U.S. Nuclear Regulatory Commission
Laptop Security Policy

1 PURPOSE

This U.S. Nuclear Regulatory Commission (NRC) Laptop Security Policy provides requirements for laptop security controls that serve to minimize the probability of NRC information compromise. This policy is effective at the date of issuance for all new laptop purchases, procurements, and managed services contracts that include laptops as part of a procurement or acquisition. Laptop system owners must ensure that all existing laptops meet the requirements of this policy within one year from the date of issuance of this policy or are disposed of in accordance with NRC security requirements.

All new contracts and contract modifications must contain requirements to abide by this policy. All existing contracts must be modified by January 1, 2012, to include these requirements. Security of NRC laptops is the responsibility of a system owner. All NRC laptops must either be designated a system or be included as part of an existing system. System owners are office directors, regional administrators, and Office of Information Services division directors.

2 APPLICABILITY

This NRC Laptop Security Policy applies to all NRC laptops owned, managed, and/or operated by the NRC or by other parties on behalf of the NRC, except as noted below. This policy will be incorporated into the next revision of Management Directive (MD) 12.5, "NRC Automated Information Security Program."

This policy does not apply to sensitive compartmented information systems for which the Director of Central Intelligence Directive (DCID) 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," dated December 1, 2005, and DCID 6/3, "Protecting Sensitive Compartmented Information within Information Systems," dated June 5, 1999, apply (i.e., sensitive compartmented information and special access programs for intelligence under the purview of the Director of Central Intelligence).

3 DEFINITIONS

Critical Updates	This includes fixes for security defects in operating systems and applications as well as current anti-virus definitions and other intrusion detection and prevention information
High Water Mark	The highest sensitivity/classification level of any information that has ever been processed by, stored on, or traversed through the system
Privileged user	Users with one or more of the following functions: • system administrators • computer operators • system engineers (i.e., those with control of the operating system or specific application software) • network administrators • database administrators

- those who control user passwords and access levels

Strong or complex password	A password that is at least 12 characters long and includes at least one instance of each of the following uppercase letters, lowercase letters, numbers, and special characters. The Office of Management and Budget (OMB) common security configuration requirements (i.e., Federal Desktop Core Configuration) outlined in OMB Memorandum M-07-18 mandates strong or complex passwords. The password should not be predictable or easily deduced and must not be easily associated with the user, such as names, car registration or tag numbers, and telephone numbers. The password must not be words found in any dictionary, spelled forwards or backwards, and must not be based on a single word (e.g., "Pa$$wOrd).

4 POLICY

This section provides the NRC policy for NRC laptops. As stated in NRC Yellow Announcement (YA) YA-08-0021, personally owned computers may not be used to process or store NRC sensitive information except when using CITRIX/NRC Broadband Remote Access System and NRC sensitive information may not be stored on personally owned computers.

Laptops must be properly tagged as required by MD 13.1, "Property Management." Laptops must be refreshed at least every 4 years. This requires that the old laptop be disposed of in accordance with NRC security requirements and replaced according to the acquisition requirements in place at that time. Disposing of a system requires that all sensitive information be erased from the system so that it is not recoverable, even using computer forensic tools. MD 12.5 provides specific requirements for disposal of equipment.

Each user must have a unique account and username with a strong password for general system usage. Each privileged user must have a unique account and username with a strong password for privileged system usage. Privileged user accounts must only be used for job related activities that require privileges, and privileged users must also have a non-privileged (general user) account if they need to perform general user activities.

Personally owned software shall not be installed on laptops.

All software installed on laptops shall be properly licensed for the intended use.

4.1 Office of Information Services Provided and Managed Laptops

Office of Information Services (OIS) provided and managed laptops are those that are purchased and maintained by the OIS Infrastructure and Computer Operations Division (OIS/ICOD) on behalf of the office that uses the laptops.

All OIS provided and managed laptops that process or access classified national security information belong to the "OIS/ICOD Classified Laptop System" and that system is owned by the director of OIS/ICOD.

All OIS provided and managed laptops that process or access Safeguards Information (SGI) and are not part of the "OIS/ICOD Classified Laptop System" belong to the "OIS/ICOD SGI Laptop System" and that system is owned by the director of OIS/ICOD.

All OIS provided and managed laptops within an office or region that are not part of the "OIS/ICOD Classified Laptop System" and the "OIS/ICOD SGI Laptop System," belong to the "OIS/ICOD General Laptop System" and that system is owned by the director of OIS/ICOD.

4.2 Organization Managed Laptops

Organization managed laptops are those laptops that organizations other than OIS/ICOD purchase and maintain.

All organization managed laptop systems are owned by the organization's office director or regional administrator, and are referenced in this policy as the laptop system owner.

All organization managed laptops that process or access classified national security information belong to that office or region's "Classified Laptop System."

All organization managed laptops that process or access Safeguards Information and are not part of the office or region's "Classified Laptop System" belong to that office or region's "SGI Laptop System."

All organization managed laptops within an office or region that are not part of the office or region's "Classified Laptop System" or the office or region's "SGI Laptop System" belong to that office or region's "General Laptop System."

4.3 Classified Laptop Systems

Classified laptop systems must meet the requirements provided in the "Standard Listed System Security Plan for Stand-alone Personal Computers and Laptops used for Classified Information Processing" available at http://www.internal.nrc.gov/CSO/Classified.html.

Classified laptop systems must be certified by the system owner as being in compliance with the classified laptop system requirements, including the Federal Desktop Core Configuration (FDCC). More information on FDCC can be obtained at the following URL: http://nvd.nist.gov/fdcc/index.cfm. Classified laptop systems must be accredited by the appropriate Designated Approving Authority prior to processing any classified national security information on the system.

Classified laptops shall be classified at the high water mark classification level.

Certification of a classified laptop system requires a system certification memo from the classified laptop system owner. The memo must include an enclosure that provides the names and contact information for the: System Owner, Certification Agent, Information System Security Officer (ISSO), Alternate ISSO, and System Administrator. For each laptop or removable hard drive that is part of the classified laptop system, the enclosure must provide the following information:

- Either a statement that the system will not be removed from NRC facilities or identification of the NSA approved encryption product and encryption technique used to perform full disk encryption on the laptop
- The physical storage location for the laptop. If the system is maintained off-site, the address, room number, and contact information for the site must be provided and the agreement that governs this off-site arrangement must be

attached along with a description of the physical security provided at that location.

- The location where the system is used
- The classification levels processed by the system, including special access controls
- A statement of whether or not privacy information is processed by the system. If privacy information is processed, the types of privacy information processed must be provided along with a copy of the privacy impact assessment performed for the system.
- Laptop brand, model, and NRC tag number
- Compact Disk (CD) and Digital Versatile Disk (DVD) drive brand and model
- Other drive brand and model
- Network card brand and model
- All other peripherals (e.g. scanner, printer) brand, model, and NRC tag number
- Operating system name, version, and service packs installed
- Antivirus software name, version, frequency of updates to signatures, and method of signature update
- Name and version of any other software used on the laptop
- A clear delineation of any additional responsibilities and system specific rules of behavior for all individuals with access to this system, including any rules/processes for properly handling the sensitive information on the laptop, which must state the consequences of inconsistent behavior or noncompliance.

Templates for the required transmittal memo stating the classified laptop system certification and the required enclosure are available at http://www.internal.nrc.gov/CSO/Classified.html

Critical updates shall be applied to the classified laptops at least semi-annually. The need to apply critical updates more frequently will be evaluated by the ISSO at least monthly. This evaluation will take into account the nature of the critical updates issued by the operating system and software vendors, the risk to the system, and the ISSO operational experience with and knowledge of the system.

All users authorized to access each classified laptop must have the need-to-know and required security clearance as verified by the system owner.

Prior to being granted system access, each user is required to read the applicable security plan, the National Industrial Security Program Operating Manual dated February 2006, and the National Telecommunication and Information Systems Security Advisory Memorandum (NTISSAM) on Office Automation Security Guideline (NTISSAM COMPUSEC/1-87) dated January 16, 1987, and sign a statement acknowledging their understanding of the requirements and procedures.

Classified laptops must only connect to classified systems operating at the same classification level. The system owner must approve the connection and include the specific laptop as part of the system.

Classified laptops must only connect to classified systems using techniques and capabilities specifically approved by the NRC Designated Approving Authorities (DAAs) for connecting to the classified system.

The background on each laptop must reflect the classification level processed by the system. Backgrounds can be obtained from:

- Confidential Information Processing: http://www.internal.nrc.gov/CSO/documents/Confidential%20Background.bmp
- Secret Information Processing: http://www.internal.nrc.gov/CSO/documents/Secret%20Background.bmp

4.4 Safeguards Information Laptop Systems

SGI laptop systems must meet the requirements provided in the "Standard Listed System Security Plan for Stand-alone Personal Computers and Laptops used for Safeguards Information Processing" available at http://www.internal.nrc.gov/CSO/SGI.html

SGI laptop systems must be certified by the system owner as being in compliance with the SGI laptop system requirements, including the FDCC. SGI laptop systems must be accredited by the appropriate DAA prior to processing any SGI information on the system.

Certification of an SGI laptop system requires a system certification memo from the SGI laptop system owner. The memo must include an enclosure that provides the names and contact information for the: System Owner, Certification Agent, Information System Security Officer (ISSO), Alternate ISSO, and System Administrator. For each laptop or removable hard drive that is part of the SGI laptop system, the enclosure must provide the following information:

- The National Institutes of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 validated encryption module, including version, as well as the encryption algorithm and key strength used to perform full disk encryption on the laptop
- The physical storage location for the laptop. If the system is maintained off-site, the address, room number, and contact information for the site must be provided and the agreement that governs this off-site arrangement must be attached along with a description of the physical security provided at that location.
- The location where the system is used
- A statement of whether or not privacy information is processed by the system. If privacy information is processed, the types of privacy information processed must be provided along with a copy of the privacy impact assessment performed for the system.
- Laptop brand, model, and NRC tag number
- CD and DVD drive brand and model
- Other drive brand and model
- Network card brand and model
- All other peripherals (e.g. scanner, printer) brand, model, and NRC tag number

- Operating system name, version, and service packs installed
- Antivirus software name, version, frequency of updates to signatures, and method of signature update
- Name and version of any other software used on the laptop
- A clear delineation of any additional responsibilities and system specific rules of behavior for all individuals with access to this system, including any rules/processes for properly handling the sensitive information on the laptop, which must state the consequences of inconsistent behavior or noncompliance.

Templates for the required transmittal memo stating the SGI laptop system certification and the required enclosure are available at http://www.internal.nrc.gov/CSO/SGI.html

Critical updates shall be applied to the SGI laptops at least semi-annually. The need to apply critical updates more frequently will be evaluated by the ISSO at least monthly. This evaluation will take into account the nature of the critical updates issued by the operating system and software vendors, the risk to the system, and the ISSO operational experience with and knowledge of the system.

All users authorized to access each laptop must have the need-to-know and background investigation required by Management Directive 12.3, "NRC Personnel Security Program," as verified by the system owner.

Prior to being granted system access, each user is required to read the applicable security plan and NUREG/BR-0168, Rev. 4, "Policy for Processing Unclassified Safeguards Information on NRC Computers" and sign a statement acknowledging their understanding of the requirements and procedures.

SGI laptops must only connect to SGI systems. The system owner must approve the connection and include the specific laptop as part of the system.

SGI laptops must only connect to SGI systems using techniques and capabilities specifically approved by the NRC DAAs for connecting to the SGI system.

The background on each laptop must reflect the fact that SGI is being processed by the system. The SGI background can be obtained from:
http://www.internal.nrc.gov/CSO/documents/SafeGuards%20Background.bmp

4.5 General Laptop Systems

General laptop systems must meet the requirements provided in the "Standard System Security Plan for Laptop Computers used only for Sensitive Unclassified Non-Safeguards Information (SUNSI) Processing" available at http://www.internal.nrc.gov/CSO/General.html

General laptop systems must be certified by the system owner as being in compliance with the general laptop system requirements, including the FDCC, prior to processing any SUNSI information on the system.

Certification of a general laptop system requires a system certification memo from the general laptop system owner. The memo must include an enclosure that provides the names and contact information for the: System Owner, Certification Agent, Information System Security

Officer (ISSO), Alternate ISSO, and System Administrator. For each laptop or removable hard drive that is part of the SGI laptop system, the enclosure must provide the following information:

- The National Institutes of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 validated encryption module, including version, as well as the encryption algorithm and key strength used to perform full disk encryption on the laptop
- The physical storage location for the laptop. If the system is maintained off-site, the address, room number, and contact information for the site must be provided and the agreement that governs this off-site arrangement must be attached along with a description of the physical security provided at that location.
- The location where the system is used
- A statement of whether or not privacy information is processed by the system. If privacy information is processed, the types of privacy information processed must be provided along with a copy of the privacy impact assessment performed for the system.
- Laptop brand, model, and NRC tag number
- CD and DVD drive brand and model
- Other drive brand and model
- Network card brand and model
- All other peripherals (e.g. scanner, printer) brand, model, and NRC tag number
- Operating system name, version, and service packs installed
- Antivirus software name, version, frequency of updates to signatures, and method of signature update
- Name and version of any other software used on the laptop
- A clear delineation of any additional responsibilities and system specific rules of behavior for all individuals with access to this system, including any rules/processes for properly handling the sensitive information on the laptop, which must state the consequences of inconsistent behavior or noncompliance.

Templates for the required transmittal memo stating the system certification and the required enclosure are available at http://www.internal.nrc.gov/CSO/General.html

Critical updates shall be applied to the general laptops at least weekly or if the laptop is not used weekly, upon first use after a week without use. The need to apply critical updates more frequently will be evaluated by the ISSO at least monthly. This evaluation will take into account the nature of the critical updates issued by the operating system and software vendors, the risk to the system, and the ISSO operational experience with and knowledge of the system. Laptops can be set to automatically install critical updates, particularly for the operating system and products such as Microsoft Office. Since the laptops are not used as desktops, this should minimize the potential for incompatibility with other software.

General laptops shall not directly connect to the NRC operational network unless a specific written approval for direct connection has been obtained from the Director of OIS/ICOD and has been made an official record.

General laptops may be used for remote access to the NRC operational network using broadband Citrix. Other types of connections must be via specific remote access implementations approved by the NRC DAAs. These approved implementations can be found on the Computer Security Office (CSO) website.

Prior to connection to the NRC network, the general laptop must be current in critical updates.

4.6 Laptop Acquisition and Inventory

Acquisition requests for all laptops must meet one of the current laptop acquisition specifications, available at: http://www.internal.nrc.gov/ois/it-infrastructure/pdf/LaptopSpecifications.pdf. These specifications provide laptop make, models, operating systems, required software, approved software, and configuration settings that are currently approved for NRC operation. There are different specifications for different capabilities to meet NRC business needs. The specifications are updated over time to ensure NRC acquisitions are in line with the NRC enterprise architecture.

Laptop inventory information shall be entered into the NRC system inventory within 30 days of receipt of the laptop system certification memo from the system owner.

The NRC system inventory shall include property tag information for all laptops and removable hard drives to enable a cross reference with the property tracking system.

4.7 Laptop Security Oversight

Although each system owner is responsible for ensuring laptop systems are in compliance with this policy, the CSO is responsible for providing oversight of laptop security.

CSO shall perform a random sampling of all laptops quarterly, ensuring that a particular laptop is only selected once per fiscal year. Each selected laptop shall be examined to verify compliance with this policy and identify all areas of non-compliance. Areas of non-compliance shall be incorporated into the Plan of Action and Milestones for the system to which the laptop belongs.

Anytime a laptop is potentially compromised, lost, or outside the control of NRC personnel, the NRC computer security incident response policy must be followed.

5 ROLES AND RESPONSIBILITIES

Roles and responsibilities are outlined as follows:

5.1 Chief Information Officer

The Chief Information Officer is responsible for the following:

(1) Ensures development of acquisition strategies and architectures to minimize costs, services and systems, achieve economies of scale, and promote interoperability and security

(2) Ensures legacy systems timely compliance with this policy

5.2 Chief Information Security Officer

The Chief Information Security Officer, CSO, is responsible for the following:

(1) Develops computer security policy, monitors compliance, and performs computer security oversight of all NRC laptop activities

(2) Ensures laptop inventory information is provided to OIS

(3) Ensures secure configurations are provided for laptops

5.3 Director, Office of Information Services

The Director, OIS, is responsible for the following:

(1) Ensures laptop inventory information, including the property tag, is incorporated into NRC's system inventory within 30 days of receipt of the laptop system certification memo from the system owner

(2) Ensures specification of an NRC enterprise architecture accessible via the NRC Intranet that includes sufficient information to direct laptop acquisition

(3) Ensures laptop acquisition specifications are available via the NRC Intranet

5.4 Designated Approving Authority

Each DAA is responsible for the following:

(1) Ensures systems are compliant with this policy

(2) Understands risks before granting exceptions to this policy

5.5 System Owner

Each system owner is responsible for the following:

(1) Ensures office or regional guidance complies with this policy

(2) Ensures laptops belonging to their systems comply with this policy

(3) Certifies owned laptop systems

(4) Verifies classified laptop user need-to-know and required security clearance before granting laptop access

(5) Verifies SGI laptop user need-to-know and required background investigation before granting laptop access

(6) Authorizes user access to each laptop and removes authorization when appropriate

(7) Maintains a list of authorized users, including updates upon user reassignment or termination, for each classified and SGI laptop and reviews the list on a monthly basis to ensure a continued need-to-know

5.6 Information System Security Officer

Each Information System Security Officer (ISSO) is responsible for the following:

(1) Completes the information system security officer computer security awareness course every three years

(2) Completes a required computer security training class every year according to the following schedule:

- ISSO role responsibilities training every three years
- Operating system computer security training in the area of responsibility every three years
- Application computer security training in the area of responsibility every three years

(3) Monitors compliance with the security requirements specified in each contract or agreement for externally hosted applications that have been established via NRC contracts or other agreements

(4) Controls system configuration

(5) Procures any necessary hardware and software for the system

(6) Serves as the point of contact with staff or contractors that perform updates or modifications to the system

(7) At least monthly, evaluates the frequency of critical updates, taking into account the nature of the critical updates issued by the operating system and software vendors, the risk to the system, and the operational experience with and knowledge of the system

(8) Performs system auditing

5.7 System Administrator

Each system administrator is responsible for the following:

(1) Ensures compliance with required configuration settings

(2) Applies critical updates

(3) Assigns each valid user a unique account and username

(4) Removes user accounts when they are no longer required

5.8 User

Each user must follow the to be issued NRC agency wide rules of behavior as well as any system specific rules of behavior established by the laptop system owner.

6 CONTACT

If you have any questions on this policy, contact the Senior IT Security Officer for Policy, Standards, and Training.

7 REFERENCES

Nuclear Regulatory Commission

- Yellow Announcements
  - YA-08-0021, “Policy Revision: Policy Prohibiting the Use of Peer-to-Peer Software, and Its Impact on Processing Sensitive Unclassified Non-Safeguards Information on NRC Information Technology Systems, Mobile Devices, and Home Computers”
  - YA-08-0093, “Information Technology Implementation Policy – Updated Computer Security Incident Response and Personally Identifiable Information Incident Response”

- Computer Security Incident Response Policy, May 18, 2008
  http://www.internal.nrc.gov/CSO/documents/Incident_Response_Policy.doc

Office of Management and Budget (OMB)

- Appendix III to OMB Circular A-130
- Memoranda, including:
  - M-08-22, "Guidance on the Federal Desktop Core Configuration (FDCC)"
    http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf
  - M-07-18 "Ensuring New Acquisitions Include Common Security Configurations"
    http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf
  - M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems"
    http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf

U.S. Department of Commerce

- NIST, FIPS (copies of FIPS publications available at the NIST Web site at http://csrc.nist.gov), including
  - FIPS 140-2, Security Requirements for Cryptographic Modules, May 25, 2001, with December 3, 2002, change notices
- NIST Special Publications, including but not limited to:
  - SP 800-46, Security for Telecommuting and Broadband Communications, August 2002
  - SP 800-88, Guidelines for Media Sanitization, Revision 1, September 2006
  - SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
  - SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access, November 2007

U.S. Department of Defense

- Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," June 5, 1999
- Director of Central Intelligence Directive 6/9, "Manual for Physical Security Standards for SCI Facilities," November 18, 2002
- National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, February 28, 2006