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

OFFICE OF THE
INSPECTOR GENERAL

February 26, 2010

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: STATUS OF RECOMMENDATIONS: INFORMATION SYSTEM SECURITY EVALUATION OF THE TECHNICAL TRAINING CENTER – CHATTANOOGA, TENNESSEE (OIG-09-A-11)

REFERENCE: DIRECTOR, COMPUTER SECURITY OFFICE, MEMORANDUM DATED JANUARY 21, 2010

Attached is the Office of the Inspector General's analysis and status of recommendations 1 - 8 as discussed in the agency's response dated January 21, 2010. Based on this response, recommendations 1, 2, 5, 7, and 8 are closed and recommendations 3, 4, and 6 remain in resolved status. Please provide an updated status of the resolved recommendations by June 30, 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

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

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 1: Provide comprehensive training on the Technical Training Center's (TTC) new physical access control systems as soon as possible. The agency should not wait until the Division of Facilities and Security (DFS) returns to install the TTC's badge access system.

Agency Response Dated January 21, 2010: On August 27, 2009, DFS has provided additional training on the new physical access control system for all TTC system administrators. This training was comprehensive and included all administrator duties.

Recommend this item be closed.

OIG Analysis: OIG spoke with CSO concerning the training given and determined that the training conducted as well as the written guidance met the intent of the recommendation. This recommendation is therefore closed.

Status: Closed.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 2: Provide comprehensive documentation on the TTC's new physical access control systems as soon as possible. The agency should not wait until the DFS returns to install the TTC's badge access system server.

Agency Response Dated January 21, 2010: DFS provided written guidance on the use of the new physical access control system to staff with a need to know and it was explained that the information may also be downloaded off the internet site. A copy of the guidance is available in the "Facility Commander Wnx User Manual" which has been placed into ADAMS under Accession No. ML100151003.

Recommend this item be closed.

OIG Analysis: OIG reviewed the user manual and determined that is comprehensive and readily available on the Internet site as well as ADAMS. This recommendation is therefore closed.

Status: Closed.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

<u>Recommendation 3</u>: Complete the hardening of the TTC’s badge access system server and install it at the TTC.

Agency Response Dated January 21, 2010: The certification and accreditation "hardening" process was completed and an Authority to Operate for ACCESS system was issued November 30, 2009.

The system is being migrated into the production environment, with completion of the TTC server final configuration and installation expected on or before March 31, 2010.

Estimated Completion Date: March 31, 2010.

OIG Analysis: The corrective action addresses the intent of this recommendation. OIG confirmed that the hardening occurred. This recommendation will be closed when OIG receives documentation that the system was installed at the TTC.

Status: Resolved.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 4: Activate the TTC's intrusion detection system to sound a local audible alarm until the agency can coordinate with the Federal Protective Service to monitor the alarms.

Agency Response Dated January 21, 2010: An agreement has been coordinated with the Federal Protective Service. A copy of the TTC Mega-Center Alarm Requirement document that was sent to the Federal Protective Service is available in ADAMS under Accession No. ML100150995. Note that the document has been redacted to prevent disclosure of system passwords, pin numbers and specific configuration information. TTC is currently developing arming control and response procedures.

Estimated Completion Date: June 30, 2010.

OIG Analysis: The corrective action addresses the intent of this recommendation. OIG acknowledges that the agreement was reached with the Federal Protective Service to monitor the alarms. This recommendation will be closed when OIG receives a copy of the arming control and response procedures.

Status: Resolved.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 5: Develop and implement procedures for storing information system backup information offsite in a location, cabinet, or safe that is waterproof and fireproof for at least 14 days or as recommended by the agency.

Agency Response Dated January 21, 2010: The TTC is currently sending backups of all other data to an offsite location. The media used is an encrypted hard drive, utilizing PGP whole disk encryption. The LAN Administrator has added one more backup job to the Arcserve backup system. This job is a duplicate of the current MS Exchange backup. The media used is a hard drive attached to the Arcserve backup server. On a weekly basis, the backup is being copied from the hard drive to the same encrypted media that is currently being used for other offsite data storage.

Recommend this item be closed.

OIG Analysis: OIG spoke with the TTC LAN administrator regarding the development and implementation of these procedures for storing the backup information and determined that the procedures are in place to store the backups at an offsite location for the duration recommended by the agency. This recommendation is therefore closed.

Status: Closed.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 6: Fully develop and implement backup procedures for the badge access system.

Agency Response Dated January 21, 2010: Additional training for the interim backup guidance was provided, however once the regional server is installed and communicating with the global server at HQ, this procedure will be performed automatically. The system backup procedures are documented in the **“**Facility Commander Wnx Installation Manual.**”** This document has been placed into ADAMS under Accession No. ML100151046.

Estimated Completion Date: March 31, 2010.

OIG Analysis: OIG reviewed the installation manual and determined that it fully documents the backup procedures. Training was provided on how to implement the guidance. OIG will close this recommendation once the regional server is installed and the procedure will be performed automatically.

Status: Resolved.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 7: Evaluate the vulnerabilities identified by the network vulnerability assessment and develop a plan and schedule to identify any false positives and to resolve the remaining vulnerabilities.

Agency Response Dated January 21, 2010: **Dormant Accounts** – The scan identified 48 accounts on the server that have never been logged in.

These accounts were identified as active directory accounts, not local server accounts. All of these accounts are outside of the TTC active directory container and therefore outside the purview of the TTC.

Minimum password age – The scan identified a server with a minimum password age policy set to 0 days.

The local TTC LAN Administrators do not have the rights to make changes to any of the Windows server policies. This is done at a higher level by members of the Network Operations Center at headquarters.

Accounts with passwords that do not expire – The scan identified 15 accounts on one server with passwords that do not expire. These accounts were identified as active directory accounts, not local server accounts. All of these accounts are outside of the TTC active directory container and therefore outside the purview of the TTC.

Guessed password – The scan was able to guess the password on one account (it was the same as the account name).

The account was identified as an Active Directory account, not a local server account. This account is outside of the TTC Active Directory container and therefore outside the purview of the TTC.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 7 (continued)

SSL certificate issues – The scan identified multiple servers and devices with SSL certificate issues. The scan found SSL certificates that are self-signed and where the subject and target of the certificate do not match. The scan also found SSL certificates that accept weak ciphers and accepts the SSLv2 protocol.

All servers and devices contain numerous SSL certificates. The scan report did not identify which SSL certificate(s) it found these issues on. The time and effort required to identify and correct the problem certificates relative to the marginal security risk they pose is not justified.

Recommend this item be closed.

OIG Analysis: OIG and its contractor who conducted the TTC evaluation reviewed the information provided regarding the vulnerabilities identified and determined that the vulnerabilities were identified and resolved. This recommendation is therefore closed.

Status: Closed.

Audit Report

Information System Security Evaluation of the Technical Training Center – Chattanooga, Tennessee

OIG-09-A-11

Status of Recommendations

Recommendation 8: Perform a network vulnerability scan following remediation to verify all vulnerabilities have been resolved.

Agency Response Dated January 21, 2010: As to the remaining items on the scan, the TTC LAN administrator has analyzed each device. Confirmed vulnerabilities have been fixed when possible on each device. Inferred vulnerabilities will be assessed and determinations will be made on how and if any action could and should be taken.

In addition to the Saint scan that was performed earlier, the TTC has, under approval on TCR # 4761, run its own internal NESSUS security scan of its network segment. Results from this scan have been reviewed by the LAN administrator. Vulnerabilities found have been corrected where possible on each device.

Recommend this item be closed

OIG Analysis: OIG and its contractor who conducted the TTC evaluation reviewed the information provided regarding the Saint scan and the NESSUS security scan and determined that the confirmed vulnerabilities were fixed where possible. This recommendation is therefore closed.

Status: Closed.