



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

OFFICE OF THE
INSPECTOR GENERAL

October 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: SYSTEM
EVALUATION OF SECURITY CONTROLS FOR
STANDALONE PERSONAL COMPUTERS AND LAPTOPS
(OIG-05-A-18)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE,
MEMORANDUM DATED OCTOBER 8, 2009

Attached is the Office of the Inspector General's analysis and status of recommendations 2, 3, 4, 5, and 6 as discussed in the agency's response dated October 8, 2009. Based on this response, recommendations 3 and 6 remain resolved. Recommendations 2, 4, and 5 are closed. Recommendations 1, 7, and 8 were previously closed. Please provide an updated status of the resolved recommendations by June 5, 2010.

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: N. Mamish, OEDO
J. Andersen, OEDO
J. Arildsen, OEDO
C. Jaegers, OEDO

Audit Report

SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS

(OIG-05-A-18)

Status of Recommendations

Recommendation 2: Develop and require users to sign a rules of behavior agreement accepting responsibility for implementing security controls on standalone PCs and laptops.

Agency Response Dated
October 8, 2009: NRC Agency-wide Rules of Behavior for Authorized computer Use were provided as part of the annual computer security awareness course. As part of the course completion, users were required to electronically acknowledge the rules of behavior.

OIG Analysis: The OIG's FISMA contractor reviewed the NRC Agency-wide Rules of Behavior for Authorized Computer Use and determined they specify user level rules for the secure use of all computing resources used to process or store sensitive NRC information. The rules apply to all NRC non-public users of NRC computing resources. Computing resources are defined as computers and IT resources, including desktop and laptop computers, networks, facilities, printers, scanners, faxes, PEDs, cell phones, electronic media, printouts, and any other IT used to store or process information. Non-public users are defined as NRC employees and support contractors at their primary workplace and at any alternative workplaces (e.g., teleworking from home or from a satellite site) and users on official travel. The rules state that users of NRC computing resources used to process NRC information or to connect to NRC systems shall implement security controls as directed by NRC policy and procedures. Users must acknowledge their responsibilities when using NRC IT resources in accordance with these rules by agreeing to the rules of behavior acknowledgement statement at the end of the annual computer security awareness course. This recommendation is closed.

Status: Closed.

Audit Report

SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS

(OIG-05-A-18)

Status of Recommendations

Recommendation 3: Develop and implement procedures for verifying all required security controls are implemented on standalone PCs and laptops.

Agency Response Dated
October 8, 2009:

The compliance review process is currently going through coordination and review. 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 1st quarter of FY2010 and begin new quarterly compliance review process 2nd quarter of FY2010.

OIG Analysis:

The proposed action addresses the intent of OIG's recommendation. This recommendation will be closed when the compliance review process is implemented and corresponding procedures are made available to the OIG for review and verification.

Status:

Resolved.

Audit Report

SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS

(OIG-05-A-18)

Status of Recommendations

Recommendation 4: Provide users guidance on compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops.

Agency Response Dated
October 8, 2009: The standard rules of behavior include statements regarding compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. The rules of behavior were electronically acknowledged as part of the computer security awareness course.

OIG Analysis: OIG's FISMA contractor reviewed the computer security awareness course and determined that the users were provided guidance on compliance. Therefore, this recommendation is considered closed.

Status: Closed.

Audit Report

SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS

(OIG-05-A-18)

Status of Recommendations

Recommendation 5: Develop and require users to sign a rules of behavior agreement acknowledging their compliance with Executive Order 13103, Computer Security Piracy, for standalone PCs and laptops.

Agency Response Dated
October 8, 2009: The standard rules of behavior include statements regarding compliance with Executive Order 13103, Computer Software Piracy, for standalone PCs and laptops. Once the rules of behavior are distributed and signed, this recommendation should be closed.

OIG Analysis: The OIG's FISMA contractor reviewed the NRC Agency-wide Rules of Behavior for Authorized Computer Use and determined they provide users guidance on compliance with Executive Order 13103. The rules state that users shall abide by Executive Order 13103 and U.S. copyright laws when using NRC systems, and shall not acquire, install, reproduce, distribute, or transmit computer software in violation of applicable copyright laws. Users must acknowledge their responsibilities when using NRC IT resources in accordance with these rules by agreeing to the rules of behavior acknowledgement statement at the end of the annual computer security awareness course. This recommendation is therefore considered closed.

Status: Closed.

Audit Report

SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS

(OIG-05-A-18)

Status of Recommendations

Recommendation 6: Develop and implement procedures for monitoring compliance with Executive Order 13103, Computer Security Piracy, for standalone PCs and laptops.

Agency Response Dated
October 8, 2009:

The compliance review process is currently going through coordination and review. 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 1st quarter of FY2010 and begin new quarterly compliance review process 2nd quarter of FY2010.

OIG Analysis:

The proposed action addresses the intent of OIG's recommendation. This recommendation will be closed when the compliance review process is implemented and corresponding procedures are made available to the OIG for review and verification.

Status:

Resolved.