AUDIT REPORT

Audit of National Source Tracking
System Information System
Development

OIG-09-A-03 November 20, 2008

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

OFFICE OF THE
INSPECTOR GENERAL

November 20, 2008

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NATIONAL SOURCE TRACKING SYSTEM INFORMATION SYSTEM DEVELOPMENT (OIG-09-A-03)

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

The report presents the results of the subject audit. Agency comments provided at the November 6, 2008, 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 follow up 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, Security and Information Management Audit Team, at 415-5911.

Attachment: As stated

Electronic Distribution

Frank P. Gillespie, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jim E. Dyer, Chief Financial Officer
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Information Services and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs
Guy P. Caputo, 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
Michael F. Weber, 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
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

EXECUTIVE SUMMARY

BACKGROUND

The National Source Tracking System (NSTS) is an initiative of the Nuclear Regulatory Commission (NRC) designed to allow Agreement State[1] and Federal Government agencies to track transactions of specific types and quantities of radiological sealed sources.[2] This will include radiological sources held by the Department of Energy, and by NRC and Agreement State licensees. Licensees are businesses and other organizations licensed to possess radiological sources. Tracking capabilities will span the entire life cycle of each source, from manufacture or import to receipt and transfer, ending with export, decay, or burial.

NRC awarded a contract worth approximately $15 million in December 2005 for NSTS information system development, operational support, and maintenance. This contract included approximately $3.1 million to fund information system development.

PURPOSE

The audit objective was to evaluate the agency's management of NSTS information system development and assess delays in the development process. The report appendix contains information on the audit scope and methodology.

RESULTS IN BRIEF

NRC had planned to develop the NSTS information system so that licensees could begin reporting radiological source data in November 2007. However, NRC's contractor did not complete system development work on schedule. NRC has therefore postponed system deployment until December 2008, and has revised the licensee reporting deadline to January 2009. System development delays resulted from a lack of clear policies and procedures for review of key system security documentation, and for coordinating efforts among internal stakeholders.

[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] Radioactive material may be in the form of a sealed source, which is the term used to describe radioactive material that is permanently sealed in a capsule or closely bonded in a solid form. This report refers to radiological sealed sources as "radiological sources."

Technological, organizational, and staffing issues were additional factors cited by NRC staff. As a result of these delays, NRC incurred added contract costs of approximately $2.8 million. Furthermore, NRC has postponed by 18 months the deployment of the NSTS information system, which agency officials consider a top-priority project for improving accountability of radiological sources. NRC is planning information systems to complement NSTS in the near future; however, these systems could face similar challenges if the agency does not address underlying causes of problems encountered during the NSTS project.

RECOMMENDATIONS

This report makes recommendations to the Executive Director of Operations to improve NRC's management of information system development.

AGENCY COMMENTS

At a November 6, 2008, exit conference, NRC senior managers agreed with the report contents and provided editorial suggestions. This final report incorporates revisions made, where appropriate, as a result of the agency's suggestions.

ABBREVIATIONS AND ACRONYMS

C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CSO	Computer Security Office
DOE	Department of Energy
FSME	Federal and State Materials and Environmental Management Programs
IAEA	International Atomic Energy Agency
NIST	National Institute of Standards and Technology
NMSS	Office of Nuclear Material Safety and Safeguards
NRC	Nuclear Regulatory Commission
NSTS	National Source Tracking System
OIS	Office of Information Services
OMB	Office of Management and Budget
PMM	Project Management Methodology

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

Introduction

The National Source Tracking System (NSTS) is an initiative of the Nuclear Regulatory Commission (NRC) designed to allow Agreement State[3] and Federal Government agencies to track transactions of specific types and quantities of radiological sealed sources.[4] This will include radiological sources held by the Department of Energy (DOE), and by NRC and Agreement State licensees. Licensees are businesses and other organizations licensed to possess radiological sources. Tracking capabilities will span the entire life cycle of each source, from manufacture or import to receipt and transfer, ending with export, decay, or burial.

Emerging Threats Drive NSTS

After the terrorist attacks in the United States on September 11, 2001, NRC conducted a comprehensive review of nuclear material security requirements. This review included a focus on radioactive materials that could be used to create a radiological dispersal device.[5] NRC's review considered the changing domestic and international threat environments and related U.S. Government-supported international initiatives in the nuclear security area, particularly activities conducted by the International Atomic Energy Agency (IAEA). In May 2003, DOE and NRC jointly issued a report titled ''Radiological Dispersal Devices: An Initial Study to Identify Radioactive Materials of Greatest Concern and Approaches to Their Tracking, Tagging, and Disposition.'' This report recommended development of a national tracking system to better monitor the location and movement of radiological sources.

[3] 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."

[4] Radioactive material may be in the form of a sealed source, which is the term used to describe radioactive material that is permanently sealed in a capsule or closely bonded in a solid form. This report refers to radiological sealed sources as "radiological sources."

[5] These devices are commonly known as "dirty bombs." According to NRC, most dirty bombs would not release enough radiation to kill people or cause severe illness; rather, conventional explosives in the device would cause greater harm than its radioactive components. However, depending on the scenario, a dirty bomb explosion could create fear and panic, contaminate property, and require potentially costly cleanup.

Legislative Basis for NSTS

The Energy Policy Act of 2005 requires NRC to issue regulations establishing a mandatory tracking system for radiation sources in the United States.[6] The act sets 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, the system is to enable reporting through a secure Internet connection. NRC fulfilled its legislative mandate in November 2006 by amending the Code of Federal Regulations (CFR) to include provisions for NSTS.[7]

Internal and External NSTS Stakeholders

The NSTS initiative involves internal NRC stakeholders and the contractor selected to develop the system, as well as external stakeholders representing other Federal Government agencies, State governments, and licensees. NRC's Office of Federal and State Materials and Environmental Management Programs (FSME) is the NSTS information system owner. The Office of Nuclear Material Safety and Safeguards (NMSS) was the initial system owner before FSME became a separate agency office in October 2006. A project team composed of FSME staff manages NSTS development, while a contractor performs most of the work needed to design, build, and deploy the information system. NRC awarded a contract worth approximately $15 million in December 2005 for NSTS information system development, operational support, and maintenance; this contract included approximately $3.1 million to fund information system development. Other NRC stakeholders include NRC's Office of Information Services (OIS), which provides project management guidance and review, and the Computer Security Office (CSO), which reviews system design documents to ensure compliance with Federal Government standards for securing information systems. Prior to the establishment of CSO as a separate agency office in November 2007, OIS performed these reviews. External stakeholders include DOE and Agreement

[6] Under the act, radiation source means a Category 1 source or a Category 2 source as defined in the IAEA Code of Conduct and any other material that poses a threat, as determined by the Commission, other than spent nuclear fuel and special nuclear material. Per NRC regulations, the term "nationally tracked source" does not include material encapsulated solely for disposal, or nuclear material contained in any fuel assembly, subassembly, fuel rod, or fuel pellet.

[7] *Federal Register*, Vol. 71, No. 216, November 8, 2006. 10 CFR Parts 20 and 32, "National Source Tracking of Sealed Sources."

State officials, who will use NSTS to conduct oversight in their respective jurisdictions, as well as licensees such as industrial businesses, medical facilities, and research organizations.

Functional Overview of NSTS Information System

Once the NSTS information system is deployed, the contractor will continue to maintain the system. Licensee personnel will report data through a secure Internet connection; however, licensees will also have the option of reporting information by mail, fax, or telephone. DOE and Agreement State officials will have access rights enabling them to view and enter data for licensees and activities under their respective jurisdictions.

To reduce risk of unauthorized personnel accessing NSTS and compromising its data, NRC will issue "hard token" authentication devices to authorized users. For NSTS, the hard token is a cryptographic device that stores digital certificates and keys for use in electronic authentication. Authentication by means of the hard token requires the user to type the password for the hard token into the user's computer during the login to NSTS. The combination of the hard token device and the user's password is known as "two-factor authentication." Figure 1.1 shows a NSTS hard token authentication card.

Figure 1.1 Example of NSTS Hard Token Authentication Card

Source: NRC

Once NSTS reporting deadlines take effect, licensees will be legally obligated to conduct annual physical inventories of source materials in their possession, and reconcile discrepancies found between their physical inventories and data stored in NSTS. NRC asserts that NSTS, on its own, will not ensure physical protection of radiological materials. Rather, the agency expects NSTS to improve accountability for radiological sources. NRC also expects

NSTS to complement two other systems being planned to enhance oversight of radiological source materials. These systems—Web-based licensing and automated license verification—are scheduled for deployment between 2010 and 2011.

Information Technology Security and Project Management Guidance

In developing the NSTS information system, NRC must comply with Federal Government regulations for information technology security. The National Institute of Standards and Technology (NIST) issues supplementary risk assessment guidance, as well as technical publications that prescribe standards for data protection and user authentication.[8] The Office of Management and Budget (OMB) issues guidance to Federal agencies for assessing information system risk and security requirements.[9] NRC Management Directive 12.5, "NRC Automated Information Security Program,"[10] provides guidance for complying with Federal regulations, and assigns roles and responsibilities to agency staff for implementing security measures to protect NRC information and information systems.

NRC staff responsible for managing information technology projects use the agency's Project Management Methodology (PMM), which became official guidance in June 2007.[11] The PMM establishes agency processes to be followed throughout all phases of an information system's life cycle. The NSTS project team was among the first to use an early version of the PMM in 2006 as it replaced NRC's previous methodology.[12] The PMM is still evolving, as the

[8] Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004; FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006; NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," Rev. 1, December 2006; FIPS Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001.

[9] OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000; OMB M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003.

[10] Management Directive 12.5, "NRC Automated Information Security Program," revised September 12, 2003.

[11] Management Directive 2.8, "Project Management Methodology," Volume 2: Information Technology, June 19, 2007.

[12] The System Development Life Cycle Management Methodology.

agency develops templates for project deliverables, and works to integrate resource planning, security, and other requirements into a mature methodology.

Within the PMM, security reviews and approvals occur through a discrete process called Certification and Accreditation (C&A).[13] Certification requires a comprehensive assessment of the managerial, operational, and technical security controls in an information system to determine the extent to which these controls are implemented correctly, operate as intended, and fulfill system security requirements. Accreditation represents the decision of a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Once in operation, an information system must be re-certified and re-accredited on a 3-year cycle.

II. PURPOSE

The audit objective was to evaluate the agency's management of NSTS information system development and assess delays in the development process. The report appendix contains information on the audit scope and methodology.

[13] CSO manages this process for NRC information systems.

III. FINDING

NSTS Information System Development Delayed Primarily by Lack of Clear Policies and Procedures

NRC had planned to develop the NSTS information system so that licensees could begin reporting radiological source data in November 2007. However, NRC's contractor did not complete system development work on schedule. NRC has therefore postponed system deployment until December 2008, and has revised the licensee reporting deadline to January 2009. System development delays resulted from a lack of clear policies and procedures for review of key system security documentation, and for coordinating efforts among internal stakeholders. Technological, organizational, and staffing issues were additional factors cited by NRC staff. As a result of these delays, NRC incurred added contract costs of approximately $2.8 million. Furthermore, NRC has postponed by 18 months the deployment of the NSTS information system, which agency officials consider a top-priority project for improving accountability of radiological sources. NRC is planning information systems to complement NSTS in the near future; however, these systems could face similar challenges if the agency does not address underlying causes of problems encountered during the NSTS project.

NSTS Timelines and Information System Development Plans

In November 2006, NRC amended its regulations[14] to establish NSTS reporting requirements for licensees that possess specific types of radiological sources. The new regulations required licensees to begin reporting Category 1 sources by November 15, 2007, and Category 2 sources by November 30, 2007.[15] The transactions to be reported to NSTS include manufacture, transfer, receipt, disassembly, and disposal of these radiological sources.

In addition to these licensee reporting dates, NRC set internal benchmarks for developing the information system to be used for processing radiological source data. In 2004, the NSTS sponsor office[16] conducted a business case analysis to evaluate four NSTS

[14] 10 CFR 20.2207.

[15] Category 1 and 2 sources are defined in the IAEA Code of Conduct, Annex I, for specific radionuclides.

[16] At this point, NMSS was the system sponsor.

information system options, and selected one particular option on the basis of cost, benefit, and risk to NRC. This analysis described how the recommended information system would operate and included a project plan for developing the system over a 19-month period. The project plan broke system development down into discrete tasks that were linked to internal review milestones. Further, the project plan assumed a "modular" design approach, which was intended to enable different information system elements to be built independently of one another so that delays in one element would not hold up the entire project. In December 2005, NRC awarded a contract to build the NSTS information system. This contract reflected NRC's business case analysis by funding system development and initial deployment support[17] for a 24-month period beginning December 22, 2005, and ending December 31, 2007. The contract's statement of work detailed information system development tasks to be performed by NRC's contractor and established project milestones. Together, these documents show that NRC staff intended—and exercised due diligence in planning—to deploy the NSTS information system to meet licensee reporting deadlines set for November 2007.

Information System Development Delays

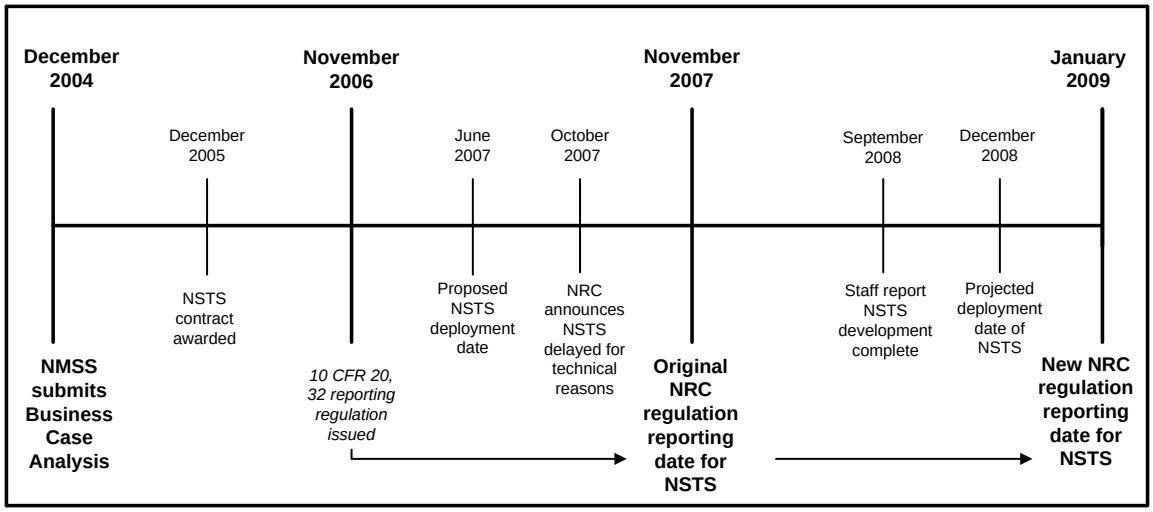
In October 2007, NRC announced that NSTS implementation would be delayed for technical reasons, and subsequently revised regulations to require licensee reporting of radiological source data by January 31, 2009, rather than the previous deadlines in November 2007. NRC attributed this delay to the emergence of new technology that would enhance NSTS security. The NSTS information system is unique insofar as it requires a high level of security, while also allowing access to NRC and DOE staff, as well as non-Federal Government users, including Agreement State officials and licensee personnel. NRC staff determined that NSTS would require a high level of security because, in their estimate, a system breach could compromise sensitive data and severely impact public health, safety, and security.[18]

[17] NSTS contract documents refer to system development as "Task 1," which entails 31 subtasks to be conducted by NRC's contractor. For instance, Task 1.1 is "Obtain Development Environment Purchase Approval"; Task 1.2 is "Develop Software Development Plan."

[18] NIST and OMB authentication guidance prescribes system security standards based upon potential effects of a system breach resulting from a user authentication error. More severe effects require a higher level of authentication assurance.

NSTS information system development concluded in September 2008. NRC plans on deploying NSTS in December 2008 to meet the revised licensee reporting deadline of January 31, 2009. In the interim, CSO staff must review C&A documentation for NSTS and grant its sponsor (FSME) either full or interim authority to operate the system. NRC must also verify the identity of prospective system users, and then issue authentication devices to authorized users.[19] In addition, NRC plans to provide training for Agreement State officials and licensee personnel. Figure 1.2 shows key events and dates in the development of the NSTS information system.

Figure 1.2: Timeline of NSTS Information System Development



Source: OIG analysis of NRC and *Federal Register* documents.

Lack of Clear Guidance for Project Management and System Documentation, and for Internal Stakeholder Coordination

Delays in NSTS development resulted in part from the lack of clear standards for project management and system design documentation, and from lack of clear direction for internal stakeholder coordination. According to NRC staff, technological challenges inherent in NSTS, NRC organizational issues, and staffing problems were additional factors.

[19] A contractor will perform these tasks for NRC.

Information System Documentation

Delays in NSTS information system development were caused in part by the lack of clear standards for project management and system security documentation. The NSTS project team was among the first to use NRC's new PMM as the agency transitioned away from its previous guidance for managing information system development. OIS was supposed to provide NRC and contractor staff with PMM guidance and templates to help them prepare system design documents, some of which are required for the C&A process. OIS had not finalized these templates when NSTS information system development began in January 2006, and NSTS project staff had to revise their initial submissions multiple times as templates changed, thereby resulting in extra work. Moreover, senior OIS and NMSS staff acknowledged in a November 2005 project kickoff meeting the need to facilitate C&A by creating documentation guidance and quality standards early in the NSTS information system development process, with January 2006 as the goal. Nevertheless, staff who were involved in the NSTS project in early 2006 told auditors that they lacked quality standards to guide preparation and review of key system design documentation. This lack of guidance is evidenced by disputes among NRC staff about whether a System Architecture Document[20] was required for C&A, the level of detail required in this document's preliminary drafts, and whether specific aspects of system security could be elaborated at a later stage in the project. Staff reported similar problems with standards for writing the system's Security Categorization, which serves as the basis for assessing security risks and selecting appropriate controls. Without consensus about quality standards for system design and security documents, NSTS project staff and OIS reviewers became involved in prolonged review and revision cycles.

Coordination of Internal Stakeholder Efforts

NSTS information system development delays also resulted from a lack of direction to coordinate internal stakeholders' work on the project. At the November 2005 project kickoff meeting, participants acknowledged the need for close coordination among NRC staff involved in NSTS development, as well as the need for early review of system security plans. In January 2006, OIS assembled a special "Tiger Team" to serve as a focal point for communications

[20] The System Architecture Document provides a comprehensive overview of an information system's architecture. It discusses design goals, constraints, and assumptions, as well as hardware layout and other technical aspects of system design.

among different OIS offices, the NSTS project team, and NRC's contractor. However, OIS and NSTS project staff told auditors that this approach did not meet its intended purpose of facilitating staff communication and coordination. Some Tiger Team staff reported that their roles and responsibilities were not clearly defined. Several NSTS project staff perceived a lack of coordination within OIS, despite Tiger Team efforts, as PMM and C&A guidance often changed without a clear reason. Also, an OIS official reportedly instructed OIS's senior security official not to communicate directly with NRC's contractor and to relay communications through the Tiger Team. In retrospect, staff recommended to auditors that periodic reviews involving key internal stakeholders such as OIS's senior security official, starting early in the development process, could have provided opportunities to address potential system design problems and resolve them before development work proceeded.

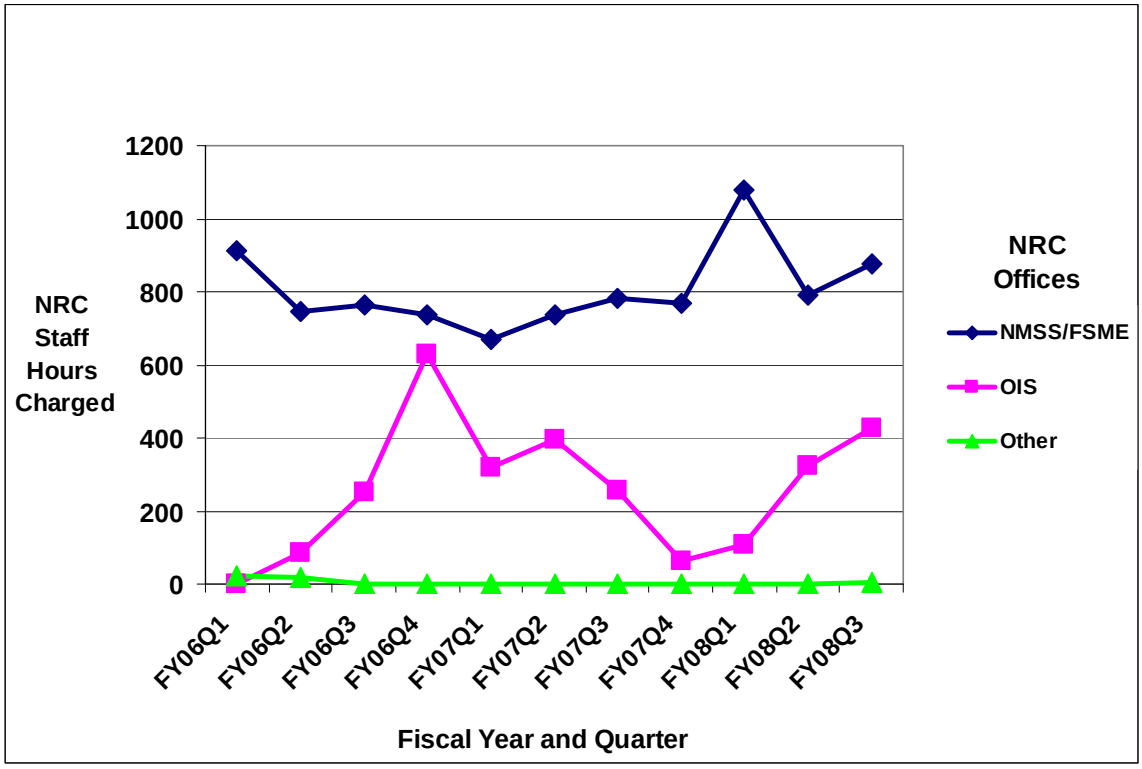
The lack of coordination among internal NRC stakeholders adversely affected the contractor's work. In one instance, installation of the contractor's data servers to be used in building the NSTS information system was delayed while NRC staff disputed whether the servers and NRC networks would be adequately secured. In another instance, which reportedly had greater bearing on the NSTS development schedule, OIS and NSTS project staff team took differing positions on the proper means for securing the system, particularly with regard to user authentication. OIS's senior security official began to review system design plans and raise concerns about security 6 months after the contractor had begun development work. In addition, OIS did not approve the Security Categorization, which the contractor needed to complete the system Risk Assessment, until 10 months after development began. As contract funds ran low and NRC staff had not reached agreement with the contractor regarding outstanding system design issues, NSTS project team staff suspended system development work. In the interim, the contractor conducted market research to identify commercially available security solutions for the NSTS project. OIS officials and NSTS project team staff eventually resolved this impasse through high-level meetings with the contractor's management and its senior subject matter expert. NRC staff estimated that this dispute prolonged the NSTS development schedule by approximately 1 year.

Technical, Organizational, and Staffing Challenges

According to NRC staff, problems with documentation standards and internal stakeholder coordination were compounded to some extent by technical challenges inherent in NSTS, NRC's decentralized approach to information system management, and staff turnover. First, the user authentication issues described above were unique to NSTS. The system requires a high level of security to protect sensitive data; however, approximately 15,000 personnel from NRC, other Federal Government agencies, Agreement State agencies, and licensee entities will have access to the system. NRC staff said that an information system of this complexity was unprecedented among civilian Federal Government agencies, and that NRC had no model on which to base its work. Second, one staff member believed that internal stakeholder coordination for NSTS was better than for most NRC information systems; however, several others claimed that integration of priorities and plans among OIS and system sponsors is a common problem at NRC, and that closer coordination starting at the outset of NSTS development could have prevented disputes over system design that impacted the project schedule. Third, staff reported that OIS personnel shortages and turnover adversely affected OIS's work on NSTS by disrupting continuity and lengthening review time.[21] Auditors analyzed NRC staff hour charges for NSTS development work and found that OIS work hours surged during the project's initial period, and again during its final stages in fiscal year 2008. While the data may reflect reasonable workflow trends, the data do not capture OIS's work on concurrent projects, which could have compounded the burden associated with NSTS. Figure 1.3 shows workload trends for NSTS information system development from the first quarter of fiscal year 2006 through the third quarter of fiscal year 2008.

[21] CSO reports that it has mitigated the personnel shortfall problem by increasing the number of NRC staff assigned to information system security tasks. Nevertheless, an August 2008 NRC assessment of the agency's information system development processes recommended that NRC review the adequacy of current staffing levels for technical personnel, particularly as information systems grow in complexity and criticality to NRC's mission.

Figure 1.3: Staff Hours Charged for NSTS Information System Development, 1st Quarter FY 2006 – 3rd Quarter FY 2008



Source: OIG analysis of NRC Human Resource Management System data.

Delays Increase Contract Cost, Postpone System Deployment, and Raise Questions About Future NRC Information Systems

As NSTS information system development approached the end of its initial contract schedule with key system design issues unresolved, NRC modified the baseline contract to increase funds for development tasks by approximately $2.8 million. This represents an increase of nearly 90 percent over the initial development task cost ceiling of $3.1 million, and only reflects cost growth directly attributable to extension of the system development schedule. In addition to these financial costs, NRC has postponed by approximately 18 months deployment of an information system that is designed to enhance accountability of radiological sources. Senior NRC officials and working-level staff have considered development of the NSTS information system a top agency priority. However, delays in system development and their underlying causes raise concerns about NRC's management of future information systems, particularly since NRC is planning two systems to complement NSTS. These and other information

systems could face similar delays and cost overruns if the agency does not mitigate or resolve procedural and organizational factors that hampered timely development of NSTS information system.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Establish policies and procedures that:

    a. Specify quality standards for C&A and PMM documents.

    b. Specify sequence and protocols for submission and review of C&A and PMM documents, to include review of milestones linked to project schedules.

    c. Clarify staff roles, responsibilities, and qualifications to better integrate internal stakeholders efforts.

2. Require staff involved in information systems development to undergo periodic training on these policies and procedures.

IV. AGENCY COMMENTS

At a November 6, 2008, exit conference, NRC senior managers agreed with the report contents and provided editorial suggestions. This final report incorporates revisions made, where appropriate, as a result of the agency's suggestions.

[Page intentionally left blank.]

Appendix

SCOPE AND METHODOLOGY

Auditors evaluated the agency's management of NSTS information system development. This audit was included as a planned audit in the fiscal year 2008 OIG Annual Plan.

The OIG audit team reviewed Federal Government information technology guidance issued by the OMB and NIST, as well as NRC internal guidance, including Management Directive 12.5, "NRC Automated Information Security Program"; and Management Directive 2.8, "Project Management Methodology."

Auditors interviewed staff from FSME, OIS, and CSO who have been involved in NSTS information system development. Auditors also reviewed Federal Government regulations, *Federal Register* notices, NRC public affairs material, NSTS contract documents, e-mail correspondence, NSTS information system design documents, briefing materials, and automated project management files. Auditors analyzed staff interview comments in conjunction with this documentary evidence to chronicle events and to identify problems in NSTS information system development and underlying causes of these problems.

Auditors further analyzed the NSTS information system contract and modifications to calculate contract costs and to identify costs directly related to system development delays. Auditors also obtained staff hour data for fiscal year 2006 through the third quarter of fiscal year 2008 to calculate staff hours charged to time codes associated with NSTS information system development.

This work was conducted at NRC headquarters from April 2008 through September 2008 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 objectives. OIG believes that the evidence obtained provides a reasonable basis for the report findings and conclusions based on the audit objective. The audit work was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; and James McGaughey, Senior Management Analyst.