AUDIT REPORT

Audit of NRC's Laptop Management

OIG-08-A-19 September 30, 2008

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

OFFICE OF THE
INSPECTOR GENERAL

September 30, 2008

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S LAPTOP MANAGEMENT
(OIG-08-A-19)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Laptop Management.*

The report presents the results of the subject audit. Agency comments provided at the September 23, 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 U.S. Nuclear Regulatory Commission (NRC) uses more than 1,550 laptop computers in its day-to-day operations. NRC owns, manages, and maintains approximately 85 percent of this laptop inventory, or approximately 1,300 laptops. The Office of Information Services (OIS), Infrastructure and Computer Operation Division (ICOD), is responsible for developing and implementing policies, standards, and configurations to maximize functionality, support, and security for laptops. Within ICOD, the Network Operations and Customer Services Branch is responsible for asset management of laptops. Although OIS has responsibility for issuing policies, standards, and configurations related to agency-owned laptops, individual offices are accountable for the immediate oversight of their assigned laptops, including management and maintenance.

PURPOSE

The audit objective was to evaluate the management of laptops including the effectiveness of NRC's security policies for laptop computers.

RESULTS IN BRIEF

The Office of the Inspector General (OIG) identified weaknesses pertaining to the implementation and monitoring of laptop security controls and other issues of concern pertaining to property management practices over agency-owned laptops.

RECOMMENDATIONS

This report contains recommendations intended to improve the implementation and monitoring of laptop security controls. A consolidated list of these recommendations appears in Section VI of this report.

AGENCY COMMENTS

At a September 23, 2008, exit conference, agency 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.]

ABBREVIATIONS AND ACRONYMS

CTF	Computer Testing Facility
ICOD	Infrastructure and Computer Operation Division
ID	identification
IT	information technology
LAN	local area network
MD	Management Directive
OIG	Office of the Inspector General
OIS	Office of Information Services
SPMS	Space and Property Management System

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

I. BACKGROUND

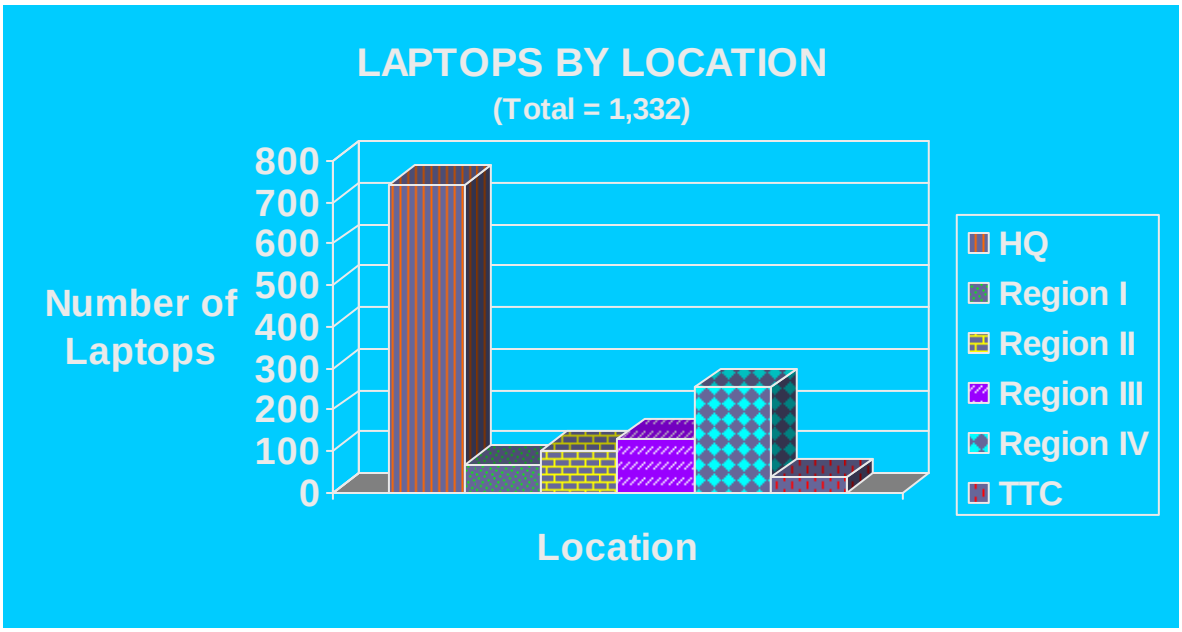
The U.S. Nuclear Regulatory Commission (NRC) uses more than 1,550 laptop computers in its day-to-day operations. NRC owns, manages, and maintains approximately 85 percent of this laptop inventory, or approximately 1,300 laptops. The remaining laptops are leased from a commercial vendor, which manages and maintains the machines. This audit report focuses specifically on agency-owned laptops and uses the term "laptops" to refer to the agency-owned machines.

The Office of Information Services (OIS), Infrastructure and Computer Operations Division (ICOD), is responsible for the development, integration, implementation, security, management, and support of the agency's information technology (IT) infrastructure, which includes laptops. Within ICOD, the Network Operations and Customer Services Branch is responsible for asset management of laptops.

A significant percentage of laptops are used by employees who engage in teleworking as part of work-related travel or who partake in the Flexible Workplace Program[1] or Special Circumstances Work-At-Home Program.[2] Other laptops are used in headquarters, regional, and resident inspector offices and the Technical Training Center as dockable desktops, classified standalone computers, or to support training, testing, software development, forensics, and security scans.

[1] The Flexible Workplace Program, also known as Flexiplace, allows employees in eligible positions to apply for a fixed-schedule telework arrangement. Under Flexiplace, employees may work at home or at an offsite location for up to 3 days per week with approval of their office director or regional administrator.

[2] The Special Circumstances Work-At-Home Program is designed to meet temporary needs resulting from conditions of personal incapacitation, personal hardship, or short-term work exigencies.



Although OIS has responsibility for issuing policies, standards, and configurations related to agency-owned laptops, individual offices are accountable for the immediate oversight of their assigned laptops, including management and maintenance. Individual office oversight of the laptops is a coordinated effort involving the office property custodian, IT coordinator, and laptop user designated on NRC Form 119, *Custodial Receipt for Sensitive Property*. Specifically, the office property custodian manages and is required to track user assignments within the office and record this information in the agency's Space and Property Management System (SPMS).[3] The office IT coordinator is required to coordinate with the Network Operations and Customer Services Branch regarding issues such as network access, software installation, and computer moves. The IT coordinator also approves office laptop acquisitions. Lastly, the individual to whom the laptop is assigned is responsible for ensuring that the machine is used in accordance with agency and Federal regulations and that the laptop itself and the data stored on it are secure.

[3] SPMS, previously known as PASS, is a database that contains records for all sensitive equipment, regardless of cost, and accountable non-sensitive equipment having an acquisition cost of at least $500. OIG recommended in audit report OIG-07-A-14, *Audit of NRC's Non-Capitalized Property*, dated July 12, 2007, to increase the threshold to $1,000, and the agency issued guidance to this effect in January 2008.

Individual offices purchase laptops out of their office budgets. The cost of each laptop ranges between $459 and $11,598. The overall total laptop acquisition cost for the agency is estimated to be $2,730,833.[4]

II. PURPOSE

The audit objective was to evaluate the agency's management of laptop computers, including the effectiveness of NRC's security policies for laptops. Appendix A contains information on the audit scope and methodology.

[4] The overall total acquisition cost was calculated using the active agency laptop inventory listing provided in March 2008 by the Office of Administration. The total acquisition cost is a summation of the purchase price of each agency-owned laptop as listed on the agency's active inventory and does not reflect depreciation values.

III. FINDING

More than 1,300 agency-owned laptops are tracked in the agency's Space and Property Management System. After surveying a sample of these laptops, OIG identified opportunities for improvement in the management of these laptops in the area of security controls.

Addressing these issues will improve the security of NRC's information infrastructure.

SECURITY CONTROLS NOT ADEQUATE

Required security controls over laptops were lacking in headquarters and each of two regional offices where OIG surveyed laptops during this audit. These controls were lacking because the agency has not established clear policies and procedures to implement security requirements.[5] As a result, the agency's laptops are susceptible to viruses and unauthorized use. This could result in the inadvertent release of sensitive NRC information when laptops are connected to the Internet, or it could pose a threat to the secure operation of the agency's network and information when laptops are connected to the NRC local area network (LAN).

Requirements

Federal guidance pertaining to the security and management of Government computers, including laptops, requires agencies to adopt controls that mitigate the risk inherent in laptop usage. Executive Order 13103[6] prohibits the use, acquisition, reproduction, distribution, and transmission of computer software that violates applicable copyright law. The Federal Desktop Core Configuration, a mandated security configuration, requires frequent password changes, no saving of login or password information, and restricted administrative rights.[7]

Additionally, NRC's Management Directive and Handbook (MD) 12.5, *NRC Automated Information Security Program*, states that users shall take appropriate precautions to protect the assets (hardware, software, data) provided for their use or to which they

[5] Policies exist for safeguards information and classified laptops, however, they are not easily understood and cannot be easily implemented.
[6] Executive Order 13103, *Computer Software Piracy*, Effective Date: September 30, 1998.
[7] Administrative rights means the user has the ability to install software and change the computer configuration.

have been granted access (e.g., workstations, microcomputers, local area networks, and associated data). Such precautions include that:

- Users should install virus-checking software on all mobile computers used to access the NRC LAN and download updates at least weekly so that the virus protection remains current.

- Current operating systems are maintained at the most current version.

- Systems shall be configured to display a warning banner[8] to users upon first accessing NRC automated information resources.

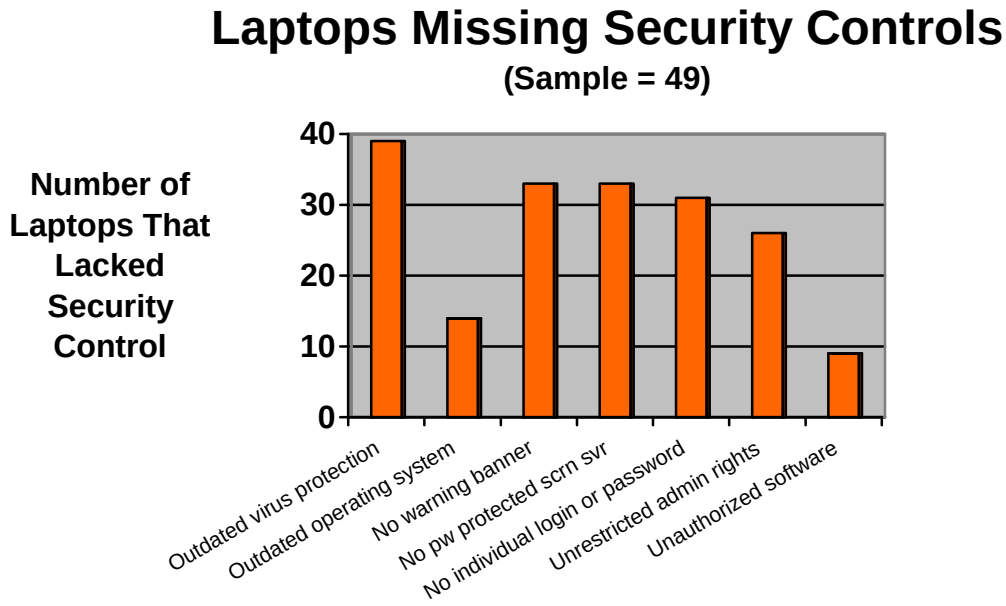
- Users shall ensure that the screen-saver password protection option is selected and the wait time is set to 15 minutes.

- User identifications (ID) must be issued on a one-to-one basis, and group user IDs are not permitted without special authorization.

Inadequate and Inconsistent Security Controls Over Agency-Owned Laptops

OIG auditors surveyed 49 laptops physically located at headquarters, two regional offices, and two resident inspector sites to assess their compliance with Federal and agency security requirements.

[8] A warning banner is information that appears on a computer screen after an individual logs onto a computer. This warning alerts the user of their rights and responsibilities when using the computer and warns against the consequences of unauthorized modification, disclosure, or destruction of agency property and sensitive information.



As the chart shows, the majority of laptops surveyed were not in compliance with Federal and agency-defined security controls. In fact:

- 80 percent (39/49) lacked current[9] virus protection.
- 29 percent (14/49) lacked current operating systems.[10]
- 67 percent (33/49) lacked warning banners.
- 67 percent (33/49) lacked password protected screen savers.
- 63 percent (31/49) lacked individual logins and/or passwords.
- 53 percent (26/49) lacked restricted administrative rights.
- 18 percent (9/49) had unauthorized[11] software downloaded.

[9] For purposes of this audit, the Office of the Inspector General (OIG) considered virus updates to be current if they were downloaded within 30 days of OIG's survey. This is a less stringent requirement than that advised by NRC; NRC guidance states that updates should occur on a weekly basis.

[10] The current operating system is Microsoft Windows XP, Service Pack 2.

[11] Unauthorized software is software that was not tested and approved by the Computer Testing Facility (CTF). A complete listing of tested software and status is available on the CTF Web site (http://nocsb.nrc.gov/).

These problems reflect a longstanding agency issue. OIG previously reported the inadequacy of security controls over agency laptops in OIG audit report 05-A-18, *System Evaluation of Security Controls For Standalone Personal Computers and Laptops,* published in September 2005.[12] To date, the agency has made little progress in improving security controls over laptops. Five of the eight recommendations in that report are still open.

Agency Policies and Procedures Lacking

Agency laptops are non-compliant with Federal and agency security control requirements because NRC has not yet formalized and communicated an agencywide policy for implementing these requirements.[13] Moreover, at headquarters there is limited means to efficiently support the implementation of and adherence to some security control requirements.

In the absence of a formalized policy, some headquarters program and regional offices have employed their own discretion in applying and monitoring implementation of security controls on laptops. This has promoted inconsistency in the application and monitoring of security controls within the agency because there is no formalized mechanism for assigning users responsibility for implementing security controls on laptops. For example, some offices require laptops be turned in to the IT coordinator at least once a year for updating. Others assume that updating laptops is a user responsibility, and provide each user with a user agreement to be signed before taking possession of the laptop.

Furthermore, at headquarters, there is only one secure open port available for users to update their laptops with virus protection and operating system patches from the Internet. NRC restricts the number of open ports to address security risks posed to the NRC network. Additionally, laptop users cannot efficiently or effectively perform these updates without adequate training on the process. A protocol is needed for headquarters users to enable them to quickly and easily update the security controls on their laptops.

[12] OIG-05-A-18 only addressed standalone laptops (laptops that are not configured for connectivity to the NRC LAN).

[13] OIG acknowledges that the agency is currently in the process of developing a "Rules of Behavior Document," which is intended to address security controls such as passwords, virus protection, and software installation. To date, this guidance has not been finalized.

Impact on Agency Network

Because a formalized agencywide policy governing the application and monitoring of security controls has not yet been implemented, agency laptops are not routinely maintained. Consequently, some laptops have inadequate security controls and are therefore susceptible to malware, viruses, and the consequences of unauthorized use. This could result in the inadvertent release of sensitive NRC information when the laptop is connected to the Internet, or it could pose a threat to the secure operation of the agency's network and the information contained therein when connected to the NRC LAN.

Additionally, non-compliance with Executive Order 13103 subjects NRC and its employees and contractors to the consequences of unauthorized software use, such as fines or imprisonment.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Develop agencywide policy and procedures regarding the implementation and monitoring of security controls, especially concerning virus protection and operating system updates, for all agency-owned laptop computers.

2. Communicate the policy in recommendation 1 to the agency when initially complete. Send periodic reminders of the policy requirements, as well as detailed instructions on how to fulfill the requirements.

3. Provide mandatory formal training to all IT coordinators and property custodians on how to update security controls on laptops.

4. Develop a process for verifying that all required security controls are implemented on agency-owned laptops.

5. Develop a protocol to facilitate the efficient and routine updating of agency-owned laptops located at headquarters.

IV. OBSERVATIONS

Property Management Observations

Given the importance of adhering to laptop computer security requirements, it is essential to have a reliable property management program to facilitate monitoring of compliance with agency requirements and industry best practices. During the course of fieldwork, OIG auditors observed issues pertaining to property management practices. OIG is not making formal recommendations to correct these issues; however, these concerns warrant management attention.

Inadequate Management of Safeguards Hard Drives

OIG auditors found no instances of non-compliance with agency requirements regarding hard drives, such as drives that were not locked in a secure container. However, removable safeguards hard drives are not tracked as agency inventory in the agency's property management system.[14] assigned an NRC property tag, or included in the agency's annual property inventory. Safeguards hard drives are small, portable devices that are used to process and store safeguards information.[15] These drives are not tracked as agency inventory because NRC MD 13.1, *Property Management,* requires that only "accountable"[16] property be tracked, and the devices do not fit the agency's definition of "accountable" property.

Consequently, there is the inherent risk of compromising sensitive agency information stored on the safeguards hard drives, especially if the hard drives are inappropriately disposed of at the end of their useful life.

[14] In this context, the term property management system refers to SPMS only; SPMS 4 is the official agency system, although other inventory systems do exist.

[15] Safeguards information means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

[16] Per MD 13.1, accountable property is any equipment, excluding furniture and supplies, that is complete in itself, is of a durable nature with an expected life of at least 2 years, and does not ordinarily lose its identity or become a component of another article, and is not consumed in its useful life.

Inventory Practices Inadequate at Resident Sites and Agreement States

Despite the MD 13.1 requirement that accountable sensitive property be physically inventoried every 2 years, laptops located in resident inspector offices and Agreement States are not physically inspected by regional personnel during the required biennial physical inventory. Instead, verification is obtained verbally when the designated property custodian calls to confirm a laptop's existence. As a result, laptops could be missing for an extended period before being noticed.

NRC Form 119 Incorrectly Completed

MD 13.1 requires that NRC Form 119, *Custodial Receipt for Sensitive Personal Property,* be completed for all sensitive property to document the assignment and custody of the property. When surveying the agency-owned laptop computers, auditors noted instances where NRC Form 119s were incorrectly completed. In one example, forms were not revised when laptops were transferred between staff and/or program offices. In another case, the person listed as being the receiver of the property was incorrect. In light of recent agency reorganizations and continuing office moves, it is prudent to keep accurate records for accountability and tracking purposes.

Contact Information Not Affixed to Agency-Owned Laptops

More than half (29) of the 49 laptops surveyed did not have contact information providing an NRC phone number or return instructions affixed to either the laptop or the laptop case. Although this is not an agency requirement, 20 surveyed laptops did have a contact information sticker. During fieldwork, auditors learned of an instance in which a lost laptop was successfully returned because the finder contacted the agency via the information provided on the contact sticker.

V. AGENCY COMMENTS

At an exit conference on September 23, 2008, NRC officials agreed with the report contents and provided editorial suggestions, which OIG incorporated as appropriate.

VI. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Develop agencywide policy and procedures regarding the implementation and monitoring of security controls, especially concerning virus protection and operating system updates, for all agency-owned laptop computers.

2. Communicate the policy in recommendation 1 to the agency when initially complete. Send periodic reminders of the policy requirements, as well as detailed instructions on how to fulfill the requirements.

3. Provide mandatory formal training to all IT coordinators and property custodians on how to update security controls on laptops.

4. Develop a process for verifying that all required security controls are implemented on agency-owned laptops.

5. Develop a protocol to facilitate the efficient and routine updating of agency-owned laptops located at headquarters.

[Page intentionally left blank.]

SCOPE AND METHODOLOGY

Auditors evaluated the agency's management of agency-owned laptop computers, including the effectiveness of NRC's security policies for its laptop computers. This audit was initiated in response to a request from the agency's Chief Information Officer and was included as a planned audit in the fiscal year 2008 Office of the Inspector General Annual Plan. Additionally, OIG used this audit to revisit issues related to laptop management and security that were identified in OIG audit report OIG-05-A-18, issued on September 22, 2005.

The OIG audit team reviewed relevant Governmentwide criteria, including Federal requirements governing Government-owned or leased computers as noted in Federal Desktop Core Configuration and Executive Order 13103, *Computer Software Piracy*. National Institute of Standards and Technology best practices pertaining to laptop security and management were also considered. Auditors reviewed agency-specific guidance, including MDs 12.5, *NRC Automated Information Security Program*; 12.6, *NRC Sensitive Unclassified Information Security Program*; and 13.1, *Property Management*. Agency-specific best practices, including those listed on the Network Operations and Customer Service Branch Web site, and the Computer Security Awareness Self-Study were reviewed, as well as general prudent business practices. Previously issued OIG audit reports addressing issues related to laptop management and security management practices were also considered.

Auditors interviewed designated agency IT coordinators and property custodians, an Information System Security Officer, and laptop owners in six NRC headquarters offices, four NRC regional offices, and two resident inspector sites.

Auditors surveyed 49 agency-owned laptops selected from the 2008 official agency inventory to determine (1) whether laptops are managed in accordance with Federal and agency standards and best practices, and (2) the consistency by which agency-owned laptops are managed and maintained across offices. To determine which laptops to survey, auditors requested a current official agencywide laptop inventory from the Office of Administration. Laptops were selected randomly from the list. When these laptops were unavailable, auditors selected alternative laptops from another randomly generated list of alternatives taken from the official agency laptop inventory. Various headquarters, regional, and resident inspector site laptops were included in the survey. The results of each survey were documented on an OIG-created

checklist, which was developed in accordance with Federal and agency requirements, standards, and best practices pertaining to laptop management. Auditors analyzed the survey results to determine whether NRC is appropriately and consistently managing the laptops it owns.

This work was conducted from March 2008 through June 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; Terri Cooper, Audit Manager; and Jaclyn Storch, Management Analyst.