OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

System Evaluation of Security Controls
for Standalone Personal
Computers and Laptops

OIG-05-A-18 September 22, 2005

EVALUATION REPORT

All publicly available OIG reports (including this report) are accessible through NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

September 22, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: SYSTEM EVALUATION OF SECURITY CONTROLS FOR STANDALONE PERSONAL COMPUTERS AND LAPTOPS (OIG-05-A-18)

Attached please find the Office of the Inspector General's report *System Evaluation of Security Controls for Standalone Personal Computers and Laptops.* Richard S. Carson and Associates, Inc., conducted this evaluation on our behalf and determined that:

- Security controls for standalone PCs and laptops are not adequate.
- Standalone PCs and laptops are not monitored for compliance with Federal regulations.
- IT coordinators have inconsistent understanding of disposal practices for standalone PCs and laptops.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on August 25, 2005, NRC officials provided comments concerning the draft audit report, which were incorporated into the report as appropriate. After reviewing the modifications, the agency opted not to submit formal written comments to this report.

If you have any questions or wish to discuss this report, please call me at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety andT Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
William N. Outlaw, Acting Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

Office of the Inspector General
Evaluation of Security Controls for
Standalone Personal Computers and Laptops

Contract Number: GS-00F-0001N
Delivery Order Number: DR-36-03-346

September 21, 2005

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include (1) an independent evaluation of an agency's information security program and practices and (2) an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines.

As part of the FY 2005 FISMA independent evaluation of the Nuclear Regulatory Commission's (NRC) automated information security program, Richard S. Carson and Associates, Inc. (Carson Associates), reviewed security controls for standalone personal computers (PCs) and laptops.

PCs and laptops used at NRC are either (1) connected to the NRC local area network (LAN) or (2) used as standalone[1] systems. Some of the standalone PCs and laptops are used to process safeguards[2] and/or classified[3] information. These are considered "listed systems."[4] PCs and laptops connected to the NRC LAN are protected by the LAN's security controls. The evaluation of security controls for listed systems was reported in OIG-05-A-14, "Office of the Inspector General System Evaluation of Listed Systems That Process Safeguards and/or Classified Information," dated August 4, 2005.

There are approximately 4,100 PCs and laptops connected to the NRC LAN, and there are approximately 117 standalone PCs and laptops that are used to process safeguards and/or classified information. However, the number of standalone PCs and laptops that do not process safeguards and/or classified information is unknown, as these standalone PCs and laptops are not tracked in a central location. Findings in this report pertain primarily, but not exclusively, to NRC's standalone PCs and laptops that are not used to process safeguards and/or classified information.

[1] For the purposes of this evaluation, standalone refers to a PC or laptop that is not configured for connectivity to the NRC LAN. Standalone PCs or laptops that are not used to process safeguards and/or classified information may be connected to the Internet, for example when an employee is on travel.

[2] Safeguards information is sensitive unclassified information that specifically identifies the (1) detailed security measures of a licensee or an applicant 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. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

[3] Classified information is information (such as a document or correspondence) that is designated National Security Information, Restricted Data, or Formerly Restricted Data.

[4] Listed systems represent one of four categories used by NRC to group the agency's systems on its master inventory of systems. A listed system is a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application when viewed from an agency perspective.

PURPOSE

The objective of this review was to evaluate the effectiveness of NRC security policies, procedures, practices, and controls for standalone PCs and laptops.

RESULTS IN BRIEF

Carson Associates evaluated the security policies, procedures, practices, and controls for standalone PCs and laptops and found that:

- Security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate.
- Standalone PCs and laptops that are not used to process safeguards and/or classified information are not monitored for compliance with Executive Order 13103, *Computer Software Piracy*.
- IT coordinators' understanding of disposal practices for standalone PCs and laptops that are used to process safeguards and/or classified information is inconsistent.

Security Controls For Standalone PCs and Laptops Are Not Adequate

Security controls for PCs and laptops are typically provided by the network to which they are connected. However, some NRC PCs and laptops are not connected to the NRC LAN and, subsequently, fail to benefit from security controls provided by the LAN. Carson Associates found that security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate. For example, updates to virus definitions and operating system software are not always performed. Security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate because users are not given sufficient guidance on implementing security controls and the agency lacks a mechanism for assigning users responsibility for implementing security controls on these PCs and laptops. In addition, the agency lacks procedures for verifying that all required security controls are being implemented on standalone PCs and laptops that are not used to process safeguards and/or classified information. Inadequate security controls, such as the lack of updated virus definitions and operating system updates, could result in the inadvertent release of sensitive NRC information when a standalone PC or laptop that is not used to process safeguards and/or classified information is connected to the Internet.

Standalone PCs and Laptops Are Not Monitored for Compliance with Executive Order 13103

Executive Order 13103, *Computer Software Piracy*, requires all executive agencies to ensure compliance with applicable copyright laws. The agency monitors for compliance PCs and laptops that are connected to the NRC network and has procedures in place to monitor standalone PCs and laptops that are used to process safeguards and/or classified

information. However, the agency does not have any procedures for monitoring compliance of standalone PCs and laptops that are not used to process safeguards and/or classified information and are not covered by the Infrastructure Services and Support Contract (ISSC).[5] As a result, the agency does not know its degree of compliance with software licenses for all standalone PCs and laptops, which makes NRC, its employees, and its contractors vulnerable to the consequences of unauthorized software use. Such consequences could include fines and even imprisonment.

IT Coordinators' Understanding of Disposal Practices for Standalone PCs and Laptops Is Inconsistent

Management Directive (MD) and Handbook 2.6, *Information Technology Infrastructure*, describe the procedures for equipment removal requests. These procedures apply only to information technology (IT) equipment that is not used to process safeguards and/or classified information. The National Security Agency (NSA) has developed policies and guidance for the proper disposal of IT equipment used to process classified information. MD and Handbook 12.2, *NRC Classified Information Security Program*, and MD and Handbook 12.6, *NRC Sensitive Unclassified Security Program*, describe procedures for handling classified and safeguards[6] information. MD and Handbook 12.5, *NRC Automated Information Security Program*, also describe procedures for processing safeguards and classified information. Carson Associates found that the disposal procedures described by the IT coordinators for standalone PCs and laptops that are used to process safeguards and/or classified information were inconsistent and not always in accordance with policy and guidance from NSA and NRC. Disposal practices described by the IT coordinators for standalone PCs and laptops that are used to process safeguards and/or classified information are inconsistent because the NRC MD and Handbooks that compose Volume 12, Security, do not clearly describe the disposal process and who is responsible for administration of the disposal process. Without clearly defined procedures for the disposal of standalone PCs and laptops that are used to process safeguards and/or classified information, the agency may not be in compliance with policy and guidance from NSA.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve the security controls for standalone PCs and laptops. A consolidated list of recommendations appears on page 11 of this report.

[5] The ISSC provides NRC with a variety of infrastructure services and support, including seat management. The term seat management is typically used to describe an information technology outsourcing approach for acquiring services from a single source in support of a desktop computing environment.

[6] NRC has determined that requirements for protecting safeguards data will be equivalent to those requirements for classified data at the Confidential level.

AGENCY COMMENTS

The Office of the Inspector General (OIG) provided this report in draft to agency officials and discussed its content at an exit conference on August 25, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

ABBREVIATIONS AND ACRONYMS

Carson Associates	Richard S. Carson and Associates, Inc.
DFS	Division of Facilities and Security
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISSC	Infrastructure Services and Support Contract
IT	Information Technology
LAN	Local Area Network
MD	Management Directive
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSIR	Office of Nuclear Security and Incident Response
NTISSAM	National Telecommunication and Information Systems Security Advisory Memorandum
OIG	Office of the Inspector General
OIS	Office of Information Services
PC	Personal Computer
SANS	System Administration, Audit, Network, Security

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002, which included FISMA.[7] FISMA outlines the information security management requirements for agencies, which include (1) an independent evaluation of an agency's information security program and practices and (2) an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines.

As part of the FY 2005 FISMA independent evaluation of NRC's automated information security program, Carson Associates reviewed security controls for standalone PCs and laptops.

PCs and laptops used at NRC are either (1) connected to the NRC LAN or (2) used as standalone systems. Some of the standalone PCs and laptops are used to process safeguards and/or classified information. These are considered "listed systems." PCs and laptops connected to the NRC LAN are protected by the LAN's security controls. The evaluation of security controls for listed systems was reported in OIG-05-A-14, "Office of the Inspector General System Evaluation of Listed Systems That Process Safeguards and/or Classified Information," dated August 4, 2005.

There are approximately 4,100 PCs and laptops connected to the NRC LAN, and there are approximately 117 standalone PCs and laptops that are used to process safeguards and/or classified information. However, the number of standalone PCs and laptops that do not process safeguards and/or classified information is unknown, as these standalone PCs and laptops are not tracked in a central location. Findings in this report pertain primarily, but not exclusively, to NRC's standalone PCs and laptops that are not used to process safeguards and/or classified information.

2 Purpose

The objective of this review was to evaluate the effectiveness of NRC security policies, procedures, practices, and controls for standalone PCs and laptops.

3 Findings

Carson Associates evaluated the security policies, procedures, practices, and controls for standalone PCs and laptops and found that:

- Security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate.

[7] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347), and replaces the Government Information Security Reform Act, which expired in November 2002.

- Standalone PCs and laptops that are not used to process safeguards and/or classified information are not monitored for compliance with Executive Order 13103, *Computer Software Piracy*.
- IT coordinators' understanding of disposal practices for standalone PCs and laptops that are used to process safeguards and/or classified information is inconsistent.

3.1 Security Controls For Standalone PCs and Laptops Are Not Adequate

Security controls for PCs and laptops are typically provided by the network to which they are connected. However, some NRC PCs and laptops are not connected to the NRC LAN and, subsequently, fail to benefit from security controls provided by the LAN. MD and Handbook 12.5, *NRC Automated Information Security Program*, state that users shall take appropriate precautions to protect the assets (hardware, software, data) provided for their use or to which they have been granted access (e.g., workstations, microcomputers, LANs, and associated data). MD and Handbook 12.5 also state that users should install virus-checking software on all mobile or home computers used to access the NRC LAN and download updates at least weekly so that the virus protection remains current.

MD and Handbook 13.1, *Property Management*, require users to sign NRC Form 119, "Custodial Receipt for Sensitive Personal Property," before receiving custody of sensitive equipment.[8]

3.1.1 Standalone PCs and Laptops Used to Process Safeguards and/or Classified Information

The evaluation of security controls for listed systems was reported in OIG-05-A-14, "Office of the Inspector General System Evaluation of Listed Systems That Process Safeguards and/or Classified Information," dated August 4, 2005. Each standalone PC or laptop used to process safeguards and/or classified information requires a security plan that describes the security controls in place for the PC or laptop. The security plan describes the required security controls, including requirements for updating virus and operating system software. The evaluation found that some security controls for standalone PCs and laptops that are used to process safeguards and/or classified information are not being implemented as required because the agency has no procedures in place for verifying that security controls described in a system's security plan are actually being implemented.

[8] Sensitive equipment is any accountable property that is desirable for personal use and can be easily removed from the premises.

3.1.2 Standalone PCs and Laptops Not Used to Process Safeguards and/or Classified Information

Carson Associates met with IT coordinators from 3 out of 30 NRC offices[9] and found that security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate. The three IT coordinators interviewed for this report stated that users are required to sign a Form 119, "Custodial Receipt for Sensitive Personal Property," when assigned a standalone PC or laptop. NRC Form 119 is used to establish responsibility for the physical protection and safekeeping of sensitive items, but does not provide users with guidance on implementing security controls on the PC or laptop and does not assign the user responsibility for implementing security controls on the PC or laptop. None of the offices contacted for this evaluation have procedures in place for verifying that all required security controls are being implemented on standalone PCs and laptops that are not used to process safeguards and/or classified information. The following are two security controls that were found to be inadequate for standalone PCs and laptops that are not used to process safeguards and/or classified information.

- **Virus Updates.** IT coordinators in the three offices contacted by Carson Associates described varying practices employed by their office to ensure virus software updates are performed on a routine basis. In one office, virus updates are not performed on standalone PCs and laptops, primarily because users view the requirement as cumbersome and difficult to achieve for PCs and laptops that are not connected to the NRC LAN. Users in another office are sometimes given verbal instructions on how to download and install the updates. A third office is currently developing rules of behavior[10] that users must sign when given a laptop or PC. The rules of behavior include a requirement to update the virus definitions at the beginning of each usage session, but provide no guidance on how to perform the updates. The requirement to sign these rules of behavior has not been fully implemented, and users in this office are not currently provided guidance on the installation of virus updates.
- **Software Updates.** None of the three offices contacted by Carson Associates (1) notify users that they are responsible for performing software updates on standalone PCs or laptops or (2) provide any guidance on how to perform the updates. PCs and laptops can be configured to perform automatic operating system updates when new updates are available. Updates would occur only when the standalone PC or laptop is connected to the Internet. However, users are not informed that this feature is enabled or that they should periodically connect to the Internet to ensure installation of the latest updates. Furthermore, they are not notified they should not disable the automatic update feature or

[9] Carson Associates focused on meeting with IT coordinators for offices that have standalone PCs and laptops that are used to process safeguards and/or classified information. Of the 30 offices listed on the IT coordinators contact sheet, only 10, plus the 4 regions, have standalone PCs and laptops that meet this criteria. Carson Associates did not include any IT coordinators from the regions as we wanted to conduct face-to-face interviews. In addition to the three IT coordinators Carson Associates met with, we contacted IT coordinators for another five offices. Of the five, three did not return our phone call, and two referred us to another point of contact, but not in enough time to arrange an interview. We feel that by including the Office of Nuclear Material Safety and Safeguards and the Office of Nuclear Regulatory Research we covered offices with many of the standalone PCs and laptops.

[10] These draft rules of behavior can be found in Appendix B.

change the frequency of the automatic updates. As noted above, one office is currently developing rules of behavior that include a requirement to leave automatic updating turned on and configured to update every 24 hours. However, the requirement to sign these rules of behavior has not been fully implemented, and users in this office are not currently provided guidance on performing software updates.

Security controls for standalone PCs and laptops that are not used to process safeguards and/or classified information are not adequate because users are not given sufficient guidance on implementing security controls and the agency lacks a mechanism for assigning users responsibility for implementing security controls on these PCs and laptops. In addition, the agency lacks procedures for verifying that all required security controls are being implemented on standalone PCs and laptops that are not used to process safeguards and/or classified information.

Although standalone PCs and laptops are not connected to the NRC LAN, PCs and laptops that are not used to process safeguards and/or classified information may be connected to the Internet. This is particularly so for laptops used during travel. While these standalone PCs and laptops do not process safeguards or classified information, they may be used to process sensitive but unclassified information. Inadequate security controls, such as the lack of updated virus definitions and operating system updates, could result in inadvertent release of sensitive NRC information when a standalone PC or laptop that is not used to process safeguards and/or classified information is connected to the Internet. The SANS Internet Storm Center (part of the SANS Institute) continuously monitors the average time (survival time) it takes for an unprotected PC (i.e., missing critical security patches and no firewall) running Microsoft Windows to be compromised after being connected to the Internet.[11] In June 2005, the average survival time was only 25 minutes.

As noted above, one office is developing rules of behavior that serve as an agreement between the employee and the agency to ensure security controls are implemented as required. Rules of behavior such as these serve as one mechanism for conveying to users their responsibility for implementing security controls for standalone PCs and laptops.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Provide users guidance for implementing security controls on standalone PCs and laptops.
2. Develop and require users to sign a rules of behavior agreement accepting responsibility for implementing security controls on standalone PCs and laptops.
3. Develop and implement procedures for verifying all required security controls are implemented on standalone PCs and laptops.

[11] http://isc.sans.org/survivalhistory.php

3.2 Standalone PCs and Laptops Are Not Monitored for Compliance with Executive Order 13103

Executive Order 13103, *Computer Software Piracy*, requires all executive agencies to ensure compliance with applicable copyright laws.[12] The agency monitors for compliance PCs and laptops that are connected to the NRC network. MD and Handbook 12.5 state users shall not install any computer program into the NRC computing environment if there is any question that the computer program may not be properly licensed. MD and Handbook 12.5 also require users to obtain approval and adhere to software copyright laws before installing software on NRC systems, including standalone PCs and laptops. Users must comply with software copyright license laws and policies that prohibit unauthorized use or copying of commercial software.

3.2.1 Standalone PCs and Laptops Used to Process Safeguards and/or Classified Information

As noted previously, the evaluation of security controls for listed systems was reported in OIG-05-A-14. The security plan required for standalone PC or laptop used to process safeguards and/or classified information states that the configuration of the laptop is controlled by the information systems security officer (ISSO) for the standalone PC or laptop. The ISSO is responsible for installing and performing updates to software. Users of the laptop are required to sign an acknowledgment indicating their complete understanding of the plan.

3.2.2 Standalone PCs and Laptops Not Used to Process Safeguards and/or Classified Information

Carson Associates met with IT coordinators from 3 out of 30 NRC offices and found there are no procedures in place for facilitating or monitoring compliance with Executive Order 13103 for standalone PCs and laptops that do not process safeguards and/or classified information and are not covered by the ISSC.

IT coordinators in two offices do not inform users not to install other software and have no mechanism for monitoring compliance with Executive Order 13103. When issuing a standalone PC or laptop, one office's IT coordinator informs users not to install other software. This office is developing rules of behavior that users must sign when given a laptop or PC. The rules include a requirement not to load unapproved applications on the PC or laptop, and include a statement that the PC or laptop can be called in for inspection at any time to check for compliance with the rules of behavior. However, the requirement to sign these rules of behavior has not been fully implemented.

Standalone PCs and laptops that are not used to process safeguards and/or classified information are not monitored for compliance with Executive Order 13103 because they are not connected to the NRC LAN and there is no mechanism in place for monitoring standalone PCs and laptops that are not covered by the ISSC. As a result, the agency does not know its degree of compliance

[12] Copyright Law is contained in Title 17 of the United States Code. The Copyright Revision Act of 1976 (Public Law 94-553), effective January 1, 1978, was amended in 1980 to include computer software under the category of "literary works."

with software licenses for standalone PCs and laptops, which makes NRC, its employees, and its contractors vulnerable to the consequences of unauthorized software use. Such consequences could include fines and even imprisonment.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Provide users guidance on compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
5. Develop and require users to sign a rules of behavior agreement acknowledging their compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
6. Develop and implement procedures for monitoring compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.

3.3 IT Coordinators' Understanding of Disposal Practices for Standalone PCs and Laptops Is Inconsistent

MD and Handbook 2.6, *Information Technology Infrastructure*, describe the procedures for IT equipment removal requests. IT coordinators should make requests for removal of excess desktop workstations and related hardware to the Office of Information Services (OIS) Customer Support Center or through an Office of Administration Labor Services request.[13] Equipment is taken to a specific room on the 2nd floor of One White Flint where OIS staff sort, redistribute, or arrange for disposal of the items. OIS staff either wipe[14] hard drives with an overwrite process or, if that is not possible, remove and destroy the hard drive. These procedures apply only to IT equipment that is not used to process safeguards and/or classified information.

According to the National Telecommunication and Information Systems Security Advisory Memorandum (NTISSAM), dated January 16, 1987, when an office automation system (i.e., a PC or laptop) has outlived its usefulness and has become obsolete, or when it has become damaged beyond repair, it must be disposed of properly. If the system has been used to process or store classified or sensitive, but unclassified, information (i.e., safeguards), certain precautions should be taken before the system can be disposed of through normal channels. These precautions will help to prevent the compromise of any classified or sensitive, but unclassified, information remaining in the system after it is beyond the control of the organization that once used it. The NTISSAM states that any removable media that once contained classified or sensitive but unclassified information that is not going to be reused should be either declassified or destroyed.

[13] NRC Form 30, Request for Administrative Services, is used to submit a Labor Services request.

[14] "Wipe" is a term used to describe a process for removing sensitive data from a hard drive in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities. Overwriting, which is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data, is a common method of "wiping" a hard drive.

The National Computer Security Center "A Guide to Understanding Data Remanence in Automated Information Systems," dated September 1991, defines declassification as a procedure and an administrative action to remove the security classification of the subject media. The procedural aspect of declassification is the actual purging[15] of the media and removal of any labels denoting classification, possibly replacing them with labels denoting that the storage media is unclassified. The guide also states that purging must be used when media is released from a secure facility to a non-cleared maintenance facility or similar non-secure environment. The NSA approves methods for purging media.

MD and Handbook 12.2, *NRC Classified Information Security Program*, and MD and Handbook 12.6, *NRC Sensitive Unclassified Security Program*, describe procedures for handling classified and safeguards information. MD and Handbooks 12.2 and 12.6 only discuss disposal of safeguards and/or classified waste that can be destroyed by shredding. The MDs and Handbooks do not describe disposal procedures for electronic media, such as hard drives (fixed and removable) used to process classified and/or safeguards information, nor do they refer the reader to the MDs and Handbooks in Volume 12, Security, that do describe the appropriate disposal methods for hard drives that were used to process classified and/or safeguard information.

MD and Handbook 12.5, *NRC Automated Information Security Program*, also describe procedures for processing safeguards and classified information. MD and Handbook 12.5 state that special approaches should be used to delete safeguards and classified data from electronic storage media. These approaches may include destruction of the physical media, obliteration of the sensitive data through the use of an approved software product, or erasure of all data through degaussing.[16] Questions regarding the appropriate method for eliminating safeguards or classified data from a storage medium should be referred to the Computer Security Staff.

3.3.1 Standalone PCs and Laptops Used to Process Safeguards and/or Classified Information

Carson Associates met with IT coordinators from three NRC offices and spoke with staff from the Division of Facilities and Security (DFS) and the Office of Nuclear Security and Incident Response (NSIR) regarding the disposal of removable hard drives used in standalone PCs and laptops that are used to process safeguards and/or classified information. The three IT coordinators interviewed have not actually disposed of any standalone PCs or laptops that are used to process safeguards and/or classified information. However, they described the procedures they would follow if the situation arises.

Carson Associates found that the disposal procedures described by the IT coordinators for standalone PCs and laptops that are used to process safeguards and/or classified information were inconsistent and not always in accordance with policy and guidance from NSA and NRC.

[15] Purging is the removal of sensitive data from an automated information system in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed through open-ended laboratory techniques.

[16] Degaussing is a procedure that uses specialized devices that generate a magnetic field used to render any previously stored data on magnetic media unreadable.

- One IT coordinator stated they would instruct the PC/laptop user to erase any sensitive information from the PC/laptop before returning it. The IT coordinator would then check the laptop for any sensitive files or folders, and then remove them before following the equipment removal procedures described in MD and Handbook 2.6. The procedures described by this IT coordinator are not in compliance with the guidance described above.
- Another IT coordinator stated they would use software to wipe the drive and then ask the OIS Computer Security Staff what to do with the PC/laptop. This procedure is in compliance with the guidance described above, but only if the IT coordinator has the proper clearance for handling the type of data stored on the PC or laptop.
- Another IT coordinator stated they would use an Office of Administration Labor Services request specifying the equipment be sent to DFS. MD and Handbook 12.5 have separate sections that discuss processing safeguards and/or classified information (sections 2.6.2 and 2.6.3 respectively). Section 2.6.2 states that all media must be properly labeled, stored, sanitized, and disposed of as specified in MD 12.2, and Section 2.6.3 states that disks, diskettes, ribbons, and printouts must be disposed of in accordance with MD 12.6. However, as stated previously, MD and Handbooks 12.2 and 12.6 do not describe procedures for disposal of magnetic media, nor do they refer the reader to the MDs and Handbooks that do describe the appropriate disposal methods. Destruction of storage media is not discussed in MD and Handbook 12.5 until Section 2.6.12. A reader unfamiliar with MD and Handbook 12.5 who is interested in disposal procedures for electronic media that are used to process safeguards and/or classified information may not read all of MD and Handbook 12.5, but only read Sections 2.6.2 and 2.6.3. There are two places in Section 2.6.12 that discuss disposal of electronic media. The first statement in Section 2.6.12 pertaining to disposal of electronic media is that "removable magnetic storage media, such as diskettes and tapes that contain classified or sensitive information, should not be disposed of in regular waste containers. These media should be sent to DFS for retention or destruction." It is unclear whether this statement applies to hard drives, as a hard drive is not something that is typically disposed of in a regular waste container. The second statement in Section 2.6.12 pertaining to disposal procedures is "if hard disk drives are removed from or replaced in a workstation, the hard drive that is removed should be unconditionally formatted before removal. If this is not possible, hard disks should be degaussed or sent to DFS for retention or destruction." It is not clear whether this statement applies to all hard disk drives, or only those that do process safeguards and/or classified information. The term "unconditionally formatted" is also not defined.
- In comments provided to the OIG, the agency stated that DFS has an arrangement with the NSA for the disposal of hard drives and media. This arrangement was mentioned by more than one staff member contacted during this evaluation; however the agency has no documentation to support the existence of this arrangement.

Carson Associates also spoke with a staff member from NSIR to discuss that office's disposal procedures. NSIR requires that all equipment used to process classified information have their hard drives removed before the equipment can be removed from NSIR. In the past, disposal of the hard drives was coordinated with a member of the OIS Computer Security Staff. This

individual no longer works in this position; subsequently, NSIR is storing the hard drives in an approved storage container until arrangements can be made for their disposal.

Disposal practices described by the IT coordinators for standalone PCs and laptops that are used to process safeguards and/or classified information are inconsistent because the NRC MDs and Handbooks that compose Volume 12, Security, do not clearly describe the disposal process and who is responsible for administration of the disposal process. For example, MD and Handbooks 12.2 and 12.6 state that DFS "plans, develops, establishes, and administers policies, standards, and procedures" for the NRC classified and sensitive unclassified information security programs. However, MD and Handbook 12.1 state that NSIR is responsible for administering the information security programs, and MD and Handbook 12.5 state that NSIR is responsible for managing NRC information security programs that specifically deal with the classification, declassification, and handling of classified, safeguards, and sensitive information. In comments provided to the OIG, the agency stated that DFS is responsible for the development and administration of policies, standards, and procedures for destruction of classified and sensitive information; however this fact is not clearly stated in any of the MDs and Handbooks that compose Volume 12.

Another example of unclear guidance is in the security plan templates required for standalone PCs and laptops used to process safeguards and/or classified information. Both templates refer the reader back to MD and Handbooks 12.2 and 12.6 for procedures on the destruction of magnetic media containing safeguards and/or classified information. However, as stated previously, MD and Handbooks 12.2 and 12.6 do not describe procedures for disposal of magnetic media, nor do they refer the reader to the MDs and Handbooks that do describe the appropriate disposal methods.

Without clearly defined procedures for the disposal of standalone PCs and laptops used to process classified information, the agency may not be in compliance with policy and guidance from NSA.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

7. Develop detailed procedures in the appropriate Management Directives for the disposal of equipment used to process safeguards and/or classified information. These procedures should then be referenced in the appropriate chapters of the Volume 12 series of directives.
8. Include the procedures for the disposal of equipment containing safeguards and/or classified information in the security plan templates.

3.3.2 Standalone PCs and Laptops Not Used to Process Safeguards and/or Classified Information

The three IT coordinators Carson Associates interviewed for this evaluation follow the disposal process described MD and Handbook 2.6 for disposing standalone PCs and laptops not used to process safeguards and/or classified information. Carson Associates also met with staff from OIS responsible for handling IT equipment sent for disposal and verified that OIS maintains logs of incoming and outgoing equipment.

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Provide users guidance for implementing security controls on standalone PCs and laptops.
2. Develop and require users to sign a rules of behavior agreement accepting responsibility for implementing security controls on standalone PCs and laptops.
3. Develop and implement procedures for verifying all required security controls are implemented on standalone PCs and laptops.
4. Provide users guidance on compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
5. Develop and require users to sign a rules of behavior agreement acknowledging their compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
6. Develop and implement procedures for monitoring compliance with Executive Order 13103, *Computer Software Piracy*, for standalone PCs and laptops.
7. Develop detailed procedures in the appropriate Management Directives for the disposal of equipment used to process safeguards and/or classified information. These procedures should then be referenced in the appropriate chapters of the Volume 12 series of directives.
8. Include the procedures for the disposal of equipment containing safeguards and/or classified information in the security plan templates.

5 OIG Response to Agency Comments

OIG provided this report in draft to agency officials and discussed its content at an exit conference on August 25, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

SCOPE AND METHODOLOGY

To perform the evaluation of the NRC security policies, procedures, practices, and controls for PCs and laptops, Carson Associates reviewed NRC policies on automated information systems security, information technology infrastructure, and property management. Carson Associates interviewed staff responsible for the ISSC, property management, and property disposal, and met with IT coordinators from three NRC offices.

One area of particular concern addressed in this evaluation was disposal procedures for standalone PCs and laptops that are used to process safeguards and/or classified information. Carson Associates reviewed several NRC management directives in order to understand the disposal procedures. Our review focused primarily on the Volume 12, Security, series of management directives. Volume 12 comprises the following management directives and handbooks:

- 12.1, *NRC Facility Security Program,* April 14, 2004
- 12.2, *NRC Classified Information Security Program,* April 27, 1999
- 12.3, *NRC Personnel Security Program,* April 27, 2004
- 12.4, *NRC Telecommunications Systems Security Program,* December 8, 1999
- 12.5, *NRC Automated Information Security Program,* September 12, 2003
- 12.6, *NRC Sensitive Unclassified Information Security Program,* December 20, 1999

Carson Associates also reviewed the following management directives and handbooks:

- 2.6, *Information Technology Infrastructure,* March 7, 2005
- 13.1, *Property Management,* January 14, 2002

The work was conducted from June 2005 to August 2005 in accordance with guidelines from the National Institute of Standards and Technology, and best practices for evaluating security controls. Jane Laroussi from Carson Associates conducted the work.

[Page intentionally left blank]

Rules of Behavior for Government Furnished Laptops, PDAs, and Cell Phones and Other Small, Portable Electronic Devices

1.0 Introduction

The United States Nuclear Regulatory Commission has purchased the item described below for the use of the identified NRC employee below in accomplishing her or his mission. The purpose of this "Rules of Behavior" agreement between the employee and the agency is to help ensure that the item is used in a manner consistent with information security and compliance NRC management directives and Federal requirements (e.g., FISMA).

Some sections of this agreement may not apply because the device or item does not have the listed capability. In that case, simply cross out that section and write "does not apply" next to the section.

2.0 Name of the Employee to whom this agreement applies

2.1 Employee Name: _____

2.2 Employee Room Number: _____

2.3 Employee Phone Number: _____ _____

3.0 Description of the Item:

3.1 Item Description: _____
(i.e., Dell Laptop, Palm PDA, etc.)

3.2 Item's NRC Tag Number: _____

3.3 Item's Location: _____

4.0 Employee Behavior Requirements

4.1 For items with built-in camera components

In accordance with MD 12.1, Part II, (A)(iii), "Use of the camera component of the equipment inside NRC buildings is prohibited without the prior approval by the Director, DFS."

I agree not to use within the NRC Headquarters complex or any NRC regional office the camera component of the item described in section 3.0 above, which was purchased with NRC funds for official business use, without the prior approval of the Director, Division of Facilities and Security. Further, I will assure that the camera component will be securely stored and carefully accounted for and that all individuals who may have access to or may use the equipment have also been advised of restrictions with respect to its use.

4.2 For items with Blue Tooth

The RES/PMDA staff has delivered the item with Blue Tooth disabled. I agree to leave the blue tooth capability of the device disabled.

4.3 For items with wireless capability (e.g., laptops or PDAs with 802.11a, b, or g {or newer} capability.)

The RES/PMDA staff has delivered the item with wireless network access disabled. I agree to leave the wireless capability of the device disabled.

4.4 Norton Antivirus

The RES/PMDA staff has delivered the item with Norton Antivirus installed and updated. I agree to update the Norton Antivirus signatures at the beginning of each usage session.

4.5 Windows Update

The RES/PMDA staff has delivered the item with automatic windows updating turned on and with a frequency of update of once every 24 hours. I agree to leave the automatic windows updating turned on and configured to update every 24 hours.

4.6 Use only of Approved Software Applications

The RES/PMDA staff has delivered this item with only approved software applications on the device. I agree not to load unapproved or unlicensed applications on the device. This includes games, American Online Software, and Instant Messaging Software.

5.0 Rules of Behavior Agreement and Signature

I, _____, agree to abide by these rules of behavior. I understand that at any time, RES/PMDA staff may call in the device/item covered by this agreement and inspect it for compliance with this agreement. I agree to fully cooperate in such inspections by making the device available to RES/PMDA staff at NRC headquarters.

_____ _____
Signature Date

[Page intentionally left blank]