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

OFFICE OF THE
INSPECTOR GENERAL

April 30, 2009

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: AUDIT OF NRC'S LAPTOP MANAGEMENT (OIG-08-A-19)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE, MEMORANDUM DATED APRIL 14, 2009

Attached is the Office of the Inspector General's analysis and status of recommendations 1, 2, 3, 4, and 5 as discussed in the agency's response dated April 14, 2009. Based on this response, recommendations 1 and 2 are closed. Recommendations 3, 4, and 5 remain in resolved status. Please provide an updated status of the resolved recommendations by October 15, 2009.

If you have any questions or concerns, please call me at 415-5915 or Beth Serepca, Team Leader, at 415-5911.

Attachment: As stated

cc: V. Ordaz, OEDO
J. Arildsen, OEDO
P. Shea, OEDO

Audit Report

AUDIT OF NRC'S LAPTOP MANAGEMENT

OIG-08-A-19

Status of Recommendations

Recommendation 1: Develop agencywide policy and procedures regarding the implementation and monitoring of security controls, especially concerning virus protection and operating system updates, for all agency-owned laptop computers.

Agency Response Dated April 14, 2009: NRC has developed the following:

- Configuration standards for NRC laptops and provided them on the Computer Security Office (CSO) web page at:

  http://www.internal.nrc.gov/CSO/standards.html

- Standard system security plans for NRC laptops and provided them on the CSO web page at:

  http://www.internal.nrc.gov/CSO/Classified.html
  http://www.internal.nrc.gov/CSO/SGI.html
  http://www.internal.nrc.gov/CSO/General.html

- Laptop security policy provided via memo to office directors and regional administrators and yellow announcement to staff (ML090120759). The policy is also available via the CSO web page at:

  http://www.internal.nrc.gov/CSO/policies.html

This recommendation should be closed.

OIG Analysis: OIG reviewed the agencywide policy and procedures described above. These documents provide guidance on implementation and monitoring of security controls, including virus protection and operating system updates. This recommendation is therefore considered closed.

Status: Closed.

Audit Report

AUDIT OF NRC'S LAPTOP MANAGEMENT

OIG-08-A-19

Status of Recommendations

Recommendation 2: Communicate the policy in recommendation 1 to the agency when initially complete. Send periodic reminders of the policy requirements, as well as detailed instructions on how to fulfill the requirements.

Agency Response Dated April 14, 2009: NRC provided the laptop security policy via memo to office directors and regional administrators and yellow announcement to staff (ML090120759). The policy requires use of the configuration standards and standard system security plans. The policy is also available via the CSO web page at:

http://www.internal.nrc.gov/CSO/policies.html

This recommendation should be closed.

OIG Analysis: OIG reviewed the laptop security policy memorandum to office directors and regional administrators, as well as the yellow announcement to staff, and determined these documents effectively communicate the laptop security policy. OIG also reviewed EDATS Number OEDO-2009-0227 to verify that annual reminders of laptop security responsibilities will be sent to NRC staff and contractors. This recommendation is therefore considered closed.

Status: Closed.

Audit Report

AUDIT OF NRC’S LAPTOP MANAGEMENT

OIG-08-A-19

Status of Recommendations

Recommendation 3: Provide mandatory formal training to all IT coordinators and property custodians on how to update security controls on laptops.

Agency Response Dated April 14, 2009: NRC is developing a course for system administrators and ISSOs. At least one instance of the course will be offered by July 1, 2009, and two more will be offered before the end of the fiscal year.

OIG Analysis: The proposed action meets the intent of the recommendation. This recommendation will be closed when OIG receives documentation that mandatory formal training for system administrators and Information System Security Officers has been provided and determines that the training contained directions on how to update the security controls on laptops.

Status: Resolved.

Audit Report

AUDIT OF NRC'S LAPTOP MANAGEMENT

OIG-08-A-19

Status of Recommendations

Recommendation 4: Develop a process for verifying that all required security controls are implemented on agency-owned laptops.

Agency Response
Dated April 14, 2009: NRC is finalizing development of a quarterly Federal Information Security Management Act (FISMA) compliance review process. This process requires meeting and auditing at the System Level and/or Program Office level to discuss specific agenda items regarding a system, common issues that impact a number of systems, and verification of security controls for PCs and laptops. CSO expects to finalize process in the 4th quarter of FY 2009.

OIG Analysis: The proposed action meets the intent of this recommendation. This recommendation will be closed when OIG receives documentation of the FISMA compliance review process and determines that it will verify that all required security controls are implemented for the agency-owned laptops.

Status: Resolved.

Audit Report

AUDIT OF NRC'S LAPTOP MANAGEMENT

OIG-08-A-19

Status of Recommendations

Recommendation 5: Develop a protocol to facilitate the efficient and routine updating of agency-owned laptops located at headquarters.

Agency Response
Dated April 14, 2009: NRC is on track to develop the protocol.

OIG Analysis: This recommendation will be closed when OIG receives the protocol and determines that it facilitates the efficient and routine updating of agency-owned laptops located at headquarters.

Status: Resolved.