UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

July 25, 2018

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017
(OIG-18-A-02)

REFERENCE: CHIEF INFORMATION OFFICER, MEMORANDUM DATED JUNE 28, 2018

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated June 28, 2018. Based on this response, all recommendations related to this evaluation report are now closed.

If you have any questions or concerns, please call me at (301) 415-5915 or Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

cc: R. Lewis, OEDO
H. Rasouli, OEDO
J. Jolicoeur, OEDO
J. Bowen, OEDO
EDO_ACS_Distribution

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 1: Perform a gap analysis to identify required IT security program documents, IT security program documents that need to be developed, and IT security program documents that need to be updated and/or finalized.

Agency Response Dated June 28, 2018: Gap analysis has been completed. The Continuous Monitoring Process documentation was updated to include development of security program documents and requirements for maintaining, reviewing and updating these documents. Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled.

Target Completion Date: Completed.

OIG Analysis: OIG reviewed the documentation provided by the agency and determined that it met the intent of the recommendation. Specifically, the agency provided appropriate evidence supporting it had performed a gap analysis to identify required IT security program documents, including those that need to be developed, updated and/or finalized. Therefore, this recommendation is considered closed.

Status: Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 2: Develop a schedule for developing, updating and completing all required IT security program documentation.

Agency Response Dated June 28, 2018: Schedules have been developed to update current processes, template, standards, procedures, guidance, and checklists. This activity includes developing new processes, templates and standards. Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled

Target Completion Date: Completed.

OIG Analysis: OIG reviewed the documentation provided by the agency and determined that a schedule for developing, updating and completing all required IT security program documentation was completed. Therefore, this recommendation is considered closed.

Status: Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 3:	Develop policies and procedures for keeping IT security program documentation up-to-date.
Agency Response Dated June 28, 2018:	The FISMA repository for this effort is currently in place. Policies and procedures have been developed and put in place to continuously monitor and track the IT security program documentation, to ensure that these documents are kept up to date. A timetable schedule has been developed and put in place for this purpose. The developed schedules are the plan for addressing updating documents as needed. Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled. **Target Completion Date:** Completed.
OIG Analysis:	OIG reviewed the documentation provided by the agency and determined that policies and procedures for keeping IT security program documentation up-to-date were developed. Therefore, this recommendation is considered closed.
Status:	Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 4: Develop and implement a schedule for reviewing and updating all security categorizations.

Agency Response Dated June 28, 2018: This activity is currently being performed during the system Periodic System Cybersecurity Assessment (PSCA) phase. In addition, the Periodic System Cybersecurity Assessment (PSCA), and security categorizations are tracked via the Cybersecurity Risk Dashboard (CRDB). Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled.

Target Completion Date: Completed.

OIG Analysis: OIG reviewed the documentation provided by the agency and determined that a schedule for reviewing and updating all security categorizations was developed and implemented. Therefore, this recommendation is considered closed.

Status: Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC’S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 5: Develop and implement a schedule for reviewing and updating all business impact assessments and for developing them if they are missing.

Agency Response Dated June 28, 2018: The Continuous Monitoring Process has been updated to include reviewing/updating all business impact assessments. This activity is performed ideally prior to the system’s contingency test to ensure accuracy of information. The business impact assessments are tracked via the Cybersecurity Risk dashboard (CRDB). Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled.

Target Completion Date: Completed.

OIG Analysis: OIG reviewed documentation provided by the agency and determined that a schedule for drafting, as appropriate, reviewing, and updating all business impact assessments was developed and implemented. Therefore, this recommendation is considered closed.

Status: Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 6: Develop and implement a schedule for reviewing and updating all contingency plans.

Agency Response Dated June 28, 2018: This process exists and is implemented during the system Periodic System Cybersecurity Assessment (PSCA) phase. This is performed during the annual contingency test. The Periodic System Cybersecurity Assessment (PSCA), contingency plans, and the annual contingency test are tracked via the Cybersecurity Risk Dashboard (CRDB). Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled.

Target Completion date: Completed.

OIG Analysis: OIG reviewed the documentation provided by the agency and determined that a schedule for reviewing and updating all contingency plans was developed and implemented. Therefore, this recommendation is considered closed.

Status: Closed.

EVALUATION REPORT

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2017

OIG-18-A-02

Status of Recommendations

Recommendation 7: Develop procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard.

Agency Response Dated June 28, 2018: The Agency is currently tracking the following matrices on the Cybersecurity Risk Dashboard (CRDB): Contingency Plans (CP), Business Impact Analysis (BIA), Plan of Action and Mitigation (POA&Ms), Conducting Periodic System Cybersecurity Assessment, Computer Security Awareness Training, Role-Based Training, Incident Trends (Data compiled from the Security Operations Center (SOC), Phishing Exercise Results, Completion of Authorizing Official (AO) conditions, Number of Authorized systems, and Number of external IT services used by NRC. As the Cybersecurity Risk Dashboard is being further enhanced and improved all activities subject to monitoring will be added to the dashboard.

For those activities still in transit for monitoring in the dashboard other mechanisms are in place in order to ensure proper and continues monitoring. These are accomplished through daily status reports and periodic scheduled activities to properly and prudently monitor such activities. These safeguards were put in place to ensure that no critical activity subject to monitoring that might not have been transitioned to the dashboard, is provided attentive oversight. Supporting documentation for this activity is enclosed with this submission. The NRC believes the intent of the OIG recommendation has been fulfilled.

Target Completion Date: Completed.

<u>Recommendation 7 (cont.)</u>:

OIG Analysis: OIG reviewed the documentation provided by the agency and determined that the procedures for monitoring completion of all continuous monitoring activities, including those that are not explicitly tracked on the Cybersecurity Risk Dashboard, were developed. Therefore, this recommendation is considered closed.

Status: Closed.