Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-1004**
Office Instruction Title:	**Laptop Enterprise Security Architecture Standard**
Version Number:	**2.0**
Effective Date:	**July 1, 2021**
Primary Contacts:	**Jon Feibus**
Responsible Organization:	**OCIO/CSO**
Description:	CSO-STD-1004, “Laptop Enterprise Security Architecture Standard,” provides the minimal security requirements that must be applied to NRC laptops.
Training:	As requested.

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	5/21/2021
CISO (Acting)	Bill Dabbs	/RA/	5/21/2021

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-1004

Laptop Enterprise Security Architecture Standard

---

1 PURPOSE

CSO-STD-1004, "Laptop Enterprise Security Architecture Standard," provides the minimum security requirements for NRC laptops processing Nuclear Regulatory Commission (NRC) information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) (or Controlled Unclassified Information [CUI]) levels.

This standard is intended to be used by system administrators and system Information System Security Officers (ISSOs) responsible for applying the requirements within this standard.

This standard applies to the following NRC laptops, under the terms and conditions identified in the NRC Service Catalog[1]:

- NRC Mobile Desktops (standard government furnished equipment [GFE] laptops issued to NRC users)
- NRC Loaner Mobile Desktops – Domestic (also commonly referred to as Domestic Loaner Laptops)
- NRC Loaner Mobile Desktops – International (also commonly referred to as International Loaner Laptops)

This standard *does **not*** address:

- NRC laptops used to process Safeguards Information (SGI) or classified information.
- The following special use NRC laptop types:
  - Standalone vulnerability scanning laptops – These laptops are used to conduct system vulnerability assessments and audit a system's configuration for security compliance.
  - Standalone training laptops for attack, exploitation, and defense – These are laptops built for training involving computer attacks, vulnerability exploitation, forensic examination, reverse engineering, and network defense. Typically, this refers to training conducted by external organizations outside of NRC. These laptops are not permitted to process or store any sensitive information.
  - Forensics – These laptops are used to gather and analyze legal evidence found in computers and electronic media.

---

[1] *NRC Service Catalog > Loaner Devices and Mobile Solutions*: https://drupal.nrc.gov/ocio/catalog/247

CSO-STD-1004 is an Enterprise Security Architecture (ESA) standard. ESA standards are not written to define requirements in accordance with the current state of technology in industry or technology that is in use at the NRC. ESA standards are written to provide objective, product-agnostic requirements that are flexible and will remain current for several years following their issuance despite changes in technology. ESA standards that cover security topics, such as laptop security, do not provide requirements that are tailored to products or platforms used predominantly by NRC at a certain point in time (e.g., certain laptop models or laptops from a specific vendor). Instead, ESA standards provide requirements that are flexible to accommodate both the current and future states of security technologies and products while providing the agency discretion on the selection, use, and configuration of security products.

2 GENERAL REQUIREMENTS

This section addresses the general requirements that all system administrators and ISSOs must comply with as the minimum set of requirements.

All covered NRC laptops owned, managed, and/or operated by the NRC or by other parties on behalf of the NRC, and are used for NRC sensitive information, must comply with this standard.

All covered NRC laptops must meet all federally mandated and NRC-defined security requirements.

2.1 Authorized Laptop Users and Rules of Behavior

NRC system owners and ISSOs are expected to make sure that policies, procedures, and processes are in place to ensure that:

- Only authorized NRC users (staff, contractors) are issued NRC laptops, and
- Authorized users sign and comply with the "NRC Agency-wide Rules of Behavior for Authorized Computer Use."[2]

All users are provided with non-privileged accounts for use with the laptops and privileged administrators accounts are only provided in accordance with requirements outline in CSO-STD-2006, "User Access Management Standard."

2.2 NRC-Approved Laptop Hardware and Software

The *NRC IT Product Standards (TRM)*[3] identifies the technologies and commercial products that are authorized for use on NRC systems, including laptop hardware, software, and peripherals.

---

[2] *NRC Agency-wide Rules of Behavior for Authorized Computer Use*
https://adamsxt.nrc.gov/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId=%7bA5B82BE6-4C33-4BDB-9896-E2448BFCC38A%7d&ForceBrowserDownloadMgrPrompt=false
NRC Agency-wide Rules of Behavior for Authorized Computer User Acknowledgement Statement
https://adamsxt.nrc.gov/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId=%7b96852D5D-33C8-4ABE-B510-9F0CCB9939E8%7d&ForceBrowserDownloadMgrPrompt=false

[3] *NRC IT Product Standards TRM*
https://usnrc.sharepoint.com/teams/NRC-Information-Technology-Standards/Lists/NRC%20IT%20Product%20Standards/NRC%20IT%20Standards%20Public%20View.aspx

2.2.1 NRC Laptops

In reference to the Technical Reference Model (TRM), the following requirements apply to NRC laptops:

- All covered NRC laptops must meet the minimum hardware requirements for the most recent NRC authorized version of an approved operating system.
- All hardware and software (e.g., operating system, browser, office productivity suites) used with NRC laptops must be identified in the TRM as authorized. All authorization conditions stated in the TRM must be applied.
- When initially provisioned, NRC laptops must use the most recent NRC authorized version of approved software in all instances.

This applies to software included in the laptop images and software requested for use that is not part of the standard image (e.g., software needed for an office, region, or specific team[s]/individuals). Software requested for use that is not included within the TRM must go through the OCIO intake process.[4]

Please note that additional software that is not found in the image should be able to operate using the existing configuration without changes. This is not intended to cover the use of new software that will be incorporated into the image. All such changes to the laptop image need to go through the Configuration Control Board (CCB) approval process.[5]

2.2.2 Peripherals

The TRM lists in addition to laptops, laptop peripherals that are considered appropriate for use at NRC.

Laptop peripherals that use wireless, Bluetooth, Near Field Communications (NFC) or Radio Frequency (RF) connectivity (e.g., keyboards, mice, other human interface devices) must be identified in the TRM as being permitted for use. The approval status for human interface devices (i.e., keyboards, mice, trackballs) does not depend on whether the device is owned by NRC.

NRC laptops must be configured to prevent automatic pairing/connectivity with any non-NRC/unauthorized devices (e.g., connectivity with non-NRC smartphone when it is placed on the NFC sensor of the laptop).

NRC laptops must be configured to prevent connectivity with non-NRC electronic media (e.g., Universal Serial Bus [USB] thumb drives, external hard drives, smartphones, tablets, printers) to the extent that is technically feasible.

NRC laptops must not permit direct connectivity via USB, Peripheral Component Interconnect Express (PCI-E), or Bluetooth with non-NRC cellular hotspots/aircards.

---

[4] *NRC Service Catalog > Hardware, Software and Custom Solutions (Intake)*: https://drupal.nrc.gov/ocio/catalog/55704
[5] *NRC Service Catalog > NRC Configuration Control Board:* https://drupal.nrc.gov/ocio/catalog/31577

NRC laptops are permitted to use non-NRC cellular hotspots in accordance with the requirements specified in CSO-STD-2105, "NRC User Remote Access and International Travel Security Standard," (e.g., connecting to the hotspot using Wi-Fi).

Laptops must be configured so that High-Definition Multimedia Interface (HDMI) ports are configured as output only (e.g., to prohibit use of Ethernet over HDMI). At the time of publication of this standard, the Office of the Chief Information Officer (OCIO) inquired and received information from Dell (NRC laptop vendor) that HDMI ports on NRC laptops are configured as output only. This configuration permits NRC personnel to connect NRC laptops to TVs over HDMI. For example, NRC personnel may connect their NRC laptop to a TV at home to provide a second or larger screen using the HDMI connection. Please contact the NRC Customer Service Center (CSC) if there are any issues with NRC laptops.

2.3 Endpoint Protections

All endpoint protection software must be installed, current, and operating as intended on all covered NRC laptops in accordance with CSO-STD-2108, "Endpoint Protection Security Standard," and the applicable external standard for the product (e.g., Defense Information Systems Agency [DISA] Secure Technical Implementation Guide [STIG], Center for Internet Security [CIS] Benchmark).

NRC laptops must be in compliance with the electronic media handling requirements specified in CSO-STD-2004, "Electronic Media and Device Handling Standard," (e.g., sanitization, decommissioning).

2.4 Security Updates

NRC laptops should have all security updates applied to them when provided to a user. This includes all applicable software and firmware updates that are required to be installed for the laptop in accordance with CSO-STD-0020, "Organization-Defined Values for System Security and Privacy Controls," (e.g., SI-2, Flaw Remediation).

For example, if there is a security patch to address a Critical vulnerability, and it is made available for a longer duration than what is specified in SI-2 (i.e., 30 days for Critical vulnerabilities at the time of the publication of this standard), then that patch should be applied before the laptop is provided to the user.

2.5 Firmware Security

For NRC laptops, the Unified Extensible Firmware Interface (UEFI) must have the following minimum security measures:

- Update the latest UEFI with a secure local update mechanism;
- Use UEFI authentication to protect access to the configuration utility;
- Change the default manufacturer UEFI authenticator(s);

- Configure UEFI settings to only boot from the authorized, trust operating system on the internal storage device (e.g., the hard drive or a solid-state drive). All other drives (e.g., CD/DVD, USB drives, secure digital [SD] card) must be disabled from the boot order. During the system boot process, users must not be able to select and boot from any device other than the internal storage device; and
- Enable UEFI Secure Boot. Secure Boot requires hardware drivers and operating systems loaders to have valid vendor digital signatures in order to be loaded by the firmware.

2.6 Full-Disk Encryption and Cryptographic Protections

In accordance with CSO-STD-2004, full-disk encryption (FDE) must be implemented on all covered NRC laptops processing SUNSI (or CUI). Both hardware and software FDE are acceptable contingent upon compliance with all applicable requirements specified in CSO-STD-2009, “Cryptographic Control Standard,” for the level of sensitive information stored, processed, or transmitted.

All cryptographic modules used in NRC laptops must be:

- Validated in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication (PUB) 140, “Security Requirements for Cryptographic Modules,” as amended;
- Operated in FIPS mode; and
- Used with moderate or high key strength(s) as required in the CSO-STD-2009.

2.7 Ad Hoc Wireless

NRC laptops are prohibited from establishing or connecting to ad hoc wireless networks. Ad hoc wireless networks do not rely on access points and permit network nodes to freely associate with other ad hoc network devices within range (e.g., a wireless printer that communicates with a laptop using an ad hoc wireless network between the two devices).

2.8 Network Bridging

Due to security risks, all covered NRC laptops processing SUNSI (or CUI) are prohibited from establishing multiple network connections that bridge networks.

The exception to this requirement is NRC laptops that do not process SUNSI (or CUI) and are used for training and development. These types of NRC laptops may require special configuration settings.

2.9 Return and Inspection of NRC Laptops

NRC laptops returned by the user (or on behalf of a user) must be sanitized in accordance with the security measures specified in CSO-STD-0020 and CSO-STD-2004.

NRC laptops assigned for temporary work assignments (e.g., training, domestic travel) must be returned within five business days after completing official NRC business.

NRC Loaner Mobile Desktops – International must be returned on the first business day after returning to the office from official international travel.[6] After the laptop is returned, it must be forensically analyzed.

2.10 Devices Supporting RF Communications

RF security requirements vary depending on the type of device:

- NRC laptops must not use RF devices that allow data transfers (i.e., sending a file from an NRC laptop to another device).
- RF devices (e.g., keyboards) may only be used for data entry, including for sensitive information (i.e., username and passwords), if the RF device encrypts data in transit.
- NRC laptops are **permitted** to use RF devices that cannot be used for data transfers or entering sensitive information. Examples of these devices include:
  - Mice
  - Remote presentation clickers
  - Other pointing devices (e.g., trackballs, trackpads)
- NRC Loaner Mobile Desktop – International should not use RF communication devices, if possible, due to the potential of greater risk associated with international travel.

2.11 Detection of Use in Unauthorized Areas

NRC laptops must be configured to detect and alert/report to the OCIO Security Operations if a laptop is being used in an unauthorized area. For example, the international use of an NRC Mobile Desktop or NRC Loaner Mobile Desktop – Domestic is not permissible in accordance with CSO-STD-2105 and must be reported to OCIO Security Operations. Whereas, NRC Loaner Mobile Desktops – International are specifically configured for such purpose and used while on international business travel.

3 SPECIFIC REQUIREMENTS

Specific requirements must be applied to NRC laptops to protect the agency and reduce risks associated with the use of NRC laptops. These specific requirements are based on the laptop type and network type (e.g., NRC managed networks, networks managed on behalf of the NRC, and external networks).

3.1 Local Network Connectivity

Specific NRC networks are associated with NRC network types and a network trust level. Refer to CSO-STD-4000, “Network Infrastructure Enterprise Security Architecture Standard,” for specific requirements pertaining to network types and their baseline network trust levels (trusted, semi-trusted, and untrusted), which are a factor in determining the networks to which NRC laptops are permitted to connect. To the extent possible, NRC laptops must be configured to comply with connectivity restrictions associated with trust levels specified for network types in CSO-STD-4000.

[6] International Travel>Travel Checklist>Loaner Devices: https://itravel.nro.nrc.gov/SitePages/Home.aspx

NRC laptops used for training (in an ad hoc manner) may be authorized to connect to trusted, semi-trusted, and restricted networks in accordance with CSO-STD-4000, as needed, for specific training classes/courses.

Non-NRC endpoints that attempt to connect to trusted NRC managed networks (specified in CSO-STD-4000) must have communications restricted. For example, a non-NRC laptop that connects to a trusted NRC managed network (e.g., enterprise wired network at an NRC facility) would only be permitted to access the NRC guest network.

3.2 Remote Access

NRC laptops must be configured to support all applicable requirements specified within CSO-STD-2105.

The NRC Service Catalog must provide the latest applicable security requirements for use of non-NRC endpoints (e.g., laptops, desktops, tablets, smartphones) by end users (directly or by reference) to remotely access NRC systems. This includes the requirements specified in the user's approved *NRC Telework Program Participation Agreement (Form 624)*[7] and requirements specified in CSO-STD-2105.

3.3 Bluetooth Connectivity

NRC laptops may use Bluetooth devices subject to the requirements in the following subsections regarding security configuration and permissible use cases.

The OCIO must make available guidance/documentation regarding NRC user responsibilities for use of Bluetooth devices, which must inform NRC users of any requirements that cannot be technically enforced (e.g., via the laptop configuration).

To the extent that it is technically feasible, NRC laptops must not permit Bluetooth pairing or communication with Bluetooth devices from vendors that are blocklisted (i.e., prohibited) from use with federal agencies and systems (e.g., per identification in the Department of Commerce "Entity List," via the Federal Acquisition Supply Chain Security Act of 2018 [FASCA]).

NRC Loaner Mobile Desktop – International should use connected devices instead of Bluetooth devices, if possible, to avoid security risks during international travel.

3.3.1 Security Configuration

Bluetooth connectivity on NRC laptops should be disabled when Bluetooth is not in use.

Bluetooth must operate in "hidden" (not discoverable) mode except when pairing a new Bluetooth device.

[7] *NRC Telework Program Participation Agreement (Form 624)*
https://usnrc.sharepoint.com/teams/NRC-Forms-Library/NRC%20Forms%20Library/NRC%20624.pdf

Additional requirements are identified in applicable external standards:

1. NRC laptops and Bluetooth devices must continue to comply with all Bluetooth security configuration requirements found within applicable external standards (e.g., the DISA Windows 10 STIG for Windows 10 operating systems).
2. Applicable external standards are identified within the CSO SharePoint Standards site for Security Configuration Baselines.8
3. Further information regarding how the external standards apply is provided in the CSO-PROS-3000, "Cybersecurity Standards Process."

3.3.2 Permissible Use Cases and Caveats

Bluetooth devices can be used with NRC laptops to support specified use cases. The use cases are identified below and include caveats (conditions) that must be met:

- Human interface devices: Mice, keyboards, trackballs, and pointers/clickers (e.g., for presentations)
  - **Caveats:** Keyboards must use FIPS encryption to protect sensitive information (e.g., SUNSI, CUI) that may be entered using the device. For example, Microsoft Bluetooth keyboards manufactured in the last ten years, typically support the Advanced Encryption Standard (AES) encryption algorithm to encrypt data in transit.
- Audio devices: Headsets, headphones/earbuds, and speakers
  - **Caveats:** If audio devices are anticipated to be used to transit sensitive information (e.g., via Microsoft Teams, Cisco WebEx conferencing), then:
    - NRC laptops must be configured to support the use of FIPS validated encryption to protect the sensitive data in transit over the Bluetooth connection; and
    - Bluetooth GFE audio devices must also support and perform FIPS encryption of data in transit.
- Bluetooth tethering: Sharing a GFE mobile device's internet connection with an NRC laptop
  - **Caveats:** Device and connection configurations must follow the applicable requirements within CSO-STD-2105.

[8] CSO SharePoint Standards Site - https://usnrc.sharepoint.com/:f:/r/teams/OCIO-CSO/CSO_FISMA_Repository/Cybersecurity_Issuances/01_STANDARDS?csf=1&web=1&e=HXQMDR

APPENDIX A. ACRONYMS

AES	Advanced Encryption Standard
AO	Authorizing Official
CCB	Configuration Control Board
CD	Compact Disk
CIS	Center for Internet Security
CSC	Customer Service Center
CSO	Computer Security Organization
CUI	Controlled Unclassified Information
DISA	Defense Information Systems Agency
DVD	Digital Video Disk
ESA	Enterprise Security Architecture
FASCA	Federal Acquisition Supply Chain Security Act of 2018
FDE	Full-Disk Encryption
FIPS	Federal Information Processing Standard
GFE	Government Furnished Equipment
ISSO	Information System Security Officer
HDMI	High-Definition Multimedia Interface
IT	Information Technology
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
PCI-E	Peripheral Component Interconnect Express
PUB	Publication
RF	Radio Frequency
SD	Secure Digital
SGI	Safeguards Information
STD	Standard
STIG	Secure Technical Implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
TRM	Technical Reference Model
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

APPENDIX B. GLOSSARY

Bluetooth	Open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices.
Cellular Devices	Cellular devices such as USB Aircard, express card, and cellular phones that provide internet access to mobile computers such as laptops.
Controlled Unclassified Information	Requires safeguarding or dissemination controls in accordance with applicable law, regulations, and government-wide policies but is not classified.
Endpoint	A communication interface of a device that is attached to a network, and is capable of sending, receiving, or forwarding information over a network.
Full-disk Encryption	Technology which protects information at rest by converting the information into unreadable code that cannot be deciphered easily by unauthorized people. Full-disk encryption is the process of encrypting every bit of data input to an internal storage drive or volume.
Guest Network	An organization's broadband network services offered to their visitors. Other government agencies (e.g., state, federal, and local agencies), telework centers, and commercial businesses often provide visitors with broadband services to access the internet. Guest networks are not entirely dedicated to the public but are provided for the organizations' visitors as a convenience to access the internet.
Hotspots	A location that offers wireless broadband network services to visitors using Wi-Fi technology. Hotspots are often located in places such as airports, train stations, libraries, marinas, conventions centers, restaurants, and hotels.
Laptop	A mobile desktop computer that is portable and suitable for use while travelling and has similar capabilities as a desktop computer.
Laptop User	NRC personnel, including full-time and part-time NRC employees and contractors, who are authorized to access NRC systems and resources via a laptop.
NRC Loaner Mobile Desktops - Domestic	Laptops provided to users by the OCIO for internal and external presentations, when traveling domestically on agency business, or for other agency-related purposes.
NRC Loaner Mobile Desktops - International	Laptops provided to users by OCIO for use during international travel on agency business.

NRC Mobile Desktops	Laptops provided to users by the OCIO, allowing users to remotely connect to the NRC infrastructure to access NRC resources and process information up to, and including, the SUNSI (or CUI) level.
Network Bridging	Where two or more network adapters (e.g., Ethernet ports, wireless cards, cellular devices) are configured to allow two or more communication networks to connect. Bridging may allow an intruder to gain access from one communication session to the other and introduce malicious traffic into the network.
Network Trust Level	The concept of trusted, semi-trusted, and untrusted networks; and the security requirements associated with each type of network.
NRC Infrastructure	NRC networks that are authorized by the Authorizing Official (AO); where the network segment or connection is considered trusted or semi-trusted (as specified in the system's authorization) and may process information up to, and including, the SUNSI (or CUI) level.
Peripheral Device	A computer component that is not part of the core computer. Examples of peripheral devices include mice, keyboards, printers, monitors, external storage drives (e.g., USB drives, CD/DVD, and Blu-Ray drives), scanners, facsimile equipment, speakers, microphones, and cameras.
Peripheral Component Interconnect Express	A high-speed serial computer expansion bus standard, used as common motherboard interface for connections to computer graphic cards, modems, hard drives, etc.
Restricted Network	Any network that is not a trusted network or semi-trusted network. This includes all networks originating from a foreign country and publicly accessible networks (e.g., public hotspots) or networks otherwise accessible to members of the public through commercial businesses (e.g., hotel networks).
Safeguard Information	A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected.
Semi-trusted Network	Networks where security controls have been applied; limiting risks of system compromise and breaches.
Sensitive Unclassified Non-Safeguards Information	Information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source).
Trusted Network	A network that employs sufficient hardware and software assurance measures to allow its use for processing SUNSI (or CUI). For the purposes of this standard, NRC managed networks are the only trusted networks.

Untrusted Network	A category of restricted networks. Network where security controls are limited or have not been applied; increasing risks of system compromise and breaches. Use of untrusted networks puts NRC laptops, information, and users at risk of possible compromise or breach due to an assumed lack of verified, effective network security controls.

CSO-STD-1004 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
04-Dec-08	1.0	Initial Release	CSO web page	
11-Feb-09	1.1	Reconciled clarity issues	CSO web page	
17-Jul-09	1.2	Updated wireless and anti-malware software information	CSO web page	
27-Jul-09	1.3	Removed references to specific wireless cards, clarified use of Symantec installation CD, and clarified SecureDoc password synchronization.	CSO web page	Mandatory training provided to all NRC ISSOs.
24-Aug-09	1.4	Convert to standard format and added requirement for Adobe Flash to ensure iLearn training courses can be completed	CSO web page	
01-Oct-09	1.4	Removed sensitivity markings	CSO web page and ISSO forum	
02-Nov-09	1.5	Modified to include home wireless router use	CSO web page and ISSO forum	
16-Nov-09	1.6	Modified to reference the strong password standard	CSO web page and ISSO forum	
06-Apr-11	1.7	Modified to allow user configuration of wireless access	CSO web page and ISSO forum	
20-May-21	2.0	Updated with the latest requirements	Post to OCIO/CSO website	N/A