




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

November 15, 2021

MEMORANDUM TO: Eric Rivera
Acting Assistant Inspector General for Audits
Office of the Inspector General

FROM: Mirela Gavrilas, Director  Signed by Gavrilas, Mirela
Office of Nuclear Security and Incident Response on 11/15/21

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF U.S. NUCLEAR
REGULATORY COMMISSION'S SAFEGUARDS INFORMATION
LOCAL AREA NETWORK AND ELECTRONIC SAFE (OIG-13-A-16)

The U.S. Nuclear Regulatory Commission (NRC) staff is responding to your memorandum, "Status of Recommendations: Audit of NRC's Safeguards Information Local Area Network and Electronic Safe (OIG-13-A-16)," dated March 15, 2021 (Agencywide Documents Access and Management System Accession No. ML21074A007). This memorandum provides an update on the staff's planned actions for Recommendations 3 and 7. These actions reaffirm the original intent of providing a secure network for authorized users to access electronic Safeguards Information (SGI) documents in a centralized electronic document management system. Therefore, the staff believes that Recommendations 3 and 7 can be closed.

Recommendation 3:

Evaluate and update the current folder structure to meet user needs.

Current Status

The modernization of the Safeguards Information Local Area Network and Electronic Safe (SLES) system is complete; a draft revised folder structure was prepared and submitted to the Office of the Chief Information Officer (OCIO). The OCIO issued a task order to enable funds for Documentum, which is the database underpinning SLES. A Documentum security specialist will analyze the suggested changes under the Global Infrastructure and Development Acquisition contract that was awarded on September 30, 2020. Previous restrictions due to the Coronavirus Disease 2019 (COVID-19) have been lifted, which allows physical access to the SLES thin clients. The revised folder structure will result in increased user efficiencies (search and organization function) and reinforce least privilege access. OCIO will coordinate deployment of the solution to the SLES production and failover environments approximately 3 to 6 months post-validation in the test environment.

Staff point of contact for this recommendation: Bern Stapleton

Completed: November 15, 2021

CONTACT: Bern Stapleton, NSIR/DSO/ISB
(301) 415-2278

Recommendation 7:

Develop a structured access process that is consistent with the Safeguards Information (SGI) need-to-know requirement and least privilege principle. This should include:

- Establishing folder owners within SLES and providing the owners the authority to approve the need-to-know authorization (as opposed to branch chiefs).
- Conducting periodic reviews of user access to folders.
- Developing a standard process to grant user access.

Current Status

With respect to the SGI need-to-know requirement and least privilege principle, improvements have been made to training, validation of need and increased attention to user access. A policy has been established that requires all users to sign in every 90 days to maintain their access to SGI. The user community has significantly decreased from the initial 600+ users in 2015. The system's need-to-know access screens out 95 percent of NRC employees and contractors. Pre-COVID-19, there were 173 users of the system; however, many have been disabled due to not logging in. As of October 21, 2021, there were 96 users (90 regular users and 6 system administrators).

Assigning owners to file folders will be partially dependent upon implementation of the revised folder structure identified in recommendation 3. Currently, the SGI senior program manager revises and approves file folder access on an individual basis based on the needs and job position of the user. Periodic reviews of user access to folders are conducted to ensure proper access is maintained. Least privilege is accomplished through several steps, including training and completion of NRC Form 772, "Safeguards LAN and Electronic Safe (SLES) New User Account Creation and Account Reactivation Request Form for SLES Viewer." Form 772 requires the information systems security officer, branch chief and SGI senior program manager to verify and limit access based on need-to-know. This procedure applies to system administrators, users, and viewers.

Staff applies an acceptable risk management approach to ensure that individuals are properly trained on the SGI need-to-know requirement and least privilege principle. Specifically:

- Training of users/viewers emphasizes a need-to-know concept. There have been no known leaks of information from authorized users.
- The SLES system meets the intent of NRC Management Directive 12.1, "NRC Facility Security Program," definition of need-to-know (in person access vs. access to system).
- Security regarding access rights, least privilege and need-to-know of the SLES system is consistent with classified programs (GOLD, SIPRNet).

Staff point of contact for this recommendation: Bern Stapleton

Completed: November 15, 2021

STATUS OF RECOMMENDATIONS: AUDIT OF NRC'S SAFEGUARDS INFORMATION LOCAL AREA NETWORK AND ELECTRONIC SAFE (OIG-13-A-16) DATE November 15, 2021

DISTRIBUTION:

BStapleton, NSIR/DSO/ISB

DParsons, NSIR/DSO/ISB

SLee, NSIR

CRobb, OCIO/ITSDOD/DTSB/SST

KDunbar, OCIO/ITSDOD/DTSB

MGavrilas, NSIR

RidsOigMailCenterResource, OIG

RidsEdoMailCenterResource, OEDO

JJolicoeur, OEDO

GButler, OIG/AIGA

RidsNsirMailCenter Resource (RidsNsirMailCenter Resourc

ADAMS Accession No.: Memo ML21309A028

OFFICE	NSIR/DSO/ISB	NSIR/DSO/ISB	OCIO/ITSDOD /DTSB/SST	OCIO/ITSDOD /DTSB
NAME	BStapleton <i>BS</i>	DParsons <i>DP</i>	CRobb <i>CR</i>	KDunbar <i>KD</i>
DATE	Nov 5, 2021	Nov 5, 2021	Nov 8, 2021	Nov 8, 2021
OFFICE	NSIR	NSIR		
NAME	SLee <i>SL</i>	MGavrilas <i>MG</i>		
DATE	Nov 9, 2021	Nov 15, 2021		

OFFICIAL RECORD COPY