



MEMORANDUM

DATE: June 15, 2023

TO: Daniel H. Dorman
Executive Director for Operations

David J. Nelson
Chief Information Officer

FROM: Hruta Virkar */RA/*
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT
EVALUATION OF NRC'S POTENTIAL COMPROMISE OF
SYSTEMS (SOCIAL ENGINEERING)
(OIG-20-A-09)

REFERENCE: CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF
INFORMATION OFFICER, MEMORANDUM DATED
JANUARY 4, 2023

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendations as discussed in the agency's response dated January 4, 2023. Based on this response, recommendations 9 and 11 remain open and resolved and recommendation 3 is closed. In addition, recommendations 1-2, 4-8, 10, and 12-13 were closed in a previous response. Please provide an update on the status of these resolved recommendations by **January 31, 2024**.

If you have questions or concerns, please call me at 301.415.5915 or Terri Cooper, Team Leader, at 301.415.5965.

Attachment:
As stated

cc: M. Bailey, AO
M. Meyer, DAO
J. Jolicoeur, OEDO
OIG Liaison Resource
EDO_ACS Distribution

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S POTENTIAL COMPROMISE OF
SYSTEMS (SOCIAL ENGINEERING)
Status of Recommendations
(OIG-20-A-09)

Recommendation 3: Within the next year, perform follow-on telephone tests to gauge the efficacy of the updated training.

Agency Response

Dated January 4, 2023:

The NRC performed an initial analysis and found that there were significant challenges associated with conducting telephone tests, also known as vishing. Among the challenges are a lack of available vendors and the risk of causing unintended emotional responses from the recipients of test phone calls. In addition, in the more than 2 years since this finding was identified, the use of agency office phones has dramatically decreased as a result of the agency's current telework policy and the increased reliance on Microsoft Teams for voice communication. This decrease in telephone use represents a commensurate decrease in the overall risk to the agency from this type of attack. However, the NRC has recently increased its vishing training and awareness activities in formats such as its annual Computer Security Awareness Training, periodic postings to Teams and SharePoint sites, and in several agencywide "Lunch Byte" seminars.

The NRC recommends Recommendation 3 be closed.

OIG Analysis:

The agency's corrective actions described above appear reasonable and meet the intent of the recommendation. This recommendation is therefore closed.

Status:

Closed.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S POTENTIAL COMPROMISE OF
SYSTEMS (SOCIAL ENGINEERING)
Status of Recommendations
(OIG-20-A-09)

Recommendation 9: Within the next year, perform follow-on checks to determine if passwords are being protected.

Agency Response

Dated January 4, 2023:

As part of its Operation Security (OpsSec) program, which is owned by the Office of Administration, the NRC will perform monthly checks to ensure NRC personnel are not writing passwords onto note cards, sticky notes or other open, visible surfaces. These checks will be conducted at the NRC's Headquarters, Regions I, II, III, IV and TTC locations.

Target Completion Date: FY 2023 Q2

OIG Analysis:

The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the OIG verifies that the NRC has performed follow-on checks to determine if passwords are being protected.

Status:

Open: Resolved.

Evaluation Report
INDEPENDENT EVALUATION OF NRC'S POTENTIAL COMPROMISE OF
SYSTEMS (SOCIAL ENGINEERING)
Status of Recommendations
(OIG-20-A-09)

Recommendation 11: Perform periodic spot checks for employees away during the 15-minute window before the screen locks to ensure that PCs are being protected from unauthorized viewing.

Agency Response

Dated January 4, 2023: As part of its Operation Security (OpsSec) program, which is owned by the Office of Administration, the NRC will perform monthly spot checks to ensure that NRC personnel have locked their workstation screens while unattended to prevent unauthorized viewing and network access. These checks will be conducted at the NRC's Headquarters, Regions I, II, III, IV, and TTC locations.

Target Completion Date: FY 2023 Q2

OIG Analysis: The proposed actions meet the intent of the recommendation. The OIG will close the recommendation when the NRC performs periodic spot checks for employees away during the 15-minute window before the screen locks to ensure that PCs are being protected from unauthorized viewing.

Status: Open: Resolved.