Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-2105**
Office Instruction Title:	**Remote Access Security Standard**
Revision Number:	**1.0**
Effective Date:	**June 1, 2015**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PCT**
Summary of Changes:	CSO-STD-2105, "Remote Access Security Standard," provides security requirements for remote access to NRC systems processing information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) level.
Training:	As requested
ADAMS Accession No.:	ML13319A198

Approvals				
Primary Office Owner	Policies, Compliance, and Training		**Signature**	**Date**
Enterprise Security Architecture Working Group Chair and Responsible SITSO	Kathy Lyons-Burke		**/RA/**	**11/18/14**
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	**/RA/**	**11/18/14**
	Director, OIS	Jim Flanagan	**/RA/**	**12/11/14**

TABLE OF CONTENTS

List of Figures

List of Tables

Computer Security Standard
CSO-STD-2105

Remote Access Security Standard

1 PURPOSE

The purpose of CSO-STD-2105, “Remote Access Security Standard,” is to provide security requirements for remote access to the Nuclear Regulatory Commission (NRC) systems processing information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) level.

This standard is intended for:

- System administrators and Information System Security Officers (ISSOs) who have the required knowledge, skill, and ability to apply and enforce the security requirements.
- NRC users, specifically regarding requirements on whether remote access is permitted for certain device types (e.g., mobile desktops).

This standard does ***not*** apply to:

- Remote access for direct access applications that do not require electronic authentication (e.g., the public web-based, Agencywide Documents Access and Management System [ADAMS], public websites).

This standard is being issued in an iterative fashion to enable implementers to begin using the standard earlier than would be possible if issuance depended upon a full and complete standard. Each iteration until the issuance of the complete standard is considered a partial standard. Partial standards include defined requirements for a subset of the information to be included in the full and complete standard. Partial standards are not subject to the limit of one change to the standard per year specified in CSO-PROS-3000, “Process for Development, Establishment, and Maintenance of NRC Security Standards.”

CSO-STD-2105 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 network infrastructure or endpoint production, do not provide requirements that are tailored to products or platforms used predominantly by NRC at a certain point in time (e.g., the most commonly used firewall device when a standard is under development or published). 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 INTRODUCTION

The security requirements specified in this standard relate to the secure design, implementation, and use of remote access methods. The requirements are derived from the following high-level concepts and terminology associated with NRC remote access.

Remote access is the use of an NRC system by an authenticated and authorized user or device communicating over the Internet. When the connection does not traverse the Internet, the access is referred to as network access.

Remote access requires user-based and device-based identification and authentication to ensure access is only permitted to authorized users and devices. Remote access allows:

- Authorized users to access their virtual desktop located on the NRC infrastructure network
- Authorized users to access NRC business/applications networks
- Authorized users to access other NRC resources, such as the NRC intranet and shared files
- Authorized devices to extend an NRC network segment from one location (e.g., NRC office) to another (e.g., contractor network), such as that used to provide the NRC infrastructure user access to Financial Accounting and Integrated Management Information System (FAIMIS).

2.1 Suggested Prioritization for Rolling Out Remote Access Changes

This section provides a suggested prioritization for rolling out remote access changes in order for systems to be in compliance with this standard. System owners and ISSOs should focus on complying with the requirements in this standard based on:

1. Remote access employed with the greatest potential risk first, then
2. Continue on towards compliance with remote access that poses progressively lower levels of potential risk.

For example, one of the areas of greatest potential risk would be remote access for system administrators. Working towards compliance with the requirements in this standard (e.g., to enable use of multi-factor authentication when required) could substantially reduce the risk posed (compared with remote access that only uses single-factor authentication). Afterwards, the focus could then transition to compliance for remote access associated with applications and user groups where the potential risk for that remote access is lower (compared to remote access for system administrators).

2.2 Remote Access Methods

NRC has three remote access methods to access NRC resources processing information up to, and including, the SUNSI level:

1. Tunneling

2. Portals
3. Direct Application Access

This section describes each remote access method. The remote access methods reference user authentication and encryption, which are addressed in detail in:

- Section 2.4, User Identification and Authentication, which provides foundational information on user authentication.
- Section 4.2, Required Minimum E-Authentication Assurance Levels, which provides user authentication requirements.
- Sections 3.4, Cryptography, which provides requirements for the use of encryption.

2.2.1 Tunneling

Tunneling occurs when data is encapsulated within another transmission protocol while traversing through internal or external networks. Merely encapsulating data within another transmission protocol without encryption is not sufficient to protect the information from unauthorized access. For example, the Teredo Internet Protocol version 6 (IPv6) transition technology that provides IPv6 connectivity on Internet Protocol version 4 (IPv4) networks does not encrypt the transmitted data and thus does not possess the qualities necessary to be an example of the NRC authorized tunneling remote access method.

Tunneling with encryption occurs when data is both encapsulated within another transmission protocol and protected using encryption while traversing through internal or external networks. When this standard refers to tunneling, the reference is to tunneling with encryption. During transmission, the information is protected from a network perspective because the nodes within the networks interpret the private protocols used in the transmission as data and are not able to view the cleartext version of the transmitted encrypted data (e.g., encrypted SUNSI).

Tunneling with encryption is used to establish and maintain secure, logical connections between separate networks, systems, or sites (i.e., business locations) with communications occurring over the network. The tunneled connection is established between two networked devices. These devices can be NRC general laptops, desktops, servers, or other network devices (e.g., virtual private network (VPN) gateways). Tunneling protects communications between separate systems, networks, or between resources in the same system in different geographic locations.

In the most common example of tunneling used to facilitate telework, authorized NRC users initiate and establish a remote session using a software program (e.g., VPN client software) on their computer (e.g., a mobile desktop) and authenticate to a VPN gateway device. For an NRC user with a mobile desktop, this provides access to NRC resources, as if locally connected at an NRC office, while encrypting the transmission so that the information cannot be obtained.

In another common example of tunneling to connect system resources and different systems, multiple VPN gateway devices are used to connect different systems (e.g., between multiple NRC systems in different geographic locations, between NRC and external systems) with communication occurring over internal and external networks. This may include networks managed on behalf of NRC, which may have an established secured tunnel to NRC managed networks.

2.2.2 Portals

Portals provide secure entry from an external network into NRC managed networks. They are typically web-based and enable authenticated and authorized NRC users to connect to NRC resources. Furthermore, portals encrypt all data in transit between the remote access user and the portal server(s). An example includes portal access to users' desktops or business applications through a centralized interface as used in virtual desktop infrastructures (VDI). Portals take advantage of terminal server and remote desktop technologies. A common example of remote access portal used at the NRC is Citrix®[1]. Citrix provides web-based remote desktop connections and enables access to NRC resources.

2.2.3 Direct Application Access

Direct application access applies to applications that require users to identify and authenticate to NRC systems and resources from external networks for accessing information up to, and including, the SUNSI level. Direct application access encrypts all data in transit between the remote access user and the direct application access server(s). The most common example of direct application access may be public facing web-based or client-server applications.

A common example of direct application access is the Electronic Information Exchange (EIE) system. This direct application access is web-based and provides authorized and authenticated users access to transmit electronic submittals securely from external networks.

2.3 Remote Access Examples

This section provides examples of remote access that traverse the Internet to and from NRC defined network types. These examples are not inclusive; however, the objective for these examples is to provide an understanding of how remote access applies to the NRC (both at the current time and in the future). The terminology used in this section is associated with CSO-STD-4000, "Network Infrastructure Standard" and CSO-STD-1004, "Laptop Security Standard."

Table 2.3-1 identifies NRC network types and provides examples of remote access to and from NRC network types.

Table 2.3-1: NRC Network Type and Remote Access Examples

Network Type		**Remote Access Examples**
NRC Wide Area Network (WAN)	*Infrastructure Networks*	• NRC mobile desktop users establish a VPN tunnel from public access networks to access NRC infrastructure networks. The VPN tunnel traverses the Internet from public access networks. • NRC desktop users on NRC infrastructure networks establish direct application access to systems hosted on vendor networks. The direct application access traverses the Internet from NRC infrastructure networks to vendor networks.

[1] Citrix® is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries."

Network Type		Remote Access Examples
	Business/Application Networks	• NRC applications in business/application networks establish a VPN tunnel to an external system, such as one hosted by a different federal agency or commercial organization, for data transfers. The VPN tunnel traverses the Internet to perform data transfers from NRC business/application networks to the external systems.
NRC Extended Networks	*Extended Licensee Networks*	• Extended licensee networks establish a VPN tunnel to access NRC infrastructure networks. The VPN tunnel traverses the Internet from licensee networks to access resources on the NRC infrastructure network.
NRC Special Purpose Networks	*Guest Networks*	• General laptop user directly accesses an application from a guest network to access an NRC web application hosted outside of NRC by a different federal agency. The direct application access traverses the Internet from the guest network to access the NRC web application hosted by a different federal agency.
	Demilitarized Zones (DMZs)	• NRC devices establish VPN tunnels from NRC DMZ to other federal agency or commercial organization DMZs. The VPN tunnel traverses the Internet from one DMZ segment to another DMZ segment.
Contractor/Government Hosted Networks Specifically for NRC		• NRC infrastructure networks establish a VPN tunnel to contractor networks to extend a portion of the NRC infrastructure network. The VPN tunnel traverses the Internet from NRC infrastructure networks to the contractor network. The extension of the network can allow NRC users to access hosted services on contractor networks. The VPN tunnel is transparent to NRC users.
Contractor/Vendor/ Government Hosted Cloud Service		• NRC desktop users on NRC infrastructure networks directly access an application provided by vendor cloud services. The direct application access traverses the Internet from NRC infrastructure networks to vendor cloud services.
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	• NRC users establish access to NRC infrastructure networks or business/application networks using an NRC issued mobile device (e.g., Aircards) with a VPN tunnel, Citrix portal, or direct application access to a web application. Remote access using these three methods traverses the Internet from service provider networks to NRC infrastructure networks or business/application networks.
	Vendor Networks Providing Maintenance Services	• Vendors establish access to NRC infrastructure networks to perform maintenance of NRC systems using a VPN tunnel, Citrix portal, or direct application access to a web application. Remote access using these three methods traverses the Internet from vendor networks to access NRC infrastructure networks or business/application networks for maintenance.

Network Type		**Remote Access Examples**
Other Government Networks		- Users from other government agencies directly access an NRC web application. The direct application access traverses the Internet from other government networks to NRC resources.
Telework Networks	*NRC Compliant Home Networks*	- NRC users teleworking from home establish access to NRC infrastructure networks or business/application networks using a VPN tunnel, Citrix portal, or direct application access to a web application. Remote access using these three methods traverses the Internet from NRC compliant home networks to NRC infrastructure networks or business/application networks.
	Public Access Networks	- NRC users on travel establish access to NRC infrastructure networks or business/application networks using a VPN tunnel, Citrix portal, or direct application access to a web application. Remote access using these three methods traverses the Internet from public access networks to NRC infrastructure networks or business/application networks.
	State Government Telework Centers	- NRC users establish a VPN tunnel from state telework centers to access NRC infrastructure networks. The VPN tunnel traverses the Internet from state telework centers to NRC infrastructure networks.
	Other Organizations' Guest Networks	- NRC users establish a VPN tunnel from other organizations' guest networks to access NRC infrastructure networks or business/application networks. The VPN tunnel traverses the Internet from other organizations' guest networks to NRC infrastructure networks or business/application networks.
Licensee and Licensee Contractor Networks		- Users from licensees directly access an NRC web application. The direct application access traverses the Internet from licensee networks to NRC resources (e.g., web applications requiring user identification and authentication).
Academia Networks		- Users from academia directly access an NRC web application, to access NRC resources. The direct application access traverses the Internet from academia networks to NRC resources (e.g., web applications requiring user identification and authentication).
Industry Networks		- Users from industry directly access an NRC web application. The direct application access traverses the Internet from academia networks to NRC resources (e.g., web applications requiring user identification and authentication).

2.4 User Identification and Authentication

Remote access for users requires electronic authentication (i.e., e-authentication). E-authentication is the process of establishing confidence in user identities electronically presented to a system.

Depending on the sensitivity of information being accessed, remote access methods may require identity proofing.

2.4.1 Identity Proofing and User Identification

Identity proofing is the process by which the credential issuer (e.g., system owner, ISSO) validates sufficient information that uniquely identifies a person applying for the credential (e.g., the identifier). The credential issuer provides the applicant with an identifier after validating the identification credentials to ensure that the individual is the person for whom access is authorized. For example, the credential issuer may request to see two forms of government issued identification that includes photographs of the individual. The identifier is then matched to the authentication information so the NRC system can authenticate the user and distinguish authorized users from all other users.

2.4.2 User Authentication

User authentication is the process of verifying user identity and applies to remote access by users to NRC systems and resources. E-authentication assurance levels are differentiated by the number, type, and strength of authentication factors used. Authentication factors are:

- Something you know (e.g., password, personal identification number [PIN]);
- Something you have (e.g., cryptographic security token, smart card); and
- Something you are (e.g., voice print, fingerprint, or other biometric information).

Multi-factor authentication occurs when two or more different types of authentication factors are considered. For example, when a user presents his or her user identifier to a system, the system validates the user identifier after receiving authentication information from the user, such as a password (i.e., something you know) and a cryptographic security token (i.e., something you have).

2.4.3 E-Authentication Assurance Levels

E-authentication assurance levels apply to remote access based on information sensitivity. The following sections provide high-level descriptions of the e-authentication assurance levels.[2]

2.4.3.1 Assurance Level One

Assurance level one is the lowest level. This assurance level:

[2] For more information on the authentication assurance levels, refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, “Electronic Authentication Guideline,” as amended.

- Allows single-factor remote network authentication
- Issues electronic credentials for access without requiring remote user identity proofing
- Allows authentication with a simple password challenge-response protocol
- Permits use of any token methods of e-authentication assurance levels 2, 3, or 4

2.4.3.2 Assurance Level Two

Assurance level two provides a moderate degree of confidence in a user's identity. This assurance level:

- Requires identity proofing
- Allows single-factor remote network authentication (as in e-authentication assurance level 1)
- Permits use of any token methods of e-authentication assurance levels 3 or 4

2.4.3.3 Assurance Level Three

Assurance level three provides a high degree of confidence in a user's identity. This assurance level:

- Requires identity proofing
- Requires multi-factor remote network authentication
- Permits use of software cryptographic tokens
- Permits use of any token methods of e-authentication assurance level 4

2.4.3.4 Assurance Level Four

Assurance level four provides the highest degree of confidence in a user's identify. This assurance level:

- Requires identity proofing
- Requires multi-factor remote network authentication
- Permits only hardware cryptographic tokens, rather than software cryptographic tokens

2.5 Device Identification and Authentication

Similar to remote access for users, remote access for devices requires some form of identification and authentication. Device identification and authentication ensures that only permitted NRC systems and devices (e.g., desktops, laptops, servers, VPN gateways) are allowed to establish a connection to an NRC system.

Uniquely identifying and authenticating devices before establishing remote access to NRC systems is accomplished by:

- Blacklisting – The practice of identifying devices that are denied access to NRC systems.
- Whitelisting – A list or register of devices that are authorized to access NRC systems.

Device certificates (i.e., public key infrastructure (PKI) certificates) and enforcement of network access controls are used to implement blacklisting and whitelisting.

2.6 Secure Object Reuse

Secure object reuse is the assurance that a storage medium (e.g., memory, disk, tape, cartridge/cassette, and Compact Disk Read-Only Memory [CD-ROM]) storing sensitive data or information has been cleared of the information and that no residual data remains before it is reassigned for other use. For example, a user may unintentionally see data associated with another user's currently active, previously established, or previously terminated session if secure object reuse requirements are not implemented.

3 GENERAL REQUIREMENTS

This section addresses the general requirements that all system administrators and ISSOs authorized to administer and configure remote access solutions must comply with as the minimum set of controls.

All devices that are owned, managed, leased, and/or operated by the NRC or by parties on behalf of the NRC, that are used for remote access must comply with all federally mandated and NRC-defined security requirements.

This standard must be used in concert with:

- CSO-STD-4000, "Network Infrastructure Standard." This standard provides guidance in following security requirements for the NRC network infrastructure.
- CSO-STD-1004, "Laptop Security Standard." This standard provides users with guidance in following security requirements for laptops.
- Other Computer Security Office (CSO) standards.

3.1 NRC-Approved Hardware and Software

The following requirement must be applied regarding NRC-approved hardware and software:

RA-NHS-G1 All hardware and software used for remote access must be listed in the NRC Technical Reference Model (TRM) as authorized for use at the NRC for the intended purpose.

3.2 Use of Approved Remote Access Methods

The following requirement must be applied regarding the use of approved remote access methods:

RA-UARAM-G1 NRC systems providing remote access must use one of the approved remote access methods specified in Section 2.1, Suggested Prioritization for Rolling Out Remote Access Changes

This section provides a suggested prioritization for rolling out remote access changes in order for systems to be in compliance with this standard. System owners and ISSOs should focus on complying with the requirements in this standard based on:

4. Remote access employed with the greatest potential risk first, then
5. Continue on towards compliance with remote access that poses progressively lower levels of potential risk.

For example, one of the areas of greatest potential risk would be remote access for system administrators. Working towards compliance with the requirements in this standard (e.g., to enable use of multi-factor authentication when required) could substantially reduce the risk posed (compared with remote access that only uses single-factor authentication). Afterwards, the focus could then transition to compliance for remote access associated with applications and user groups where the potential risk for that remote access is lower (compared to remote access for system administrators).

Remote Access Methods.

3.3 Data in Transit

The following requirement must be applied regarding data in transit:

RA-DIT-G1 All remote access sessions must encrypt data in transit.

3.4 Cryptography

All cryptography used must comply with CSO-STD-2009, “Cryptographic Control Standard.”

3.5 Network Ports, Protocols, and Services

All network ports, protocols, and services used by remote access methods must comply with CSO-STD-2008, “Network Protocol Standard.”

3.6 Identification and Authentication

System owners must comply with applicable CSO standards, such as CSO-STD-2006, “User Access Management,” CSO-STD-0001, “NRC Strong Password Standard,” and CSO-STD-0020, “Organization Defined Values for System Security Controls,” for all identification and authentication control requirements. This applies to user and device identification and authentication.

3.7 System Auditing

Auditing parameters for software applications must be configured and audit information must be reviewed as defined in the applicable CSO standards.

3.8 Secure Object Reuse

The following requirement must be applied regarding secure object reuse:

RA-SOR-G1 To prevent data from being disclosed to unauthorized users, remote sessions must be configured to not be able to connect to other user sessions regardless of the remote access method used. For example, users using portal access to connect to NRC managed networks must not be able to view or access another user’s data (e.g., residual data within applications used by different users in different sessions) from other portal sessions.

4 SPECIFIC REQUIREMENTS

This section provides specific security requirements for remote access. These security requirements address:

- E-authentication assurance levels based on NRC information sensitivity and remote access method;
- Permitted remote access methods for different device types (e.g., NRC desktop, general laptop, Bring Your Own Devices [BYODs]);
- Device identification and authentication; and
- Object preservation for reuse.

4.1 Remote Access Information Sensitivity

The following requirement must be applied regarding remote access information sensitivity:

RA-RAIS-S1 The remote access information types and each type’s associated information sensitivity shall be identified through the review of the system’s approved security categorization document.

- If the system is broken up into multiple subsystem components and remote access only provides the user access to information within a subsystem component, then the information types and associated information sensitivities may be identified through review of the subsystem component’s approved security categorization document.
- If the approved security artifacts for the system or subsystem component do not explicitly identify the information types associated with the specific remote access implemented, the highest information sensitivity for the associated system or subsystem component must be used as the remote access information sensitivity.

The following simplified example of direct application access that is used to provide remote access to a web application provides an overview of how the information types made available by remote access, the associated information sensitivities, and the remote access information sensitivity can be identified and determined. In this example, the information types, impact levels for security objectives (e.g., confidentiality, integrity, availability) for each information type, and Information sensitivity for each information type are documented within the associated system's approved security categorization.

Please note that the potential impact levels and information sensitivity for each information type in the example are solely for clarifying this section and should not be construed as direction or guidance.

- Remote Access Method: Direct Application Access
- Remote Access Description: An externally accessible NRC web application that provides access to various legal investigation, research, and general purpose data to authenticated and authorized human users.
- Information Types[3]:
  - Legal Investigation
  - Scientific and Technological Research and Innovation
  - General Purpose Data and Statistics
- Information Sensitivity: Table 4.1-1 provides the following:
  - Information types
  - Potential impact levels for the security objectives for each information type
  - Information sensitivity for each information type, which is the highest impact level listed for all security objectives for the information type
  - Remote access information sensitivity, which is the highest information sensitivity for all information types

Table 4.1-1: Information Sensitivities Example

Information Type	Potential Impact Levels			Information Sensitivity
	Confidentiality	Integrity	Availability	
Legal Investigation	Moderate	Moderate	Moderate	Moderate
Scientific and Technological Research and Innovation	Low	Moderate	Low	Moderate
General Purpose Data and Statistics	Low	Low	Low	Low
Remote Access Information Sensitivity				Moderate

The remote access example provides users with access to three information types. The three information types either have an information sensitivity of low or moderate. The highest information sensitivity is moderate. The remote access information sensitivity for the remote access example is moderate.

[3] FIPS 199 and NIST SP 800-60, "Guide for Mapping Types of Information and Systems to Security Categories" provide assistance with information types.

4.2 Required Minimum E-Authentication Assurance Levels

Required minimum e-authentication assurance levels for remote access are specified in this section and apply to all remote access that provides access to human users. The requirements in this section do not apply to remote access that only provides access between network devices (e.g., two VPN gateways that establish a tunnel between two separate organizations).

Remote access to NRC systems and resources provides access to one or more information types. Each of these information types has an associated information sensitivity (i.e., Low, Moderate, or High). The information sensitivity is determined by the potential impact of compromise of the information confidentiality, integrity, and availability in accordance with the Federal Information Security Management Act of 2002 (FISMA) and Federal Information Processing Standards (FIPS) 199, “Standards for Security Categorization of Federal Information and Systems.” For further detail on information types and sensitivities, please refer to section 4.1, Required Minimum E-Authentication Assurance Levels, which also provides an example.

The required minimum e-authentication assurance level for remote access is determined using the formula in Figure 4.2-1:

Figure 4.2-1: Determininig Required Minimum e-Authentication Assurance Levels

Remote Access Information Sensitivity*	**+**	**Remote Access Method Used**	**=**	**Required Minimum e-Authentication Assurance Level****

*Highest information sensitivity of all the information type that the user can access through the remote access method.
**E-authentication assurance levels are described in Section 2.4.3, E-Authentication Assurance Levels.

RA-RMEAL-S1 The following base requirements must be used together to determine the required minimum e-authentication assurance level:

- Remote Access Information Sensitivity Requirements:

  Low
  – E-authentication assurance level permitted to be as low as *level 1*.
  – The associated remote access method can increase the e-authentication assurance level requirement.

  Moderate or High
  – E-authentication assurance level must be at *level 3 or above*.
  – The increased information sensitivity necessitates the increased assurance provided by e-authentication assurance level 3, which is the lowest level that requires multi-factor authentication.

- Remote Access Method Requirements:

  Direct Application Access
  – E-authentication assurance level permitted to be as low as *level 1*.
  – The associated information sensitivity can increase the e-authentication assurance level requirement.

Tunneling and Portal	– E-authentication assurance level must be at *level 3 or above*. – These remote access methods provide a point of entry to NRC managed networks and networks managed on behalf of NRC (e.g., through creating and allowing use of tunnels, providing access to VDI). This requires a more robust assurance level.

Table 4.2-1 provides the required minimum e-authentication assurance levels based on the remote access information sensitivity and the specific remote access method.

Table 4.2-1: Required Minimum E-Authentication Assurance Levels for the Specific Remote Access Method

Remote Access Information Sensitivity	Remote Access Method		
	Tunneling	Portal	Direct Application Access
High	Level 3	Level 3	Level 3
Moderate	Level 3	Level 3	Level 3
Low	Level 3	Level 3	Level 1

Using the remote access example described in Section 4.1, Remote Access Information Sensitivity, the required minimum e-authentication assurance level that applies is level 3. The remote access method of direct application access permits an assurance level as low as level 1; however, the remote access information sensitivity of moderate requires that the assurance level be increased to level 3.

4.3 Permitted Remote Access Methods for Specific Device Types by Originating Network Type

This section identifies the permitted remote access methods for NRC general laptops, desktops, BYODs, and NRC mobile devices depending upon where remote access originates from (e.g., NRC infrastructure networks, NRC compliant home networks), which is also referred to as the originating network type. This section is for the use of NRC users, in addition to the main audience for the standard of system administrators and ISSOs.

System administrators and ISSOs should be aware that the requirements in this section must be used in tandem with the requirements in Section 4.4, Remote Access Restrictions by Destination Device Type. Section 4.4 provides further requirements that indicate whether an NRC device or BYOD is permitted to establish a remote access connection to another device type. These requirements must be taken together with the requirements in this section to determine whether remote access is permitted.

This section provides explanatory information for why the remote access method is permitted, not permitted, or not applicable based on the network types the connection is originating from and the specific device type initiating the remote access request, which is referred to as the originating device type. For example, mobile desktops connecting from NRC compliant home networks to access NRC systems and resources on NRC infrastructure networks can connect remotely using the permitted remote access methods (e.g., tunneling, portal, direct application access). In some cases, all three remote access methods are permitted and in other cases, one or two remote access methods are permitted.

The following defines the information contained within the table columns of each table presented in the following sections:

- Originating Device Type: The specific name of the type of device initiating the remote access request.
- Network Type (Remote Access Originating From): The type of network where the remote access originates from. In other words, this is the network where the device is locally connected (e.g., a local connection to an NRC compliant home network). Network types are defined in CSO-STD-4000.
- Remote Access Method: Identifies the authorized remote access method (e.g., tunnel, portal, direct application access) permitted for use when the remote access originates from the network type.
  - Permitted: The device is permitted to use the remote access method (e.g., tunneling, portal, direct application access) when connecting from the network type.
  - Not Permitted: The device is not permitted to use the remote access method (e.g., tunnel, portal, direct application access) when connecting from the network type.
  - Not Applicable: A determination of permitted or not permitted does not apply. The device is not permitted to locally connect to the network type (remote access originating from) specified. For example, an NRC desktop is not permitted to locally connect to an NRC compliant home network. Thus, all remote access methods are not applicable for the NRC desktop when the network type is an NRC compliant home network.

4.3.1 NRC Desktops

NRC desktops are permanent workstations assigned to NRC users working from NRC facilities or Resident Inspector Site Expansion (RISE) sites. NRC desktops do not include mobile desktops. Since NRC desktops are not mobile, all remote access methods are not applicable from the following networks:

- NRC Extended Networks
- Contractor, Vendor, and Service Provider Networks
- Other Government Networks
- Telework Networks
- Licensee and Licensee Contractor Networks
- Home Networks

NRC desktops are directly connected to NRC infrastructure networks or RISE networks. Thus, tunneling and portal remote access methods are not applicable.

<u>RA-NRCD-S1</u> From NRC infrastructure networks or RISE networks, the direct application access method is permitted. NRC users may connect from NRC infrastructure networks to NRC systems hosted outside of the NRC WAN. NRC desktops are not permitted to use any other remote access methods.

A common example of the direct application access method is the NRC iLearn®[4] system. This system is hosted by a vendor outside of the NRC WAN, and NRC users remotely access iLearn over the Internet. Thus, an NRC user could use an NRC desktop to remotely access the iLearn web application, which is an example of the direct application access method.

Table 4.3-1 summarizes the permitted remote access methods for NRC desktops.

Table 4.3-1: Permitted Remote Access Methods to NRC Desktops

NRC DESKTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Permitted
	RISE Networks	Not Applicable	Not Applicable	Permitted
NRC Extended Networks	*Guest Networks*	Not Applicable	Not Applicable	Not Applicable
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	Not Applicable	Not Applicable	Not Applicable
	Other Contractor, Vendor, and Service Provider Networks	Not Applicable	Not Applicable	Not Applicable
Other Government Networks		Not Applicable	Not Applicable	Not Applicable
Telework Networks	*NRC Compliant Home Networks*	Not Applicable	Not Applicable	Not Applicable
	Public Access Networks			
	Transit Hotspots	Not Applicable	Not Applicable	Not Applicable
	Lodging Hotspots	Not Applicable	Not Applicable	Not Applicable
	State Government Telework Centers	Not Applicable	Not Applicable	Not Applicable
	Other Organizations' Guest Networks	Not Applicable	Not Applicable	Not Applicable
Licensee and Licensee Contractor Networks		Not Applicable	Not Applicable	Not Applicable

[4] iLearn® is a registered trademark of iLearn, Inc. for its informational services.

4.3.2 General Laptops

This section identifies the permitted remote access methods for the following general laptop categories:

- Mobile Desktops
- Loaner Laptops
- Office Managed Laptops
- Training Laptops

4.3.2.1 Mobile Desktops

Unlike NRC desktops, mobile desktops ***are*** permitted to directly connect to different network types; however, this does not always permit the use of all three remote access methods. The network types that a mobile desktop is permitted to directly connect to are specified in CSO-STD-1004.

RA-GL-S1 When mobile desktops are locally connected to NRC infrastructure networks and RISE networks, tunneling and portal remote access methods ***are not*** applicable. From NRC infrastructure networks or RISE networks, the direct application access method ***is*** permitted. NRC users may connect from NRC infrastructure networks to NRC systems hosted outside of the NRC WAN. As in examples for NRC desktops, an NRC user could use the direct application access method to connect to iLearn when using a mobile desktop while connected to an NRC infrastructure network (e.g., while at an NRC facility).

RA-GL-S2 When the remote access originates from any of the networks listed below, tunneling ***is*** the only permitted remote access method. These networks are either unsecured or the enforcement of the security controls cannot be validated by the NRC. Tunneling provides a higher level of security by routing the user's network traffic through NRC infrastructure networks.

- Guest Networks
- Transit Hotspots
- Lodging Hotspots
- State Government Telework Centers
- Other Organizations' Guest Networks

RA-GL-S3 When the connection originates from any of the networks listed below, all three remote access methods ***are*** permitted. NRC has limited oversight or assurance for these networks through mutual understanding that home networks are secured in accordance with CSO standards, agreements between the NRC and Internet service providers, or interconnection security agreements (ISAs) between the NRC and other government agencies in accordance with CSO-STD-4000.

- NRC Compliant Home Networks
- Contractor, Vendor, and Service Provider Networks

- Other Government Networks

Per CSO-STD-4000, mobile telecommunications carrier (e.g., Verizon, AT&T) networks are an example of Contractor, Vendor, and Service Provider Networks and agreement state networks are an example of an Other Government Network.

RA-GL-S4 During a declared state of emergency or emergency training exercises, NRC mobile desktops ***are*** permitted to connect to the networks listed below using all three remote access methods in accordance with the requirements specified in CSO-STD-1004.

- Licensee and Licensee Contractor Networks

Table 4.3-2 summarizes the permitted remote access methods for mobile desktops.

Table 4.3-2: Permitted Remote Access Methods for Mobile Desktops

MOBILE DESKTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Permitted
	RISE Networks	Not Applicable	Not Applicable	Permitted
NRC Extended Networks	*Guest Networks*	Permitted	Not Permitted	Not Permitted
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	Permitted	Permitted	Permitted
	Other Contractor, Vendor, and Service Provider Networks	Permitted	Permitted	Permitted
Other Government Networks		Permitted	Permitted	Permitted
Telework Networks	*NRC Compliant Home Networks*	Permitted	Permitted	Permitted
	Public Access Networks			
	Transit Hotspots	Permitted	Not Permitted	Not Permitted
	Lodging Hotspots	Permitted	Not Permitted	Not Permitted
	State Government Telework Centers	Permitted	Not Permitted	Not Permitted
	Other Organizations' Guest Networks	Permitted	Not Permitted	Not Permitted
Licensee and Licensee Contractor Networks		Permitted*	Permitted*	Permitted*

* Remote access associated with declared states of emergency or emergency training exercises, when permitted, must be performed in accordance with the requirements specified in CSO-STD-1004.

4.3.2.2 Loaner Laptops

This section identifies the permitted remote access methods for the following NRC loaner laptops:

- Internal Loaner Laptops
- External (Domestic) Loaner Laptops
- International Loaner Laptops

4.3.2.2.1 Internal Loaner Laptops

The following requirement must be applied regarding internal loaner laptops:

RA-GL-S5 Internal loaner laptops have the same requirements as mobile desktops, which are specified in Section 4.3.2.1, Mobile Desktops.

4.3.2.2.2 External (Domestic) Loaner Laptops

External (domestic) loaner laptops ***are*** permitted to directly connect to different network types; however, this does not permit the use of all three remote access methods.

RA-GL-S6 External (domestic) loaner laptops ***are not*** permitted to directly connect to NRC infrastructure networks or RISE networks; therefore, use of remote access methods from NRC infrastructure networks or RISE networks are not applicable.

RA-GL-S7 When the remote access originates from any of the networks listed below, tunneling is not permitted since external (domestic) loaner laptops ***are not*** permitted to establish tunneled connections with NRC managed networks or networks managed on behalf of NRC. In this instance, portal and direct application access methods ***are*** permitted.

- Guest Networks
- Transit Hotspots
- Lodging Hotspots
- State Government Telework Centers
- Other Organizations' Guest Networks

RA-GL-S8 When the connection originates from any of the networks listed below, portal and direct application access methods ***are*** permitted. NRC has limited oversight or assurance for these networks through mutual understanding that home networks are secured in accordance with CSO standards, agreements between the NRC and Internet service providers, or ISAs between the NRC and other government agencies in accordance with CSO-STD-4000.

- NRC Compliant Home Networks
- Contractor, Vendor, and Service Provider Networks
- Other Government Networks

RA-GL-S9 During a declared state of emergency or emergency training exercises, external (domestic) loaner laptops ***are*** permitted to connect to the networks listed below using the portal and direct application access methods in accordance with the requirements specified in CSO-STD-1004.

- Licensee and Licensee Contractor Networks

Table 4.3-3 summarizes the permitted remote access methods for domestic loaner desktops.

Table 4.3-3: Permitted Remote Access Methods for External (Domestic) Loaner Laptops

EXTERNAL (DOMESTIC) LOANER LAPTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Not Applicable
	RISE Networks	Not Applicable	Not Applicable	Not Applicable
NRC Extended Networks	*Guest Networks*	Not Applicable	Permitted	Permitted
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	Not Applicable	Permitted	Permitted
	Other Contractor, Vendor, and Service Provider Networks	Not Applicable	Permitted	Permitted
Other Government Networks		Not Applicable	Permitted	Permitted
Telework Networks	*NRC Compliant Home Networks*	Not Applicable	Permitted	Permitted
	Public Access Networks			
	Transit Hotspots	Not Applicable	Permitted	Permitted
	Lodging Hotspots	Not Applicable	Permitted	Permitted
	State Government Telework Centers	Not Applicable	Permitted	Permitted
	Other Organizations' Guest Networks	Not Applicable	Permitted	Permitted
Licensee and Licensee Contractor Networks		Not Applicable	Permitted*	Permitted*

* Remote access associated with declared states of emergency or emergency training exercises, when permitted, must be performed in accordance with the requirements specified in CSO-STD-1004.

4.3.2.2.3 International Loaner Laptops

International loaner laptops ***are*** permitted to directly connect to different network types; however, this does not permit the use of all three remote access methods.

RA-GL-S10 International loaner laptops ***are not*** permitted to directly connect to NRC infrastructure networks or RISE networks; therefore, the remote access methods from NRC infrastructure networks or RISE networks are not applicable.

RA-GL-S11 When the remote access originates from any of the networks listed below, tunneling is not applicable since international loaner laptops ***are not*** permitted to establish tunneled connections with NRC managed networks or networks managed on behalf of NRC. In this instance, portal and direct application access methods ***are*** permitted.

- NRC Guest Networks
- Transit Hotspots, including International Transit Hotspots
- Lodging Hotspots, including International Lodging Hotspots
- State Government Telework Centers (within the United States)
- Other Organizations' Guest Networks

RA-GL-S12 When the connection originates from any of the networks listed below, portal and direct application access methods ***are*** permitted. NRC has limited oversight or assurance for these networks through mutual understanding that home networks are secured in accordance with CSO standards, agreements between the NRC and Internet service providers, or ISAs between the NRC and other government agencies in accordance with CSO-STD-4000.

- NRC Compliant Home Networks
- Contractor, Vendor, and Service Provider Networks
- Other Government Networks (within the United States)

RA-GL-S13 During a declared state of emergency or emergency training exercises, international loaner laptops ***are*** permitted to connect to the networks listed below using the portal and direct application access methods in accordance with the requirements specified in CSO-STD-1004.

- Licensee and Licensee Contractor Networks

Table 4.3-4 summarizes the permitted remote access methods for international loaner desktops.

Table 4.3-4: Permitted Remote Access Methods for International Loaner Laptops

INTERNATIONAL LAPTOPS				
Network Type **(Remote Access Originating From)**		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Not Applicable
	RISE Networks	Not Applicable	Not Applicable	Not Applicable
NRC Extended Networks	*Guest Networks*	Not Applicable	Permitted	Permitted
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	Not Applicable	Permitted	Permitted
	Other Contractor, Vendor, and Service Provider Networks	Not Applicable	Permitted	Permitted
Other Government Networks (within the United States)		Not Applicable	Permitted	Permitted
Telework Networks	*NRC Compliant Home Networks*	Not Applicable	Permitted	Permitted

INTERNATIONAL LAPTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
	Public Access Networks			
	Transit Hotspots; including International	Not Applicable	Permitted	Permitted
	Lodging Hotspots; including International	Not Applicable	Permitted	Permitted
	Government Telework Centers (within the United States)	Not Applicable	Permitted	Permitted
	Other Organizations' Guest Networks (within the United States)	Not Applicable	Permitted	Permitted
Licensee and Licensee Contractor Networks		Not Applicable	Permitted*	Permitted*

* Remote access associated with declared states of emergency or emergency training exercises, when permitted, must be performed in accordance with the requirements specified in CSO-STD-1004.

4.3.2.3 Office Managed Laptops

This section identifies the permitted remote access methods for the following office managed laptops:

- Telecommuting Laptops
- Research Laptops
- Development Laptops

4.3.2.3.1 Telecommuting Laptops

The following requirement must be applied regarding telecommuting laptops:

RA-GL-S14 Telecommuting laptops have the same requirements as external (domestic) loaner laptops, which are specified in Section 4.3.2.2.2, External (Domestic) Loaner Laptops.

4.3.2.3.2 Research Laptops

Research laptops ***are*** permitted to directly connect to different network types; however, this does not permit the use of all three remote access methods.

RA-GL-S15 Research laptops ***are not*** permitted to directly connect to NRC infrastructure networks or RISE networks; therefore, the use of remote access methods from NRC infrastructure networks or RISE networks are not applicable.

RA-GL-S16 When the remote access originates from any of the networks listed below, tunneling is not applicable since research laptops ***are not*** permitted to establish tunneled connections with NRC managed networks or networks managed on behalf of NRC. In this instance, portal and direct application access methods ***are*** permitted.

- Guest Networks
- Transit Hotspots
- Lodging Hotspots
- State Government Telework Centers
- Other Organizations' Guest Networks

RA-GL-S17 When the connection originates from any of the networks listed below, portal and direct application access methods ***are*** permitted. NRC has limited oversight or assurance for these networks through mutual understanding that home networks are secured in accordance with CSO standards, agreements between the NRC and Internet service providers, or ISAs between the NRC and other government agencies in accordance with CSO-STD-4000.

- NRC Compliant Home Networks
- Contractor, Vendor, and Service Provider Networks
- Other Government Networks

RA-GL-S18 During a declared state of emergency or emergency training exercises, research laptops ***are*** permitted to connect to the networks listed below using the portal and direct application access methods in accordance with the requirements specified in CSO-STD-1004.

- Licensee and Licensee Contractor Networks

Table 4.3-5 summarizes the permitted remote access methods for research laptops.

Table 4.3-5: Permitted Remote Access Methods for Research Laptops

RESEARCH LAPTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Not Applicable
	RISE Networks	Not Applicable	Not Applicable	Not Applicable
NRC Extended Networks	*Guest Networks*	Not Applicable	Permitted	Permitted
Contractor, Vendor, and	*Phone/Data Carriers*	Not Applicable	Permitted	Permitted

RESEARCH LAPTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
Service Provider Networks	*Other Contractor, Vendor, and Service Provider Networks*	Not Applicable	Permitted	Permitted
Other Government Networks		Not Applicable	Permitted	Permitted
Telework Networks	*NRC Compliant Home Networks*	Not Applicable	Permitted	Permitted
	Public Access Networks			
	Transit Hotspots	Not Applicable	Permitted	Permitted
	Lodging Hotspots	Not Applicable	Permitted	Permitted
	State Government Telework Centers	Not Applicable	Permitted	Permitted
	Other Organizations' Guest Networks	Not Applicable	Permitted	Permitted
Licensee and Licensee Contractor Networks		Not Applicable	Permitted*	Permitted*

* Remote access associated with declared states of emergency or emergency training exercises, when permitted, must be performed in accordance with the requirements specified in CSO-STD-1004.

4.3.2.3.3 Development Laptops

Development laptops ***are*** permitted to directly connect to different network types; however, this does not permit the use of all three remote access methods.

RA-GL-S19 Development laptops **are not** permitted to directly connect to NRC infrastructure networks or RISE networks; therefore, the use of remote access methods from NRC infrastructure networks or RISE networks are not applicable. In addition, since development laptops are not used for telecommuting or travel, remote access from the following networks is not applicable:

- Transit Hotspots
- Lodging Hotspots
- State Government Telework Centers
- Other Organizations' Guest Networks
- Other Government Networks
- Licensee and Licensee Contractor Networks

RA-GL-S20 When the connection originates from any of the networks listed below, direct application access method ***is*** permitted. Development laptops are used for the purpose of development; therefore, the use of portal remote access method is not applicable. The NRC guest network is for NRC guests and visitors and not available to the public. Since NRC guest networks are located within NRC facilities, development laptops ***are*** permitted to connect. NRC has some security oversight for the other network types listed through mutual understanding that home networks are secured in accordance with CSO standards and agreements between the NRC and Internet service providers in accordance with CSO-STD-4000.

- NRC Guest Networks
- NRC Compliant Home Networks
- Contractor, Vendor, and Service Provider Networks

RA-GL-S21 Security configuration requirements for development laptops are more permissive than most other general laptops (e.g., allowing in some cases for network bridging). Development laptops ***are not*** permitted to directly connect to licensee or licensee contractor networks; therefore, remote access from licensee and licensee contractor networks is not applicable.

Table 4.3-6 summarizes the permitted remote access methods for development laptops.

Table 4.3-6: Permitted Remote Access Methods for Development Laptops

DEVELOPMENT LAPTOPS				
Network Type (Remote Access Originating From)		**Remote Access Method**		
		Tunneling	**Portal**	**Direct Application Access**
NRC WAN	*Infrastructure Networks*	Not Applicable	Not Applicable	Not Applicable
	RISE Networks	Not Applicable	Not Applicable	Not Applicable
NRC Extended Networks	*Guest Networks*	Not Applicable	Not Applicable	Permitted
Contractor, Vendor, and Service Provider Networks	*Phone/Data Carriers*	Not Applicable	Not Applicable	Permitted
	Other Contractor, Vendor, and Service Provider Networks	Not Applicable	Not Applicable	Not Applicable
Other Government Networks		Not Applicable	Not Applicable	Not Applicable
Telework Networks	*NRC Compliant Home Networks*	Not Applicable	Not Applicable	Permitted
	Public Access Networks			
	Transit Hotspots	Not Applicable	Not Applicable	Not Applicable
	Lodging Hotspots	Not Applicable	Not Applicable	Not Applicable
	State Government Telework Centers	Not Applicable	Not Applicable	Not Applicable

DEVELOPMENT LAPTOPS				
Network Type (Remote Access Originating From)		Remote Access Method		
		Tunneling	Portal	Direct Application Access
	Other Organizations' Guest Networks	Not Applicable	Not Applicable	Not Applicable
Licensee and Licensee Contractor Networks		Not Applicable	Not Applicable	Not Applicable

4.3.2.4 Training Laptops

Training laptops have multiple connection restrictions as defined in CSO-STD-1004. This section provides remote access requirements for each type of training laptop.

4.3.2.4.1 Isolated Training

The following requirement must be applied regarding isolated training laptops:

RA-GL-S22 Isolated training laptops are only permitted to directly connect to isolated training environments; and therefore, isolated training laptops ***are not*** permitted to use remote access to connect to any network.

4.3.2.4.2 SUNSI Training

The following requirement must be applied regarding SUNSI training laptops:

RA-GL-S23 Since SUNSI training laptops are used for internal training, these laptops have the same requirements as NRC desktops, which are specified in Section 4.3.1, NRC Desktops.

4.3.2.4.3 International Training

The following requirement must be applied regarding international training laptops:

RA-GL-S24 International training laptops ***are*** only permitted to directly connect to isolated training environments overseas; therefore, international training laptops ***are not*** permitted to connect to any NRC network.

4.3.3 NRC Mobile Devices

NRC mobile devices will be addressed in a future issuance of this document.

4.3.4 BYODs

BYODs will be addressed in a future issuance of this document.

4.4 Remote Access Restrictions by Destination Device Type

This section provides remote access restrictions that indicate whether an NRC device or BYOD is permitted to establish a remote access connection to another device type. These requirements are based upon the originating device type and the destination device type. The originating device type, such as a general laptop, is the type of device that is making the request to initiate a remote access connection. The destination device type, such as a network device or server, is the type of device in which the originating device type is attempting to establish a remote access connection. For example, in a scenario with an NRC mobile desktop being used to remotely access NRC webmail remotely, a mobile desktop, which is a general laptop, would be considered the originating device type and an NRC server (e.g., representing NRC servers running Microsoft Windows that provide access to NRC webmail) would be considered the destination device type.

This section addresses the device types shown in Table 4.4-1, listed and accompanied by example devices that have requirements based on whether the device type is being considered as an originating or a destination device type.

Table 4.4-1: Device Types

Device Type	Examples of Devices
NRC Desktops	Physical or virtual desktops.
General Laptops	Mobile desktops, loaner laptops, office managed laptops, and training laptops
NRC Mobile Devices	Tablets and smartphones.
BYODs	Personally owned smartphones, tablets, or laptops enrolled in an authorized NRC BYOD program.
NRC Network Devices	A physical or virtual network device. Examples include: VPN gateways, integrated services routers, unified threat monitoring devices, and other network gateways and appliances presented on NRC networks.
NRC Servers	Physical or virtual server with a role of web application server or portal server.

Requirements will be provided for all of the above device types considering each device type from the perspective of an originating and destination device type. For each unique combination of originating and destination device type, all remote access methods, some remote access methods, or no remote access methods may be permitted. The following defines the information contained within the table columns of each table presented in the following sections, which are organized by destination device type:

- Device Type: The specific name of the originating device type.
- Remote Access Method: Identifies the authorized remote access method (e.g., tunnel, portal, direct application access) permitted to provide remote access to the specified originating device type.
  - Permitted: The destination device type is permitted to use the remote access method (e.g., tunneling, portal, direct application access) to provide remote access to the specified originating device type.

  - Not Permitted: The destination device type is not permitted to use the remote access method (e.g., tunnel, portal, direct application access) to provide remote access to the specified originating device type.

- Conditions: Identifies any conditions that apply to the destination device type when using a remote access method to provide remote access to the specified originating device type.

These requirements must be taken together with the requirements in Section 4.3, Permitted Remote Access Methods for Specific Device Types by Originating Network Type, to determine whether remote access is permitted based on both the originating network and device type (requirements provided in Section 4.3) and the originating and destination device type (requirements provided in this section).

4.4.1 NRC Desktop Restrictions

The following requirement must be applied regarding NRC desktop restrictions:

RA-NRCDR-S1 NRC desktops must not provide any remote access to any other NRC desktop or other device type. Thus, NRC desktops ***are not*** permitted to provide remote access using any of the three remote access methods to any originating device type. For example, an NRC server cannot, as an originating device type, initiate a remote access connection to an NRC desktop.

4.4.2 General Laptop Restrictions

The following requirement must be applied regarding general laptop restrictions:

RA-GLR-S1 General laptops must not provide any remote access to any other general laptop or other device type. Thus, general laptops ***are not*** permitted to provide remote access using any of the three remote access methods to any originating device type. For example, an NRC server cannot, as an originating device type, initiate a remote access connection to a general laptop.

4.4.3 NRC Mobile Devices

NRC mobile devices will be addressed in a future issuance of this document.

4.4.4 BYODs

BYODs will be addressed in a future issuance of this document.

4.4.5 NRC Network Devices

The following requirement must be applied regarding NRC network devices:

RA-NRCND-S1 NRC network devices located in DMZs ***are*** permitted to provide remote access. For example, a common remote access scenario for NRC users with general laptops is to establish a remote access connection using a VPN tunnel, which is provided by NRC network devices (e.g., VPN gateways).

RA-NRCND-S2 NRC network devices, such as VPN gateways, ***are*** permitted to provide remote access using the tunneling remote access method to all originating device types except for one. NRC desktops are directly connected to NRC infrastructure networks or RISE networks. Thus, tunneling and portal remote access methods are not permitted. NRC network devices must not provide remote access using tunneling to general laptops and NRC mobile devices connected to NRC infrastructure or RISE networks. This is due to the risk posed by not allowing for the inspection of data within the tunnel when a tunnel is established from an internal NRC network. NRC network devices must only provide remote access using tunneling to NRC servers and network devices located in DMZ networks.

RA-NRCND-S3 NRC network devices, such as Citrix NetScaler Gateways, ***are*** permitted to provide remote access using the portal remote access method. NRC network devices are permitted to provide remote access using the portal remote access methods to general laptops, NRC mobile devices, and BYODs.

RA-NRCND-S4 NRC network devices, such as locked down network appliances working as hardened web servers, ***are*** permitted to provide remote access using the direct application access method. NRC network devices ***are*** permitted to provide remote access using the direct application access methods to NRC desktops, general laptops, NRC mobile devices, and BYODs.

Table 4.4-2 summarizes the remote access restrictions for NRC network devices.

Table 4.4-2: Remote Access Restrictions for NRC Network Devices

NRC NETWORK DEVICES				
Originating Device Type	**Remote Access Method**			**Conditions**
	Tunneling	**Portal**	**Direct Application Access**	
NRC Desktops	Not Permitted	Not Permitted	Permitted	
General Laptops	Permitted*	Permitted	Permitted	*Tunneling:* Permitted except when connected to NRC infrastructure or RISE networks.
NRC Mobile Devices	Permitted*	Permitted	Permitted	*Tunneling:* Permitted except when connected to NRC infrastructure or RISE networks.
BYODs	Permitted	Permitted	Permitted	
NRC Servers	Permitted*	Not Permitted	Not Permitted	*Tunneling:* Permitted only when connected to DMZ networks.
NRC Network Devices	Permitted*	Not Permitted	Not Permitted	*Tunneling:* Permitted only when connected to DMZ networks.

* The remote access method is only permitted based upon the requirements specified in the conditions column.

4.4.6 NRC Servers

The following requirement must be applied regarding NRC servers:

RA-NRCS-S1 NRC network devices and other NRC servers ***are not*** permitted to connect to NRC servers providing remote access. NRC servers located in DMZs ***are*** permitted to provide remote access. For example, a common remote access scenario for NRC users with general laptops is to establish a remote access connection to NRC webmail, which is provided by NRC web application servers running Microsoft Windows.

RA-NRCS-S2 NRC servers, such as Citrix XenApp servers, ***are*** permitted to provide remote access using the portal remote access method to general laptops, NRC mobile devices, and BYODs. NRC desktops are directly connected to NRC infrastructure networks or RISE networks. Thus, the portal remote access method is not permitted.

RA-NRCS-S3 NRC servers, such as web application servers, ***are*** permitted to provide remote access using the direct application access method to NRC desktops, general laptops, NRC mobile devices, and BYODs.

Table 4.3-3 summarizes the remote access restrictions for NRC servers.

Table 4.4-3: Remote Access Restrictions for NRC Servers

NRC SERVERS			
Originating Device Type	**Remote Access Method**		
	Tunneling	**Portal**	**Direct Application Access**
NRC Desktops	Not Permitted	Not Permitted	Permitted
General Laptops	Not Permitted	Permitted	Permitted
NRC Mobile Devices	Not Permitted	Permitted	Permitted
BYODs	Not Permitted	Permitted	Permitted
NRC Servers	Not Permitted	Not Permitted	Not Permitted
NRC Network Devices	Not Permitted	Not Permitted	Not Permitted

4.5 Device Identification and Authentication

This section provides device identification and authentication requirements for remote access methods.

4.5.1 Tunneling

The following requirement must be applied regarding isolated training laptops:

RA-T-S1 Tunneling device identification and authentication must be configured to identify and authenticate devices attempting to connect and determine if the device is:

- An authorized device from an external system (e.g., for tunnels between NRC systems and systems for other organizations).
- An authorized device in the NRC system (e.g., a VPN gateway used to establish a tunnel across two separate physical sites for the system).

4.5.2 Portal

Portal device identification and authentication must meet the following requirements:

RA-P-S1 Identify and authenticate devices authorized to store SUNSI. For example, users accessing NRC resources through portal access are permitted to store or process SUNSI through transferring data and files to local drives (e.g., through drive mapping) if they are using an authorized device, such as a mobile desktop.

RA-P-S2 Identify devices not authorized to store SUNSI. The device may be authorized for access but not authorized to store SUNSI.

Portals must apply the following requirements based on the results of the device identification and authentication:

RA-P-S3 Devices authorized to store SUNSI are permitted to store and process SUNSI through transferring data and files to and from local drives (e.g., through drive mapping, other access to drives of the user's computer from within the portal session, copying and pasting data from the portal session).

RA-P-S4 Devices that are authorized to connect, but are not authorized to store SUNSI must not be permitted to transfer data and files to and from local drives.

4.5.3 Direct Application Access

Direct application access device identification and authentication must meet the following requirements:

RA-DAA-S1 Identify and authenticate devices that are authorized to store SUNSI.

RA-DAA-S2 Identify devices not authorized to store SUNSI. The device may be authorized for access but not authorized to store SUNSI.

Direct application access must apply the following requirements based on the results of the device identification and authentication:

RA-DAA-S3 Devices authorized to store SUNSI are permitted to store and process SUNSI through caching or downloading of SUNSI (e.g., downloading of email attachments).

RA-DAA-S4 Devices that are authorized to connect, but are not authorized to store and process SUNSI must not be permitted cache SUNSI or download files containing SUNSI.

4.6 Object Preservation for Reuse Settings

Object preservation for reuse settings support the resolution of the following connectivity issues:

- User accidentally disconnects from a portal session, and reconnects to establish connection to the same session.
- User accidentally closes a direct access application and reconnects to the same session to complete an application transaction (e.g., filling out a form).

RA-OPRS-S1 To preserve user data and facilitate the resumption of work when a user's session is unintentionally disconnected, disconnected sessions (including data associated with the session) are to be preserved for up to the required amount of time, based on the NRC system security categorization (e.g., low, moderate, high), identified below in

Table 4.6-1, Object Preservations for Reuse Time Limits. Object preservation for reuse settings only applies to portal and direct application remote access.

Table 4.6-1: Object Preservation for Reuse Time Limits

Security Categorization	Object Reuse Preservation Time Limit (minutes)
Low	10
Moderate	10
High	5

APPENDIX A. ACRONYMS

ADAMS	Agency-wide Documents Access and Management System
BYOD	Bring Your Own Device
CD-ROM	Compact Disk Read-Only Memory
CSO	Computer Security Office
DAA	Designating Approving Authority
DMZ	Demilitarized Zone
EIE	Electronic Information Exchange
ESA	Enterprise Security Architecture
FAIMIS	Financial Accounting and Integrated Management Information System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISA	Interconnection Security Agreement
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIS	Office of Information Services
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RISE	Resident Inspector Site Expansion
PROS	Process
SP	Special Publication
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
TRM	Technical Reference Model
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX B. GLOSSARY

Bring Your Own Device

Device (e.g., tablet, smartphone, laptop) not leased or owned by NRC, which NRC has agreed can process sensitive information as long as the user signs an agreement to incorporate specific controls on the device and follow NRC rules regarding processing such information on the device.

Demilitarized Zone

Perimeter network segment that is logically placed between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from external networks.

Direct Application Access

Applications that require users to identify and authenticate to NRC systems and resources from external networks such as the Internet for accessing information up to, and including, the SUNSI level while encrypting data in transit.

Electronic Authentication

The process of establishing confidence in user identities electronically presented to a system.

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.

External System (or Component)

A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Network

Networks that interconnect with the NRC network or are used by individuals to connect to NRC networks, systems, and applications.

General Laptop

Laptops owned, leased, and managed by the NRC and used throughout the NRC. These laptops fall into four categories: Mobile Desktops, Loaner Laptops, Training Laptops, and Office-managed Laptops.

Identification

An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

Identity Proofing

The process by which the credential issuer (e.g., system owner, ISSO) validates sufficient information that uniquely identifies a person applying for the credential (e.g., the identifier). The credential issuer provides the applicant with an identifier after validating the identification credentials to ensure that the individual is the person for whom access is authorized.

Interconnection Security Agreement

An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations.

Loaner Laptop

Laptops provided to users by the Office of Information Services (OIS) for internal and external presentations, when traveling on agency business, or for other agency-related purposes.

Mobile Desktop

Laptops provided to users by the OIS, allowing users to remotely connect to the NRC infrastructure to access NRC resources and process information up to, and including, the SUNSI level.

Multi-factor Authentication

Multi-factor authentication occurs when two or more different types of authentication factors is considered. For example, when a user presents their user identifier to a system, the system validates the user identifier after receiving additional information from the user such as a password (i.e., something you know) and a cryptographic security token (i.e., something you have) which the user provides.

Network Access Control

A feature provided by hardware, software, and rule sets that allows access based on a user's credentials and the results of health checks performed on the client device.

Network Bridging

The process of configuring two or more network adapters (e.g., Ethernet ports, wireless cards, or cellular devices) to allow two or more communication networks to connect.

Networks Managed on Behalf of NRC

Networks and systems operated by other parties (e.g., contractors) on behalf of NRC that connect to NRC managed networks for the purpose of supporting core mission operations and other internal business or enterprise services.

NRC Compliant Home Networks

Networks configured in accordance with the following standards are considered to be NRC compliant home networks.:

- CSO-STD-1801, "Home Wireless Networking Configuration Standard."
- CSO-STD-1802, "Home Wired Network Configuration Standard."

NRC Extended Networks

NRC network that is specifically stretched to accommodate a specific remote facility, where NRC controls both endpoints.

NRC Managed Networks

Networks that are managed or operated by NRC personnel at NRC facilities and include Infrastructure Support and Business/Application Networks, NRC Extended Networks, and NRC Special Purpose Networks.

NRC Special Purpose Networks

Special purpose networks exist to support either a specific information sensitivity level that requires special controls or to support a specialized function.

Office Managed Laptops

Laptops (i.e., telecommuting, development, and training) owned and managed by individual NRC offices.

One-time Password

A password that is only valid for one login session or transaction.

Partial Standard

Partial standards include defined requirements for a subset of the information to be included in the full and complete standard. Partial standards are not subject to the limit of one change to the standard per year specified in CSO-PROS-3000, “Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards.” Standards are issued in an iterative fashion to enable implementers to begin using the standard earlier than would be possible if issuance depended upon a full and complete standard. Each iteration until the issuance of the complete standard is considered a partial standard.

Portal

Secure entry from an external network, such as the Internet, into NRC managed networks. They are typically web-based and enable authorized NRC users to connect to NRC resources.

Public Key Cryptography

Encryption system that uses a public-private key pair for encryption and/or digital signature.

Remote Access

Remote access is authenticated access to a system by an authorized user or an authorized device communicating through the Internet.

Remote Access Information Sensitivity

The highest information sensitivity of all the information types that a user can access through a remote access method used in a system.

Remote Access Method

The vendor and product agnostic means of providing remote access to an NRC system.

Remote Session

An interactive exchange of data over a communication path established between a remote device and a local device.

Safeguards Information

A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected.

Secret Key

A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

Secured Container

A security mechanism for separating running programs, data, or both on a computing device. The security mechanism places the programs in a protected state on the device by creating a secured isolated environment for the protected data at rest and while programs are executed. Secured containers are commonly used to support BYOD efforts.

Secure Object Reuse

The assurance that a storage medium (e.g., memory, disk, tape, cartridge/cassette, and CD-ROM) storing sensitive data or information has been cleared of the information and that no residual data remains before it is reassigned for other use.

Security Token

Software or hardware-based cryptographic solution to authenticate a user’s identity through use of secret key, public key cryptography, or one-time password to prevent against compromise.

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, etc.).

Single-factor Authentication

The use of one authentication factor to authenticate to a system.

Smart Card

A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

Teredo

IPv6 transition technology that provides IPv6 connectivity on IPv4 networks.

Terminal Server

A server that provides users with access to an NRC desktop environment with a common connection point to NRC managed networks.

Training Laptops

Laptops provided by OIS or individual NRC offices to users for use during training events. Users may use training laptops to participate in NRC internal training courses, vendor courses, and international training events. Training laptops are typically not used for telecommuting; however, depending on unique use cases, these laptops may be used to access NRC resources (e.g., webmail) remotely while on travel.

Tunneling

Data that is encapsulated and transmitted over another network. The information is protected and nodes within the external network only recognize the private protocols used in the transmission as data.

User Authorization

Verifying the identity of a user and that the user is allowed to access NRC information types. For example, a user must be identified as an authorized NRC employee to access information up to, and including, the SUNSI level.

User Identifier

A series of numbers or letters assigned to a user from which the user is identified to various NRC resources.

Virtual Private Network

Protected system link utilizing tunneling and security controls.

CSO-STD-2105 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
17-Nov-14	1.0	Initial Issuance	Distribution at ISSO forum and posting on CSO web page	Upon request