Audit of NRC's Network Security Operations Center (OIG-16-A-07)
Status of Recommendations

Recommendation 1: Revise information technology service contract requirements to include SOC-specific performance objectives

Agency Response Dated February 8, 2016: Agree. OCIO will revise the existing information technology service contract requirements to include new SOC specific performance objectives that will be negotiated and jointly developed with the current information technology contractor. Any revisions made to the current contract that incorporate new performance objectives will be made within the existing contract framework in order to prevent increased contract costs. The new performance objectives developed during the course of the current contract will be incorporated into the future information technology services contract.

Target Completion Date: May 31, 2016

OIG Analysis Dated July 28, 2016: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives verification that NRC revised the requirements to include SOC specific performance objectives in the contract.

Status: Resolved.

Agency Response Dated October 31, 2016: On April 19, 2016, the Office of the Chief Information Officer (OCIO) and the current information technology service contractor negotiated and jointly developed new Security Operations Center (SOC)-specific performance objectives. The new performance objectives did not require a formal contract modification to the current information technology service contract.

OCIO, in coordination with the current information technology service contractor, updated the SOC Procedures Guide (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16124A914) to incorporate new SOC procedures and processes as well as new technologies that have been added to the security environment. The information technology service contractor follows the SOC Procedures Guide to provide operational guidance during contract performance.

Accompanying the SOC Procedures Guide is a checklist to indicate which security operations support contractor completed the tasks each day. The review procedures are being conducted on a weekly basis and sample checklist documents can be found in the Daily Review of Security Reports (ADAMS Accession No. ML16292A677).

The new SOC-specific performance objectives have been incorporated into the draft statement of work (SOW) for the follow-on information technology services contract.

Target Completion Date: March 31, 2017

Point of Contact: Michael Williams, 301-287-0660

Recommendation 2: Revise information technology service contract requirements to define SOC functional requirements.

Agency Response Dated February 8, 2016: Agree. OCIO will develop SOC specific functional requirements and the SOC team will update the existing SOC procedures guide and SOC services briefing. These revised requirements will be incorporated into the next information technology services contract.

Target Completion Date: September 30, 2016

OIG Analysis Dated July 28, 2016: The proposed actions meet the intent of the recommendation. OIG will close this recommendation when OIG receives verification that NRC revised the information technology service contract requirements to define the SOC functional requirements.

Status: Resolved.

Agency Response Dated October 31, 2016: After further analysis, OCIO determined that it was most prudent to focus efforts on thoroughly defining SOC functional requirements for inclusion in the follow-on information services contract. The current information technology service contract expires on May 17, 2017.

To address the finding as it relates to the current contract, OCIO, in coordination with the current information technology service contractor, updated the SOC Procedures Guide (ADAMS Accession No. ML16124A914) and SOC services briefing (ADAMS Accession No. ML15167A405) to incorporate new SOC procedures and processes as well as new technologies that have been added to the security environment.

Target Completion Date: May 17, 2017

Point of Contact: Michael Williams, 301-287-0660

Audit of NRC's Network Security Operations Center (OIG-16-A-07)
Status of Recommendations

Recommendation 3:	Define in policy, SOC functions and support obligations to NRC stakeholders, with emphasis on information reporting and technical support requirements.
Agency Response Dated February 8, 2016:	Agree. Management Directive 12.5 and the OCIO Incident Response policy and procedure documents currently provide guidance for SOC functions, support obligations, roles and responsibilities. OCIO will review and update the OCIO Incident Response policy and procedures to more clearly define SOC functions and support obligations to NRC stakeholders with emphasis on information reporting and technical support requirements. **Target Completion Date**: September 30, 2016
OIG Analysis Dated July 28, 2016:	The proposed actions meet the intent of the recommendation. This recommendation will be closed when OIG receives verification that the SOC functions and support obligations to NRC stakeholders are defined to include information reporting and technical support requirements.
Status:	Resolved.
Agency Response Dated October 31, 2016:	Due to competing priorities, the staff has not yet updated OCIO Incident Response (IR) policy and procedure documents to more clearly define SOC functions and support obligations to NRC stakeholders with an emphasis on information reporting and technical support requirements. Two interim actions have been taken to address the finding. Management and staff have agreed that the SOC is responsible for security infrastructure monitoring and management and needs to have the ability to operate 24/7 and that the Computer Security Incident Response Team (CSIRT) is responsible for incident declaration in alignment with business and system owners, processes, security events, and incidents and is interdependent with the SOC. Also, the CIO and CISO now meet daily with the involved staff to ensure that all SOC related activities have been properly communicated and dispositioned. OCIO will update and revise the IR response policy and revise and develop clear SOC roles and responsibilities to support obligations to NRC stakeholders. OCIO would like to revise the target completion date to May 17, 2017. **Revised Target Completion Date**: May 17, 2017 **Point of Contact**: Thorne Graham, 301-415-7260

Audit of NRC's Network Security Operations Center (OIG-16-A-07)
Status of Recommendations

Recommendation 4: Revise the information technology services contract to align with agency policy defining SOC functions and support obligations to NRC stakeholders.

Agency Response Dated February 8, 2016: The current information technology service contract will be updated to incorporate the revision of the existing OCIO Incident Response policy and procedures (OIG Recommendation 3).

Target Completion Date: September 30, 2016

OIG Analysis Dated July 28, 2016: The proposed actions meet the intent of the recommendation. OIG will close this recommendation when NRC provides evidence that the contract has been revised to align with agency policy defining SOC functions and support obligations to NRC stakeholders.

Status: Resolved.

Agency Response Dated October 31, 2016: After further analysis, OCIO determined that it was most prudent to focus efforts on thoroughly defining SOC specific requirements to ensure alignment of SOC policies with obligations to support NRC stakeholders for inclusion in the follow-on information services contract. The current information technology service contract expires on May 17, 2017.

OCIO has updated the Information Technology Infrastructure (ITI) Service Level Agreements (SLAs) and memorandum of understandings (MOUs) with each office. This updating is a vehicle for communicating with stakeholders. For example, the ITI MOU with the Office of Nuclear Materials Safety and Safeguards (NMSS) (ADAMS Accession No. ML16165A287) provides an agreement that both OCIO and NMSS agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. Each party certifies that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and NRC policies.

Target Completion Date: May 17, 2017

Point of Contact: Michael Williams, 301-287-0660