AUDIT REPORT

Audit of NRC's Deployment of the National Source Tracking System

OIG-10-A-16 August 30, 2010

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

OFFICE OF THE
INSPECTOR GENERAL

August 30, 2010

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S DEPLOYMENT OF THE NATIONAL SOURCE TRACKING SYSTEM (OIG-10-A-16)

Attached is the Office of the Inspector General's (OIG) audit report titled, *NRC's Deployment of the National Source Tracking System.*

This report presents the results of the subject audit. Agency comments provided during a July 28, 2010, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915 or Beth Serepca, Team Leader, at 415-5912.

Attachment: As stated

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee
on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety
and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Hubert T. Bell, Inspector General
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Michael F. Weber, Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director
for Corporate Management, OEDO
Martin J. Virgilio, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Nader L. Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Office
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
and Environmental Management Programs
Cheryl L. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Catherine Haney, Director, Office of Nuclear Material Safety
and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
James T. Wiggins, Director, Office of Nuclear Security
and Incident Response
Marc L. Dapas, Acting Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

EXECUTIVE SUMMARY

NATIONAL SOURCE TRACKING SYSTEM OVERVIEW

The National Source Tracking System (NSTS) is a centralized database developed and managed by the Nuclear Regulatory Commission (NRC) to help NRC and Agreement State regulatory agencies[1] account for select categories of high-risk radiological sources held by approximately 1,300 licensees.[2] Specifically, NSTS is used to monitor transactions and inventories of nationally tracked sources as defined in Title 10 of the Code of Federal Regulations, Part 20, Section 1003 (10 CFR 20.1003).[3] These nationally tracked sources include Category 1 and 2 radiological sealed sources[4] that have industrial, medical, and research uses.[5] The International Atomic Energy Agency (IAEA) characterizes Category 1 and 2 sources as radiological materials that pose the greatest health risks if not safely managed or securely protected.[6]

NRC developed NSTS in response to the U. S. Government's endorsement of the *IAEA Code of Conduct on the Safety and Security of Radioactive Sources,* which is the current standard used by the

[1] The Atomic Energy Act of 1954 allows NRC to delegate to State governments some authority to license and regulate radiological materials. States that have signed formal regulatory agreements with NRC are known as "Agreement States."

[2] Licensees are businesses and other organizations licensed by NRC and Agreement States to possess radiological sources.

[3] 10 CFR 20.1003 defines a nationally tracked source as, "a sealed source containing a quantity equal to or greater than Category 1 or Category 2 levels of any radioactive material listed in Appendix E of this part. In this context a sealed source is defined as radioactive material that is sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It does not mean material encapsulated solely for disposal, or nuclear material contained in any fuel assembly, subassembly, fuel rod, or fuel pellet. Category 1 nationally tracked sources are those containing radioactive material at a quantity equal to or greater than the Category 1 threshold. Category 2 nationally tracked sources are those containing radioactive material at a quantity equal to or greater than the Category 2 threshold but less than the Category 1 threshold."

[4] A table of radiological sources subject to NSTS reporting appears in Appendix A.

[5] These sources do not include materials encapsulated solely for disposal, or nuclear materials contained in fuel assemblies, subassemblies, fuel rods, or fuel pellets.

[6] The IAEA's five-category scale provides a relative ranking of radiological sources in terms of each source's potential to cause immediate harmful health effects if not safely managed or securely protected. Category 1 sources are the most hazardous, and can cause permanent injury or death if mishandled; Category 5 sources are the least hazardous, and could not cause permanent injury.

international community to govern safety and security of radioactive material based on the IAEA categorization system.[7] In addition, the Energy Policy Act of 2005 required NRC to issue regulations establishing a mandatory tracking system for radiation sources in the United States. NRC deployed NSTS in December 2008, thereby enabling licensees to begin reporting radiological source inventories and transactions by January 31, 2009, as required by Title 10 of the Code of Federal Regulations, Part 20, Section 2207.

NSTS enables licensees to report via the Internet transactions of nationally tracked sources, including the manufacture, import, export, transfer, and receipt of these sources.[8] Licensees can also report transaction data by other means such as facsimile, e-mail, or standard mail. Approximately 200 source transactions are processed daily in NSTS.

PURPOSE

The audit's objective was to determine if the National Source Tracking System meets its required operational capabilities.

RESULTS IN BRIEF

NSTS satisfies basic operational requirements, including functional capabilities for capturing data and security features for protecting data. However, Office of the Inspector General (OIG) auditors developed findings regarding NSTS smart card utilization, data quality, and access controls.

Licensees Have Not Fully Adopted NSTS Technology

NSTS was designed primarily to be an Internet-based system enabling direct data entry by licensees. However, a majority of the licensee user

[7] A joint Department of Energy /NRC Interagency Working Group on Radiological Dispersal Devices also recommended a national source tracking system following its work during 2002-2003.

[8] The Energy Policy Act of 2005 established requirements for identifying individual radiological sources (e.g., by serial number), and for reporting any change of possession or loss of control of these materials. In addition, this legislation required a capability for reporting through a secure Internet connection.

population has not fully adopted technology required for direct access to NSTS. This trend is caused by challenges inherent in the NSTS credentialing process, as well as technical problems encountered by licensees in using the smart card devices. Further, Help Desk contractor personnel are not always capable of resolving application and set-up problems encountered by NSTS users. As a result, NRC has incurred administrative costs from updating NSTS on behalf of licensees who opt not to enter their source transaction and inventory data into NSTS.

NSTS Has Data Quality Problems with Timeliness and Accuracy

Internal control standards for Federal Government agencies recommend that data be processed in a timely manner to maintain its relevance and operational value to management. NSTS is designed with automated security controls to ensure the integrity of data entered into the system; however, OIG auditors found problems with the timeliness of NSTS data regarding source transfers. These problems result primarily from the process by which data is reported and manually uploaded into NSTS. Although NSTS cannot provide "real time" tracking of licensees' source transactions and inventories, NRC and Agreement State personnel must have reliable information to perform their oversight duties.

Least Privilege Principle Not Consistently Applied to NSTS Access Controls

Federal Government internal controls standards for information systems recommend security controls to protect systems and networks from inappropriate access and unauthorized use. Although NSTS access rights for licensee personnel are scaled to individual users' job needs, some NRC staff have broader access rights that do not reflect individuals' job needs or organizational roles. This occurs because NRC lacks a procedure for scaling staff access rights to their respective job needs. Although OIG auditors did not find evidence of internal NSTS data breaches, the lack of a procedure to ensure consistent application of the least privilege principle increases the risk that NSTS data could be intentionally or accidentally compromised.

RECOMMENDATIONS

This report makes four recommendations. A consolidated list of recommendations appears in Section IV of this report.

AGENCY COMMENTS

At an exit conference held on July 28, 2010, agency management stated their general agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

ABBREVIATIONS AND ACRONYMS

CFR	Code of Federal Regulations
CSO	Computer Security Office
FSME	Office of Federal and State Materials and Environmental Management Programs
FTE	Full Time Equivalent
IAEA	International Atomic Energy Agency
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSTS	National Source Tracking System
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget

TABLE OF CONTENTS

I. BACKGROUND

National Source Tracking System Overview

The National Source Tracking System (NSTS) is a centralized database developed and managed by the Nuclear Regulatory Commission (NRC) to help NRC and Agreement State regulatory agencies[9] account for select categories of high-risk radiological sources held by approximately 1,300 licensees.[10] Specifically, NSTS is used to monitor transactions and inventories of nationally tracked sources as defined in Title 10 of the Code of Federal Regulations, Part 20, Section 1003 (10 CFR 20.1003).[11] These nationally tracked sources include Category 1 and 2 radiological sealed sources[12] that have industrial, medical, and research uses.[13] The International Atomic Energy Agency (IAEA) characterizes Category 1 and 2 sources as radiological materials that pose the greatest health risks if not safely managed or securely protected.[14]

NRC developed NSTS in response to the U. S. Government's endorsement of the *IAEA Code of Conduct on the Safety and Security of Radioactive Sources,* which is the current standard used by the

[9] The Atomic Energy Act of 1954 allows NRC to delegate to State governments some authority to license and regulate radiological materials. States that have signed formal regulatory agreements with NRC are known as "Agreement States."

[10] Licensees are businesses and other organizations licensed by NRC and Agreement States to possess radiological sources.

[11] 10 CFR 20.1003 defines a nationally tracked source as, "a sealed source containing a quantity equal to or greater than Category 1 or Category 2 levels of any radioactive material listed in Appendix E of this part. In this context a sealed source is defined as radioactive material that is sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It does not mean material encapsulated solely for disposal, or nuclear material contained in any fuel assembly, subassembly, fuel rod, or fuel pellet. Category 1 nationally tracked sources are those containing radioactive material at a quantity equal to or greater than the Category 1 threshold. Category 2 nationally tracked sources are those containing radioactive material at a quantity equal to or greater than the Category 2 threshold but less than the Category 1 threshold."

[12] A table of radiological sources subject to NSTS reporting appears in Appendix A.

[13] These sources do not include materials encapsulated solely for disposal, or nuclear materials contained in fuel assemblies, subassemblies, fuel rods, or fuel pellets.

[14] The IAEA's five-category scale provides a relative ranking of radiological sources in terms of each source's potential to cause immediate harmful health effects if not safely managed or securely protected. Category 1 sources are the most hazardous, and can cause permanent injury or death if mishandled; Category 5 sources are the least hazardous, and could not cause permanent injury.

international community to govern safety and security of radioactive material based on the IAEA categorization system.[15] In addition, the Energy Policy Act of 2005 required NRC to issue regulations establishing a mandatory tracking system for radiation sources in the United States. NRC deployed NSTS in December 2008, thereby enabling licensees to begin reporting radiological source inventories and transactions by January 31, 2009, as required by 10 CFR 20.2207.

NSTS enables licensees to report via the Internet transactions of nationally tracked sources, including the manufacture, import, export, transfer, and receipt of these sources.[16] Licensees can also report source transaction data by other means such as facsimile, e-mail, or standard mail. Approximately 200 source transactions are processed daily in NSTS.

Program Offices

The Office of Federal and State Materials and Environmental Management Programs (FSME) is responsible for NSTS operations. FSME staff conduct training for Agreement State and licensee personnel, and maintain an Internet page offering user guidance and program updates. FSME staff also monitor data in NSTS, and conduct an annual inventory review in which licensees compare their physical inventories with NSTS inventory data, and reconcile any discrepancies between the two.[17] A contractor operates and maintains NSTS for FSME, and also processes data submitted by licensees for entry into NSTS.[18] The FSME contractor also runs the NSTS Help Desk, whose personnel provide technical assistance to NSTS users. As of March 2010, total obligated

[15] A joint Department of Energy-NRC Interagency Working Group on Radiological Dispersal Devices also recommended a national source tracking system following its work during 2002-2003.

[16] The Energy Policy Act of 2005 established requirements for identifying individual radiological sources (e.g., by serial number), and for reporting any change of possession or loss of control of these materials. In addition, this legislation required a capability for reporting through a secure Internet connection.

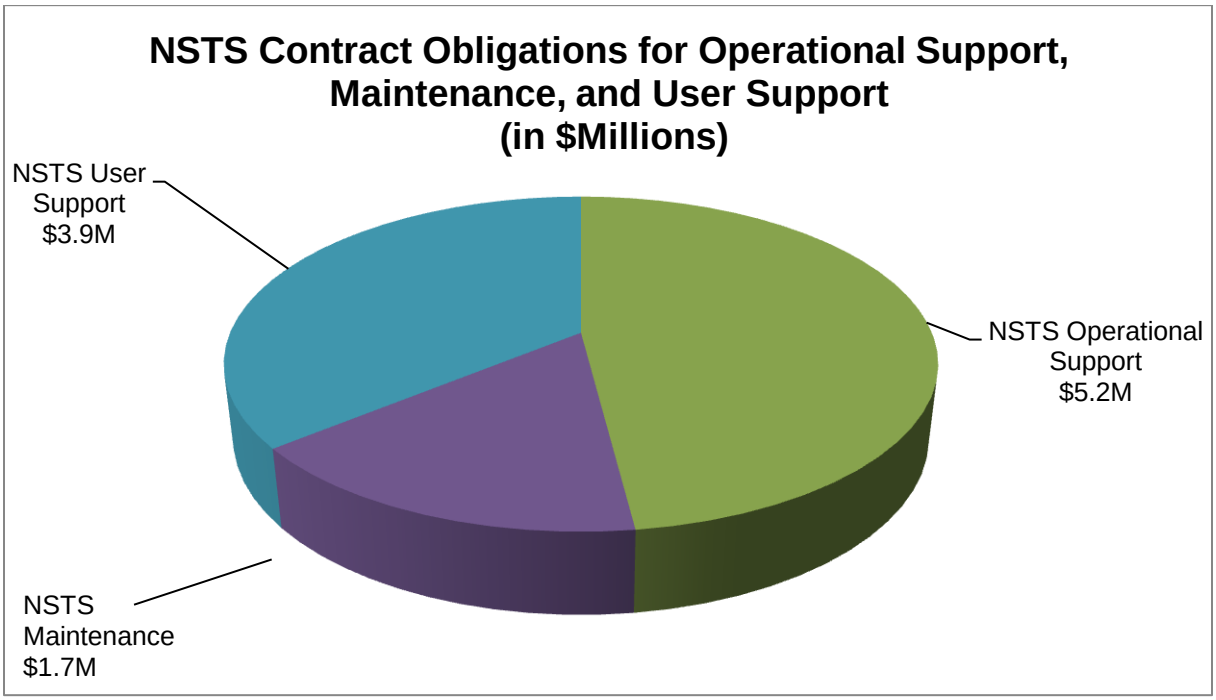
[17] This "annual inventory reconciliation" is required by 10 CFR 20.2207. Licensees must validate their inventory data in NSTS by January 31 of each year.

[18] For clarity, this report refers to FSME's NSTS contractor as the "FSME contractor."

funding for the NSTS contract was approximately $20 million, which included approximately $10.8 million for operations, maintenance, and user support.[19] Graph 1 illustrates a breakout of operational support, maintenance, and user support contract costs current as of March 2010.

NSTS Program Resources

Graph 1: Obligated Contract Funds for NSTS Operational Support, Maintenance, and User Support



Source: OIG Analysis

The Office of Information Services (OIS) supports NSTS by managing a contract for credentialing NSTS users and providing users with equipment needed to access NSTS via the Internet.[20] OIS provides credentialing services for other NRC programs under this agencywide contract; however, contract costs directly attributable to NSTS were approximately $3.2 million from October 2008 through March 2010. In addition to contract management, OIS staff assist NSTS users with technical problems that the NSTS Help Desk cannot resolve.

[19] The remaining $9.2 million in contract obligations reflect NSTS development tasks.

[20] For clarity, this report refers to OIS's credentialing contractor as the "OIS contractor."

The Computer Security Office (CSO) is responsible for ensuring that NSTS complies with the Federal Information Security Management Act (FISMA), which outlines the information security management requirements for Federal agencies. As part of this effort, CSO conducts annual testing of automated and procedural security controls listed in the NSTS system security plan to ensure these controls function as planned. In addition to ensuring FISMA compliance, CSO staff lead incident response activities in the event of an information system breach.

NRC staff based in all of the regional offices use NSTS data for conducting inspections of licensees. Some region-based staff also serve on temporary assignments in support of NSTS program operations. In total, NRC committed 7.4 direct full-time equivalent personnel (FTE) to the NSTS program in Fiscal Year 2009, and 5.8 FTE through the second quarter of Fiscal Year 2010. Although several headquarters offices support NSTS, only FSME and OIS had direct labor charges to the program.

NSTS User Credentialing

To access NSTS online, users must become credentialed through a multi-step process. After NRC staff identify potential NSTS online users based on their job requirements, the first step in credentialing requires an applicant to enroll online. The second step is to review and approve the online application. In the third step, OIS contractor personnel mail an enrollment package to prospective NSTS users, who must complete forms in their enrollment packages, sign an identity declaration in the presence of a public notary, and return the completed enrollment packages to the OIS contractor. Finally, after receiving the completed enrollment packages, OIS contractor personnel verify the identity and employment status of each prospective NSTS user.

Following successful completion of the application process, each NSTS user receives a "smart card" and card reader. Smart cards help prevent unauthorized access to NSTS by authenticating users when they log into the system via the Internet. Figure 1 depicts an NSTS smart card.

Figure 1: NSTS Smart Card Illustration

Source: NRC

Upon receiving this equipment, an NSTS user must download digital certificates[21] onto the smart card, and install on his/her computer software that enables the smart card equipment to function. Once NSTS users set up this hardware and software on their computers, FSME staff activate users' accounts, thereby enabling them to read and enter data into NSTS.

II. PURPOSE

The audit's objective was to determine if the National Source Tracking System meets its required operational capabilities. See Appendix E for more information on the audit scope and methodology.

[21] A digital certificate is an electronic identifier that establishes a user's credentials when processing transactions on the Internet. NSTS is designed with multi-factor authentication to verify each user's identity. System users must enter a user name and password in conjunction with their smart cards to gain access to NSTS.

III. FINDINGS

NSTS satisfies basic operational requirements, including functional capabilities for capturing data and security features for protecting data.[22] Further, an NSTS configuration control board comprised of NRC staff, information technology contractors, Agreement State representatives, and a representative from industry meets several times a year to evaluate potential system upgrades on a cost-benefit basis. This internal control mechanism enables NRC to gather feedback from system users on ways to improve NSTS functionality, and provides NRC management with information to guide resourcing decisions. During this audit, Office of the Inspector General (OIG) auditors developed findings and associated recommendations regarding NSTS smart card utilization, data quality, and access controls. By addressing these issues, NRC can improve program efficiency and strengthen oversight of licensees that possess and transfer Category 1 and 2 radiological sealed sources.

A. Licensees Have Not Fully Adopted NSTS Technology

NSTS was designed primarily to be an Internet-based system enabling direct data entry by licensees. However, a majority of the licensee user population has not fully adopted technology required for direct access to NSTS. This trend is caused by challenges inherent in the NSTS credentialing process, as well as technical problems encountered by licensees in using the smart card devices. Further, Help Desk contractor personnel are not always capable of resolving application and set-up problems encountered by NSTS users. As a result, NRC has incurred administrative costs from updating NSTS on behalf of licensees who opt not to enter their source transaction and inventory data into NSTS.

NSTS Is Designed Primarily for Internet-Based Use

Since the early stages of system development, NSTS was designed primarily to be an Internet-based system enabling direct data entry by licensees. The NSTS System Requirements and Needs Analyses supporting system design explicitly state this assumption and note that

[22] CSO performed the first annual security controls testing of NSTS in March 2010 to determine compliance with security requirements documented in the System Security Plan, and to verify that the security controls identified in the plan are correctly implemented. CSO recommended enhancements for 7 of the 128 controls tested.

licensees need a Web-based interface for "near real-time" reporting. NRC's Office of Management and Budget (OMB) Exhibit 300 submission, which declares costs and benefits of NRC information technology investments to OMB, describes qualitative benefits expected to result from NSTS's Internet-based architecture, such as minimized data processing time and ready support for an expandable user base.

Licensees Have Not Adopted Technology Needed for Internet Access to NSTS

Despite these assumptions, the licensee user population has not fully adopted technology required for direct Internet access to NSTS. For example, an NRC staff analysis estimated that only one-third of licensee personnel who must report source data to NSTS had online system access by November 2009. The analysis predicted that the population of licensees with direct access to NSTS would not increase substantially. This analysis is reinforced by May 2010 data showing that about 41 percent of licensees[23] had one or more credentialed users at this point in time.[24] Further, OIG auditors' survey of licensee personnel who are listed as active NSTS users (i.e., users with active NSTS accounts) found that approximately 31 percent of the respondents typically report transaction data to NRC by facsimile.[25]

Credentialing and Technical Issues Present Challenges to Online Use

Licensees' low participation in using NSTS Internet-based technology is caused by challenges inherent in the NSTS credentialing process, as well as technical problems encountered by licensees in their deployment and use of smart card devices. Credentialing process challenges include rigorous standards for completing NSTS application documents, which do not allow for even minor discrepancies between an applicant's personal information as stated on these documents and corresponding information in NRC's records.[26] Such discrepancies result in rejection of credentialing

[23] 537 of 1,321 licensees.

[24] An additional 17 users were undergoing the credentialing process.

[25] See Appendix D for information on survey methodology.

[26] After OIG auditors completed fieldwork for this report, agency staff presented plans to streamline employment verification and identity proofing procedures. NRC staff expect the revised procedures to

applications, thereby obligating the applicant to restart the credentialing process. Further obstacles include the efforts associated with completing applications and submitting notarized identity declarations. Process lag time presents yet another credentialing obstacle; although NRC aims for a 30-day turnaround time, nearly one half of licensees surveyed by OIG auditors reported a 2- to 6-month wait to complete NSTS applications and gain access to the system.

Technical challenges present further obstacles to online use of NSTS. First, NSTS users must install card readers, download digital certificates, and download card reader software within 30 days of completing the credentialing process; failure to do so results in account deactivation. Second, users must configure their computers to be compatible with NSTS, which may require technical support for users who are less skilled or have less familiarity with information technology. In some cases, users' network security settings prevent their computers from connecting to NSTS. Third, some operating systems and Internet browsers are not compatible with NSTS.[27] Lastly, NSTS users have encountered technical problems that NSTS Help Desk personnel could not immediately resolve.

Licensees Shift Administrative Burden of Data Reporting to NRC

As a result of low direct use of NSTS by licensee personnel, NRC has incurred costs associated with the administrative burden of processing NSTS data on behalf of licensees. These costs are most clearly reflected in NSTS Help Desk and user support contract ceilings, which increased 54 percent during the first year of operation from $2.52 million to $3.87 million. According to NRC staff, these cost increases are largely attributable to unanticipated need for Help Desk support and data entry work performed on behalf of licensees who do not report their data directly to NSTS via the Internet. Moreover, these contract costs do not account for the resource impact on NRC staff who support licensee personnel with technical troubleshooting and correction of erroneous data.

reduce the number of licensees whose NSTS applications are rejected because of minor discrepancies between employment information in NRC licensing documents and State government records.

[27] These include the Microsoft Vista and Windows 2000 operating systems, Apple operating systems, and Apple and Firefox browsers.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Assess the feasibility of alternative credentialing strategies, such as:

    a. Targeting select types of licensees for smart card use based on risk, business case justification, or other criteria.

    b. Reviewing NSTS e-authentication risk assessment for currency and, if appropriate, identify technological alternatives to smart card authentication.

2. Develop and implement a policy to ensure Help Desk staff are kept current regarding credentialing and technical issues that may adversely impact NSTS applicants and users.

B. NSTS Has Data Quality Problems with Timeliness and Accuracy

Internal control standards for Federal Government agencies recommend that data be processed in a timely manner to maintain its relevance and operational value to management. NSTS is designed with automated security controls to ensure the integrity of data entered into the system; however, OIG auditors found problems with the timeliness of NSTS data regarding transfers of nationally tracked sources. These problems result primarily from the process by which data is reported and manually uploaded into NSTS. Although NSTS cannot provide "real time" tracking of licensees' transactions and inventories, NRC and Agreement State personnel must have reliable information to perform their oversight duties.

Government Agencies Should Ensure Timeliness and Accuracy of Data Processed by Agency Systems

General internal control standards for Federal Government agencies recommend that data be processed in a timely manner to maintain its relevance and operational value to management. Likewise, internal control standards for Government information systems recommend automated and administrative controls to ensure the accuracy and validity of data processed by agencies' systems.

High Percentages of Source Transfer Records Are Incomplete

NSTS is designed with automated security controls to ensure the integrity of data entered into the system; however, OIG auditors found problems with the timeliness and accuracy of NSTS data. For example, one report from December 2009 showed that about 19 percent[28] of nationally tracked source transfers were at least 6-months "overdue" – that is, licensees had reported outbound shipments, but the shipments lacked receipt records in NSTS indicating that these shipments had reached their intended destinations. Similarly, another report generated in April 2010 showed that approximately 19 percent[29] of shipments were at least 30-days "overdue." Shipments that appear "overdue" in NSTS are not necessarily lost or misdirected. According to FSME staff, there were no reports of lost or missing nationally tracked sources during the time of this audit. Rather,

[28] 106 of 560 transactions.

[29] 242 of 1,276 transactions.

some cases reflect backlogged reports. In other instances, anomalies may reflect data entry errors such as reports of shipments that never occurred, licensees reporting of sub-Category 2 radiological sources,[30] and duplication of shipment records.[31]

NSTS Data Quality Problems Result From Reliance on Manual Processes for Reporting Data

Problems with the accuracy and timeliness of transaction data in NSTS result from the process by which data is reported and manually uploaded into NSTS. Although NSTS is designed to enable direct data entry by credentialed licensee personnel, most transactions are processed by NRC's contractor on behalf of licensees. For example, a December 2009 report showed that the FSME contractor processed approximately 70 percent[32] of transactions during that month. Likewise, a report for one week in April 2010 showed that about 48 percent of outgoing source shipments were entered online by licensees,[33] and approximately 28 percent of shipment receipts were entered online by licensees.[34]

Licensees who do not enter their own transaction and inventory data into NSTS typically send this information by facsimile[35] to the FSME contractor site, where multiple contractor personnel are involved in processing the data. FSME contractor personnel log receipt of each facsimile, and must work directly with licensees to resolve problems such as incomplete or illegible information. FSME contractor personnel have tried various approaches for managing document flow but acknowledged some

[30] NRC regulations do not require licensees to report shipments and inventories of sub-Category 2 sources to NSTS; however, some licensees report this information.

[31] Duplicate records can appear in NSTS when a licensee reports receipt of a nationally tracked source shipment before the sender's shipment information has been uploaded to NSTS. In such cases, the recipient must create a placeholder shipment record in NSTS to correspond with the receipt record. When the sender's shipment information is later uploaded to NSTS, this creates a duplicate "sent" shipment record.

[32] 2,025 of 2,910 transactions.

[33] 262 of 547 outgoing shipments.

[34] 36 of 127 receipts.

[35] To report NSTS data by facsimile or mail, licensees must submit a completed NRC Form 748 describing source types, serial numbers, transaction dates, and other relevant information. See Appendix B for a sample NRC Form 748.

difficulties, particularly during high-volume work periods. An NRC internal analysis completed in January 2010 also found problems with the FSME contractor's document controls, citing reports by licensees of NSTS data that remained incorrect despite licensees' repeated efforts to submit correct information to the FSME contractor. In addition, licensees do not receive notification when the FSME contractor receives their Form 748s; as a result, licensees may be unaware of failed or incomplete facsimile transmissions.[36]

Lack of Timely, Accurate Data Could Compromise Oversight and Emergency Response

Federal and State Government officials need reliable information to perform their oversight duties and respond to emergencies. Untimely and inaccurate data in NSTS can weaken oversight of licensees because NRC and Agreement State regulators use NSTS data for inspections as well as the annual review of licensee inventories. In the event of a serious emergency, untimely and inaccurate data could compromise authorities' response planning and hinder effective deployment of emergency response assets to protect public health and safety. Further, the legislative mandate for NSTS reflects Congress's concern that Government officials maintain visibility over radiological materials that could present safety hazards and security risks if lost or stolen.

Recommendation

OIG recommends that the Executive Director for Operations:

3. Develop and implement document control policies and processes to improve accountability for NSTS data submitted by licensees to NRC for uploading to NSTS.

[36] FSME contractor personnel cited cases in which they received blank or illegible Form 748s via facsimile, but lacked contact information to notify licensees of the need to re-transmit the forms. After this audit was completed, FSME staff told OIG auditors that NRC is working with the FSME contractors to implement an e-mail system to acknowledge receipt of 748s submitted via facsimile. Staff expect this system to be implemented by late summer 2010.

C. Least Privilege Principle Not Consistently Applied to NSTS Access Controls

Federal Government internal controls standards for information systems recommend security controls to protect systems and networks from inappropriate access and unauthorized use. Although NSTS access rights for licensee personnel are scaled to individual users' job needs, some NRC staff have broader access rights that do not reflect individuals' job needs or organizational roles. This occurs because NRC lacks a procedure for scaling staff access rights to their respective job needs. Although OIG auditors did not find evidence of internal NSTS data breaches, the lack of a procedure to ensure consistent application of the least privilege principle increases the risk that NSTS data could be intentionally or accidentally compromised.

Access Rights Should Reflect Individual and Organizational Business Needs

Federal Government internal controls standards for information systems recommend access security controls to protect systems and networks from inappropriate access and unauthorized use. Specifically, National Institute of Standards and Technology guidance[37] recommends the "least privilege" principle, according to which access privileges are scaled to information system users' individual and organizational needs.

Some Staff Access Rights Not Scaled to Business Needs

Although NSTS access rights for licensee personnel are scaled to individual users' job needs, some NRC staff have broader access rights that do not reflect their job needs or organizational roles. One headquarters employee reported having edit capabilities that were not necessary for routine work, and said that office management had instructed staff not to edit NSTS data. In addition, OIG auditors found that one employee had edit rights while on a temporary assignment, but retained edit rights 2 months after this assignment ended.[38]

[37] National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3; August 2009.

[38] This staff member reportedly notified a branch chief and the NSTS Help Desk of the situation, but no change in edit rights resulted.

NRC Lacks Procedure for Scaling Staff Access Rights to Business Needs

Some NRC staff possess unneeded NSTS edit rights because NRC lacks a procedure for ensuring individual staff access rights are scaled to their respective job needs. FSME staff told OIG auditors that NRC management has raised concerns and requested a "read only" option for staff who need to view, but not edit, NSTS data. However, during the time of this audit, NRC had not implemented this "read only" option on an as-needed basis.[39]

Increased Risk of Data Breach

Granting NSTS users access rights that exceed individual or organizational business needs increases the risk that NSTS data could be intentionally or accidentally compromised. Although NSTS automatically logs edits, NRC staff and contractors who administer the system must monitor it for suspicious activity. Applying the principle of least privilege to NRC staff who use NSTS would provide an automated control to prevent accidental data loss or corruption, and reduce the manual monitoring burden for NRC staff who administer NSTS.

Recommendation

OIG recommends that the Executive Director for Operations:

4. Implement "read only" capability in NSTS for NRC staff who must use NSTS, but do not need edit rights to conduct duties in accordance with individual or organizational business needs.

[39] NRC staff have performed a review of staff access rights to the NSTS, established access controls, and are formalizing a procedure for the continual monitoring of user accounts.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Assess the feasibility of alternative credentialing strategies, such as:

    a. Targeting select types of licensees for smart card use based on risk, business case justification, or other criteria.

    b. Reviewing NSTS e-authentication risk assessment for currency and, if appropriate, identify technological alternatives to smart card authentication.

2. Develop and implement a policy to ensure Help Desk staff are kept current regarding credentialing and technical issues that may adversely impact NSTS applicants and users.

3. Develop and implement document control policies and processes to improve accountability for NSTS data submitted by licensees to NRC for uploading to NSTS.

4. Implement "read only" capability in NSTS for NRC staff who must use NSTS, but do not need edit rights to conduct duties in accordance with individual or organizational business needs.

V. AGENCY COMMENTS

At an exit conference held on July 28, 2010, agency management stated their general agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

Appendix A

TABLE OF NATIONALLY TRACKED SOURCES LISTED IN 10 CFR 20, APPENDIX E

The Terabecquerel (TBq) values are the regulatory standard. The curie (Ci) values specified are obtained by converting from the TBq value. The curie values are provided for practical usefulness only and are rounded after conversion.

Radioactive material	Category 1 (TBq)	Category 1 (Ci)	Category 2 (TBq)	Category 2 (Ci)
Actinium-227	20	540	0.2	5.4
Americium-241	60	1,600	0.6	16
Americium-241/Be	60	1,600	0.6	16
Californium-252	20	540	0.2	5.4
Cobalt-60	30	810	0.3	8.1
Curium-244	50	1,400	0.5	14
Cesium-137	100	2,700	1	27
Gadolinium-153	1,000	27,000	10	270
Iridium-192	80	2,200	0.8	22
Plutonium-238	60	1,600	0.6	16
Plutonium-239/Be	60	1,600	0.6	16
Polonium-210	60	1,600	0.6	16
Promethium-147	40,000	1,100,000	400	11,000
Radium-226	40	1,100	0.4	11
Selenium-75	200	5,400	2	54
Strontium-90	1,000	27,000	10	270
Thorium-228	20	540	0.2	5.4
Thorium-229	20	540	0.2	5.4
Thulium-170	20,000	540,000	200	5,400
Ytterbium-169	300	8,100	3	81

Appendix B

NRC FORM 748 NSTS TRANSACTION REPORT

NRC FORM 748 (12-2009) 10 CFR 20.2207	U.S. NUCLEAR REGULATORY COMMISSION	APPROVED BY OMB: NO. 3150-0202	EXPIRES: 12/31/2012
NATIONAL SOURCE TRACKING TRANSACTION REPORT		Estimated burden per response to comply with this mandatory information collection request: 15 minutes. NRC requires this information to populate the National Source Tracking System for certain sealed sources. Send comments regarding burden estimate to the Records and FOIA/Privacy Services Branch (T-5 F53), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by internet e-mail to infocollects.resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0202), Office of Management and Budget, Washington, DC 20503. If a means used to impose an information collection does not display a currently valid OMB control number, the NRC may not conduct or sponsor, and a person is not required to respond to, the information collection.	

1. LICENSEE			2. TYPE OF TRANSACTION ☐ NEW ☐ CORRECTION	3. DATE OF TRANSACTION
A. LICENSEE NAME AND ADDRESS	B. LICENSE NO.	C. DOCKET NO.	☐ NEW SOURCE MANUFACTURED ☐ DISASSEMBLE ☐ RECEIPT ☐ DISPOSAL ☐ TRANSFER ☐ REPORT SOURCE	

4. PREPARER		
A. NAME OF PREPARER	B. DATE PREPARED	C. TELEPHONE NO. OF PREPARER

5. SOURCE DATA

A. MANUFACTURER	B. MODEL NO.	C. SERIAL NO.	D. RADIOACTIVE MATERIAL	E. ACTIVITY AND UNIT	F. ACTIVITY DATE	G. WASTE MANIFEST NO.	H. CONTAINER ID	I. COMMENT

6. TRANSFER DATA

6A. NAME AND ADDRESS OF RECIPIENT	B. LICENSE NO.	C. DOCKET NO.	D. ESTIMATED ARRIVAL DATE	E. COMMENT

7. RECEIPT DATA

7A. NAME AND ADDRESS OF SHIPPING LICENSEE	B. LICENSE NO.	C. DOCKET NO.	D. COMMENT

8. DISPOSAL DATA

A. WASTE MANIFEST NO.	B. CONTAINER ID	C. METHOD OF DISPOSAL	D. COMMENT

WARNING: FALSE STATEMENTS IN THIS CERTIFICATE MAY BE SUBJECT TO CIVIL AND/OR CRIMINAL PENALTIES. NRC REGULATIONS REQUIRE THAT SUBMISSIONS TO THE NRC BE COMPLETE AND ACCURATE IN ALL MATERIAL RESPECTS. 18 U.S.C. SECTION 1001 MAKES IT A CRIMINAL OFFENSE TO MAKE A WILLFULLY FALSE STATEMENT OR REPRESENTATION TO ANY DEPARTMENT OR AGENCY OF THE UNITED STATES AS TO ANY MATTER WITHIN ITS JURISDICTION.

NRC FORM 748 (12-2009)

Appendix C

SURVEY DISTRIBUTED TO AGREEMENT STATE PERSONNEL

OIG auditors sent a survey questionnaire by e-mail to 42 Agreement State personnel to gather feedback regarding deployment and use of NSTS, and received 38 responses. This was a non-statistical survey; consequently, results cannot be projected to the entire population of Agreement State personnel who use NSTS. However, the survey's high response rate gives auditors confidence that survey results provide relevant information about Agreement State user experiences. A copy of the survey questionnaire follows.

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

OFFICE OF THE
INSPECTOR GENERAL

Dear Agreement State NSTS user:

The U.S. Nuclear Regulatory Commission's Office of the Inspector General (OIG) is conducting a performance review of the National Source Tracking System (NSTS). As part of this review, OIG is surveying end-users to obtain feedback about NSTS operations. All responses will be saved in a secure, confidential OIG database. Survey participants will remain anonymous for reporting purposes.

Survey participation is strictly voluntary. However, OIG greatly appreciates your help in identifying ways to improve NSTS operations. If you have any questions or concerns, please contact one of the following OIG staff:

Paul Rades, Audit Manager; (301) 415-6228; paul.rades@nrc.gov
Mitzi Lorette, Senior Auditor; (301) 415-7856; maxinne.lorette@nrc.gov
Rob Woodward, Senior Auditor; (301) 415-6779; robert.woodward@nrc.gov

Please complete the following questionnaire by March 5, 2010, and return it by e-mail to: OIGSURVEY@nrc.gov. Thank you in advance for your participation.

1. Have you been credentialed to use NSTS?
[ ] Yes
[ ] No
If you answered "no," please explain below and then skip to question 6 on the next page.

2. How long did the credentialing process take for you?
[ ] 1 month or less
[ ] 2 to 6 months
[ ] More than 6 months

QUESTIONS CONTINUE ON NEXT PAGE

3. Did you experience any problems obtaining NSTS credentials?
[ ] Yes
[ ] No
If you answered "Yes," please briefly describe the problem(s).

4. Did you experience any problems downloading NSTS digital certificates and/or installing your smart card reader(s)?
[ ] Yes
[ ] No
[ ] N/A
If you answered "Yes," please briefly describe the problem(s).

5. Based on your experience, how do you rate NSTS for ease of use?
[ ] Easy
[ ] Average (compared to other information technology)
[ ] Difficult
If you answered "Difficult," please describe specific problems you've had using NSTS.

6. When you report source transactions to NRC, do you typically:
[ ] Enter information directly into NSTS at your computer?
[ ] Fax information to the NSTS Help Desk?
[ ] Transmit NSTS information to NRC by other means?
Please check all answers that apply. If you do not typically enter information directly into NSTS at your computer, please briefly explain why.

7. If you would like to provide more details about your responses, or wish to address any issues not covered by this questionnaire, please write your comments below.

This concludes our questionnaire. Please return this form by e-mail to: OIGSURVEY@nrc.gov. **Thank you again for your participation.**

Appendix D

SURVEY DISTRIBUTED TO LICENSEE PERSONNEL

OIG auditors sent a survey questionnaire by e-mail to 68 licensee personnel to gather feedback regarding deployment and use of NSTS. Auditors selected these personnel from NRC records of active NSTS accounts and transaction data. Auditors received 27 responses. This was a non-statistical survey; consequently, results cannot be projected to the entire population of licensee personnel who use NSTS. However, auditors stratified this survey to obtain information from licensees characterized as high, medium, and low-volume users based on their respective rates of transactions performed in NSTS. The survey's response rate, which includes responses from all three groups of high, medium, and low-volume users, gives auditors confidence that survey results provide relevant information about user experiences from a diverse group of licensee organizations. A copy of the survey questionnaire follows.

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

OFFICE OF THE
INSPECTOR GENERAL

Dear NSTS user,

The U.S. Nuclear Regulatory Commission's Office of the Inspector General (OIG) is conducting a performance review of the National Source Tracking System (NSTS). As part of this review, OIG is surveying end-users to obtain feedback about NSTS operations. All responses will be saved in a secure, confidential OIG database. Survey participants will remain anonymous for reporting purposes.

Survey participation is strictly voluntary. However, OIG greatly appreciates your help in identifying ways to improve NSTS operations. If you have any questions or concerns, please contact one of the following OIG staff:

Paul Rades, Audit Manager; (301) 415-6228; paul.rades@nrc.gov
Mitzi Lorette, Senior Auditor; (301) 415-7856; maxinne.lorette@nrc.gov
Rob Woodward, Senior Auditor; (301) 415-6779; robert.woodward@nrc.gov

Please complete the following questionnaire by March 19, 2010, and return it by e-mail to: OIGSURVEY@nrc.gov. Thank you in advance for your participation.

1. Have you been credentialed to use NSTS?
[ ] Yes
[ ] No
If you answered "No," please explain below and then skip to question 6 on the next page.

2. How long did the credentialing process take for you?
[ ] 1 month or less
[ ] 2 to 6 months
[ ] More than 6 months

QUESTIONS CONTINUE ON NEXT PAGE

3. Did you experience any problems obtaining NSTS credentials?
[ ] Yes
[ ] No
If you answered "yes," please briefly describe the problem(s).

4. Did you experience any problems downloading NSTS digital certificates and/or installing your smart card reader(s)?
[ ] Yes
[ ] No
[ ] N/A
If you answered "yes," please briefly describe the problem(s).

5. Based on your experience, how do you rate NSTS for ease of use?
[ ] Easy
[ ] Average (compared to other information technology)
[ ] Difficult
If you answered "Difficult," please describe specific problems you've had using NSTS.

6. If you would like to provide more details about your responses, or wish to address any issues not covered by this questionnaire, please write your comments below.

This concludes our questionnaire. Please return this form by e-mail to: OIGSURVEY@nrc.gov. Thank you again for your participation.

Appendix E

SCOPE AND METHODOLOGY

The objective of this audit was to determine if the National Source Tracking System meets its required operational capabilities.

Auditors reviewed Federal Government laws and regulations, NRC guidance, security controls, and internal controls associated with the National Source Tracking System to include:

- 2005 Energy Policy Act.
- The Code of Federal Regulations.
- National Institute of Standards and Technology Special Publications.
- Federal Bridge Certification Authority Certificate Policy.
- Government Accountability Office *Standards for Internal Control in the Federal Government.*

Auditors interviewed staff from FSME, OIS, CSO and contractors who have worked with NSTS. Auditors reviewed contract documents, NSTS reports, e-mail correspondence, NSTS information system design documents, and briefing materials. Auditors provided a survey to Agreement State and licensee personnel, and analyzed the survey results. Appendixes C and D contain copies of the survey forms distributed to Agreement State and licensee personnel.

Auditors further analyzed NSTS and credentialing services contract documents to calculate contract costs directly related to the system's use. Auditors also obtained staff hour data for fiscal year 2009 through the first quarter of fiscal year 2010 to calculate staff hours charged for NSTS operations.

This performance audit was conducted at NRC headquarters from January 2010 through May 2010 in accordance with generally accepted Government auditing standards. Those standards require that the audit is planned and performed with the objective of obtaining sufficient, appropriate evidence to provide a reasonable basis for any findings and conclusions based on the stated audit objective. OIG believes that the evidence obtained provides a reasonable basis for the report findings and conclusions based on the audit objective. Internal controls related to the

audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program. The audit work was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Robert Woodward, Audit Manager; and Mitzi Lorette, Senior Auditor.