescinded once the process completes. **Target Completion Date:** Q3 FY 2017
Agency Response Dated September 29, 2017	The NRC continues to engage with system owners and system administrators. The Change Control Board (CCB) through the use of a change request form (CRQ), documents decommissioning efforts. The decommissioning process validates that all decommissioning steps are taken before the CRQ can be closed. This process is mandatory for all system changes for new and existing systems. The NRC is requesting that Recommendation 7 be closed. **Point of Contacts:** Allen Sullivan, 240-415-8950 Bill Dabbs, 301-415-0524