INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 (OIG-19-A-08)

Response to Recommendations

Recommendation 1:	Develop and implement a process to remove all non-standard software that has not been approved by an authorized agency official.
Agency Response Dated May 01, 2019:	The U.S. Nuclear Regulatory Commission (NRC) will develop and implement a process to remove all nonstandard software that has not been approved by an authorized agency official.
Agency Response Dated January 24, 2020:	The NRC has developed a process to remove all nonstandard software that has not been approved by an authorized agency official. The process implementation is on track with the current target completion date. **Target Completion Date:** March 31, 2020 **Points of Contact:** Michael Williams, OCIO/SDOD/SOB 301-287-0660 David Offutt, OCIO/SDOD/SOB 301-287-0636
Recommendation 2:	Implement a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network.
Agency Response Dated May 01, 2019:	The NRC will implement a process to manage nonstandard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on the NRC's network. The agency will review and update the current Office of the Chief Information Officer (OCIO) process for Information Technology (IT) Business Need Requests to meet the requirements outlined in Recommendation 2. In addition, the new End User Computing contract specifies that all software must be approved and have a service ticket before software may be installed.
Agency Response Dated January 24, 2020:	The NRC has developed and implemented a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network. Please refer to Agencywide Documents Access and Management

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 (OIG-19-A-08)

Response to Recommendations

System (ADAMS) Main Library (ML) ML20024E443 for the intake review process.

The NRC believes the intent of this recommendation has been fulfilled.

Target Completion Date: Completed

Points of Contact: Michael Williams, OCIO/SDOD/SOB
301-287-0660
David Offutt, OCIO/SDOD/SOB
301-287-0636

Recommendation 3: Monitor the approved installed software on NRC's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found.

Agency Response Dated May 01, 2019: The NRC will monitor the approved installed software on the agency's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found.

Agency Response Dated January 24, 2020: All endpoints in the NRC's production networking environment are periodically scanned and inspected for known vulnerabilities on a continuous basis as directed by DHS guidance. The results from the vulnerability scanning are used for system vulnerability assessments that are performed as part of the agency's continuing monitoring process to mitigate and remediate known system vulnerabilities. In addition, vulnerability reporting is included in the daily cybersecurity report where actions to remediate the vulnerabilities are discussed. Refer to ADAMS ML20024E508 for a sample of the Cybersecurity Daily Report and ADAMS ML20024E448 for examples of actions taken to remediate known high-risk vulnerabilities. A review of software is performed when software contracts are renewed to determine whether software is still in use. The software review is used to determine appropriate licensing of software products used by the NRC. The resulting action is that software is updated to a supported version or the software is removed.

Response to Recommendations

The NRC believes the intent of this recommendation has been fulfilled.

Target Completion Date: Completed

Points of Contact: Michael Williams, OCIO/SDOD/SOB
301-287-0660
David Offutt, OCIO/SDOD/SOB
301-287-0636

Recommendation 4: Develop and establish processes and procedures to govern the installation of non-standard software, including processes and procedures on determining impact to agency operations or cybersecurity.

Agency Response Dated May 01, 2019: The NRC will develop and establish processes and procedures to govern the installation of nonstandard software, including processes and procedures for determining the impact to agency operations or cybersecurity. The agency will review and update the current OCIO process for IT Business Need Requests to meet the requirements outlined in Recommendation 4. The new End User Computing contract specifies that all software must be approved and have a service ticket before software may be installed.

Agency Response Dated January 24, 2020: The NRC has developed processes and procedures to govern the installation of non-standard software, including processes and procedures on determining impact to agency operations or cybersecurity. Please refer to ADAMS ML20024E443 for the intake review process, ADAMS ML20024E444 and ADAMS ML20024E446 for the process flow documents, and the NRC Service Catalog, "Hardware, Software and Custom Solutions (Intake)" (https://drupal.nrc.gov/ocio/catalog/55704), for additional information.

The NRC believes the intent of this recommendation has been fulfilled.

Target Completion Date: Completed

Points of Contact: Michael Williams, OCIO/SDOD/SOB
301-287-0660
David Offutt, OCIO/SDOD/SOB
301-287-0636

INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2018 (OIG-19-A-08)

Response to Recommendations

Recommendation 5:	Implement a process to remove unsupported software from NRC networks.
Agency Response Dated May 01, 2019:	The NRC will develop and implement a process to remove unsupported software from the agency's network environment.
Agency Response Dated January 24, 2020:	The NRC has developed a process to remove unsupported software from the agency's network environment. Part of the process is generating a report of the unsupported software that exists in the production environment. Refer to ADAMS ML20024E556 for a sample report. The implementation of this process is on track with the current target completion date. **Target Completion Date:** March 31, 2020 **Points of Contact:** Michael Williams, OCIO/SDOD/SOB 301-287-0660 David Offutt, OCIO/SDOD/SOB 301-287-0636
Recommendation 6:	Implement a process to mitigate known high-risk vulnerabilities.
Agency Response Dated May 01, 2019:	The NRC will implement a process to mitigate known high-risk vulnerabilities for application software that resides on NRC networks.
Agency Response Dated January 24, 2020:	The NRC has implemented a process to mitigate known high-risk vulnerabilities for application software that resides on NRC networks. All endpoints in the NRC's production networking environment are scanned for vulnerabilities continually as directed by DHS guidance. The results from the vulnerability scanning are used for system vulnerability assessments that are performed as part of the agency's continuing monitoring process to mitigate and remediate known system vulnerabilities. In addition, high-risk vulnerabilities are included in the daily cybersecurity report where actions to remediate the vulnerabilities are discussed. Please refer to ADAMS ML20024E508 for an example of the Cybersecurity Daily Report and ADAMS ML20024E448 for an example of actions taken to remediate know high-risk vulnerabilities.

Response to Recommendations

The NRC believes the intent of this recommendation has been fulfilled.

Target Completion Date: Completed

Points of Contact: Michael Williams, OCIO/SDOD/SOB
301-287-0660
David Offutt, OCIO/SDOD/SOB