



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

OFFICE OF THE
INSPECTOR GENERAL

November 4, 2009

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INDEPENDENT
EVALUATION OF NRC'S IMPLEMENTATION OF THE
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOR FISCAL YEAR 2008 (OIG-08-A-18)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE,
MEMORANDUM DATED OCTOBER 9, 2009

Attached is the Office of the Inspector General's analysis and status of recommendations 1, 2, 3, and 4 as discussed in the agency's response dated October 9, 2009. Based on this response, recommendations 1, 2, and 4 are resolved. Recommendation 3 is now closed. Please provide an updated status of the resolved recommendations by March 31, 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. Arlidsen, OEDO
C. Jaegers, OEDO

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 1: Update the U.S. Nuclear Regulatory Commission (NRC) System Information Control Database to identify all interfaces between systems.

Agency Response Dated
October 9, 2009: CSO in coordination with OIS has ensured that the NSICD system has been updated to identify interfaces for systems listed in the inventory and this recommendation has been completed. CSO requests that this recommendation be closed. Completed June 15, 2009.

OIG Analysis: The actions do not fulfill the intent of the recommendation. The OIG analyzed the interface information in NSICD and while there is more interface information present that was found during the FY 2008 independent evaluation, the information is still incomplete and inconsistent. This recommendation remains resolved until the agency corrects the inconsistencies that still exist in the inventory information in NSICD.

Status: Resolved.

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 2: Develop and implement procedures to ensure interface information in the NRC System Information Control Database is consistent with interface information in security plans and risk assessments.

Agency Response Dated
October 9, 2009:

CSO has developed and implemented procedures for security information and interfaces are consistent with information in corresponding system security plans and risk assessments. CSO requests that this recommendation be closed. Completed June 15, 2009.

OIG Analysis:

The actions do not fully accomplish the intent of the recommendation. The OIG analyzed the guide that was developed for the Computer Security Office's (CSO) administrative staff for entering data into security records within NSICD to ensure interface information is consistent with interface information in security plans and risk assessments. While the document includes guidance on entering interface information into NSICD, it suggests obtaining this information from either the system's security categorization or risk assessments. These documents are not updated on a period basis, so the interface information found in these documents may not be current. The OIG also found that some security plans, which are required to be updated at least annually, did not include interface details, but referred the reader to other documents, which in some cases were not as current as the security plans. As a result, the interface information obtained from the security categorizations, risk assessments, and some security plans, did not reflect the actual interfaces for the system. This recommendation should remain resolved until the procedures developed to ensure interface information in NSICD is consistent with interface information in security

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 2 (continued):

plans and risk assessments are further refined. The OIG suggests that the agency add additional guidance to the procedures on where to find current interface information, as well as how to ensure interface information remains consistent within NSICD.

Status: Resolved.

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 3: Develop agencywide policy and procedures regarding the implementation and monitoring of Federal Desktop Core Configuration controls for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless whether or not they are connected to the agency's network.

Agency Response Dated
October 9, 2009:

CSO in coordination with OIS has developed the following:

– Configuration standards for NRC laptops and provided them on the CSO web page at:

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

– Guidance for general laptops and provided them on the CSO web page at:

<http://www.internal.nrc.gov/CSO/guidelines.html>

– Procedures for applying critical updates to Safeguards Information (SGI) laptops and provided them on the CSO web page at:

<http://www.internal.nrc.gov/CSO/procedures.html>

– An SGI Stand Alone Listed System Minimum Security Checklist to ensure appropriate laptop configuration and provided them on the CSO web page at

<http://www.internal.nrc.gov/CSO/checklists.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>

Additionally, all computers connected to the NRC network receive FDCC settings through the use of Group Policy Object (GPO) objects settings. Computers that are not attached to the network are loaded with these controls as

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 3 (continued):

part of the standard configuration image and additional controls are implemented through Local Security Policy. These controls were implemented June 15, 2009. CSO recommends that this recommendation be closed. Completed June 15, 2009.

OIG Analysis:

The OIG's FISMA contractor reviewed the configuration guidance, procedures, configuration standards, and standard system security plans for laptops developed by the CSO, as well as the new *Laptop Security Policy*. The laptop standards and the Laptop Security Policy require the application of current FDCC security policies to all laptops that are not used as desktops, or are used for safeguards information or classified national security information. Computers that are not attached to the network (standalone systems) are loaded with these controls as part of the standard configuration image and additional controls are implemented through local security policy. All computers connected to the NRC network receive FDCC settings through the use of group policy object settings. This recommendation is therefore closed.

Status:

Closed.

Audit Report

INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008

OIG-08-A-18

Status of Recommendations

Recommendation 4: Develop a process for verifying that all Federal Desktop Core Configuration controls are implemented for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.

Agency Response Dated
October 09, 2009:

The NRC has deployed the Security Content Automation Protocol (SCAP) scanners to verify that the agency is compliant with M-08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)" during the system certification and accreditation process. The CSO is currently fielding its Information Assurance System to provide real-time assessment of FDCC compliance for networked computers as part of its continuing monitoring assurance activities. Standalone systems are configured to FDCC standards during computer build-out. This recommendation is partially closed pending the completion of the IAS which is necessary for the NRC to provide agency wide, real-time FDCC assessments. The system is currently scheduled for completion by September 30, 2010.

OIG Analysis:

The proposed action addresses the intent of this recommendation. This recommendation will be closed when OIG verifies that the agency has completed the IAS which is necessary for NRC to provide agencywide real-time FDCC assessments.

Status:

Resolved.