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

OFFICE OF THE
INSPECTOR GENERAL

June 30, 2020

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF NUCLEAR REGULATORY COMMISSION'S (NRC) SHARED "S" DRIVE (OIG-11-A-15)

REFERENCE: OFFICE OF THE CHIEF INFORMATION OFFICER MEMORANDUM DATED APRIL 22, 2020

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated April 22, 2020. Based on this response, recommendations 2 and 3 from this report are now closed. Recommendations 1, 4, and 5 were closed previously. All recommendations related to this audit report are now closed.

If you have any questions or concerns, please call me at (301) 415-5915 or Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

cc: C. Haney, OEDO
D. Jackson, OEDO
J. Quichocho, OEDO
J. Jolicoeur, OEDO
S. Miotla, OEDO
RidsEdoMailCenter Resource
OIG Liaison Resource
EDO_ACS Distribution

Audit Report

AUDIT OF NRC'S SHARED "S" DRIVE

OIG-11-A-15

Status of Recommendations

Recommendation 2:	Revise current information security training for NRC staff to address specific practices for protecting Sensitive Unclassified Non-Safeguards Information (SUNSI) on the agency's shared network drives.
Agency Response Dated April 22, 2020:	In the August 15, 2019, memorandum, the OIG concluded that the proposed action provided on May 8, 2019, meets the intent of the recommendation and that this recommendation would be closed when OIG receives documentation verifying that training for NRC staff addresses protection of SUNSI on the agency's shared network drives. The effort to develop an NRC Controlled Unclassified Information (CUI) policy statement and accompanying guidance is still in progress. Management Directive (MD) 12.6 will provide guidance to staff to support the implementation of the NRC's CUI program once implemented. The Office of the Chief Information Officer (OCIO) anticipates additional delays with publishing the NRC CUI policy statement and draft MD 12.6 as a result of its efforts to resolve internal NRC comments. After MD 12.6 is published, agency-wide CUI training will be developed in coordination with the Office of the Chief Human Capital Officer (OCHCO). The NRC CUI Working Group began development of the CUI training module in December 2019. However, since NRC policy decisions will impact the final content of the CUI training module, this effort is not complete. Although the NRC has not transitioned to CUI, there is a current need for staff to receive training that addresses the protection of SUNSI on the agency's network drives. As a result, the NRC's annual Computer Security Awareness Training was updated in 2019 to address the protection of SUNSI on shared network drives (ADAMS Accession No. ML20084H788). The NRC believes that the intent of this recommendation has been completed.
OIG Analysis:	OIG verified the training documentation for NRC staff addressed protection of SUNSI within CUI on the agency's shared network drives. Therefore, this recommendation is now closed.
Status:	Closed

Audit Report

AUDIT OF NRC'S SHARED "S" DRIVE

OIG-11-A-15

Status of Recommendations

Recommendation 3:	Develop Controlled Unclassified Information (CUI) policies and guidance for storing and protecting CUI in agency shared drives, and: a. post this guidance on the NRC intranet; and b. include this guidance in annual training.
Agency Response Dated April 22, 2020:	As described in the response to Recommendation 2, OCIO's efforts to finalize the CUI policy statement and accompanying MD 12.6 have been delayed as a result of the agency's efforts to resolve internal comments on draft MD 12.6. As a result of the need to provide guidance to NRC staff on the storage and protection requirements for SUNSI on agency shared drives, OCIO issued YA-19-0102, "Policy Reminder of the U.S. Nuclear Regulatory Commission's policy for protecting sensitive Unclassified Non-Safeguards Information as Described In The NRC Policy For Handling, Marking, and Protecting Sensitive Unclassified Information and Applicable Management Directives," dated December 9, 2019. In YA-19-0102, the NRC staff is reminded of the need to protect SUNSI, including on shared network drives. A link to YA-19-0102 is included on the NRC's SUNSI webpage (https://drupal.nrc.gov/sunsi). This guidance was also included in the recent NRC annual Cybersecurity Training (ADAMS Accession No. ML20084H788). Guidance currently in place under SUNSI, in regard to the protection of SUNSI on shared agency network drives, will be transitioned to CUI policies and training. The draft version of MD 12.6 currently references MD 12.5, "NRC Cybersecurity Program." MD 12.5 already contains the agency requirements for the protection of information that is processed electronically and stored on shared agency drives (Refer to Section V.M.1.j (iv) in MD 12.5). The NRC believes that the intent of this recommendation has been completed.
OIG Analysis:	OIG verified CUI policies and guidance are developed, posted on the intranet, and included in biennial training. Therefore, this recommendation is now closed.
Status:	Closed