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

OFFICE OF THE
INSPECTOR GENERAL

April 9, 2018

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF NRC'S NETWORK SECURITY OPERATIONS CENTER (OIG-16-A-07)

REFERENCE: CHIEF INFORMATION OFFICER, MEMORANDUM DATED MARCH 16, 2018

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated March 16, 2018. Based on this response, recommendations 1, 2, and 4 are closed. Recommendation 3 was closed previously. All recommendations related to this report are now closed.

If you have 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. Bowen, OEDO
J. Jolicoeur, OEDO
EDO_ACS Distribution

Audit Report

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 March 16, 2018:	The NRC Security operations Center (SOC) function has been divided into three distinct service areas, each with their own statement of work (SOW). SOC specific performance objectives have been incorporated into each SOW for each service area. The SOC is composed of SOC analysis and incident response (SOCAIR), SOC data exfiltration and email monitoring (SOC-DEEM) and SOC security engineering (SOC-ENG). SOC-AIR and SOCENG have been awarded under the new GLINDA contract and SOC-DEEM has been awarded under the Cyber Monitoring and Incident Response (CMIR) contract. Please refer to the following Agencywide Documents Access and Management System (ADAMS) SOW documents: SOC-AIR: ML18037B103 SOC-ENG: ML18037B105 SOC-DEEM: ML18037B104 **Target Completion Date: Completed**
OIG Analysis:	OIG reviewed the ADAMS documents and determined that the contract was revised to include SOC specific performance objectives. Therefore, this recommendation is considered closed.
Status:	Closed.

Audit Report

AUDIT OF NRC'S NETWORK SECURITY OPERATIONS CENTER

OIG-16-A-07

Status of Recommendations

Recommendation 2:	Revise information technology service contract requirements to define SOC functional requirements.
Agency Response Dated March 16, 2018:	The NRC SOC function has been divided into three distinct service areas, each with their own statement of work (SOW). SOC functional requirements have been incorporated into each SOW for each service area. The SOC is composed of SOC analysis and incident response (SOC-AIR), SOC data exfiltration and email monitoring (SOC-DEEM) and SOC security engineering (SOCENG). SOC-AIR and SOC-ENG have been awarded under the new GLINDA contract and SOC-DEEM has been awarded under the CMIR contract. Please refer to the following ADAMS SOW documents: SOC-AIR: ML18037B103 SOC-ENG: ML18037B105 SOC-DEEM: ML18037B104 **Target Completion Date: Completed**
OIG Analysis:	OIG reviewed the ADAMS documents and determined that the contract was revised to include SOC functional requirements. Therefore, this recommendation is considered closed.
Status:	Closed.

Audit Report

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 March 16, 2018:	The NRC SOC function has been divided into three distinct service areas, each with their own statement of work (SOW). Each SOC SOW is aligned with agency policy defining SOC service area functions and support obligations to NRC stakeholders. The SOC is composed of SOC analysis and incident response (SOC-AIR), SOC data exfiltration and email monitoring (SOC-DEEM) and SOC security engineering (SOCENG). SOC-AIR and SOC-ENG have been awarded under the new GLINDA contract and SOC-DEEM has been awarded under the CMIR contract. Please refer to the following ADAMS SOW documents: SOC-AIR: ML18037B103 SOC-ENG: ML18037B105 SOC-DEEM: ML18037B104 **Target Completion Date: Completed**
OIG Analysis:	OIG reviewed the ADAMS documents and determined that the contract was revised to align with agency policy defining SOC functions and support obligations to NRC stakeholders. Therefore, this recommendation is considered closed.
Status:	Closed.