

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

Office Instruction: **CSO-STD-2105**

Office Instruction Title: **NRC User Remote Access and International Travel Security Standard**

Version Number: **2.2**

Effective Date: **January 4, 2021**

Primary Contacts: **Jonathan Feibus**

Responsible Organization: **OCIO/CSO**

Description: CSO-STD-2105, "NRC User Remote Access and International Travel Security Standard," provides the minimum security requirements that must be met for NRC user remote access to NRC systems processing information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) or Controlled Unclassified Information (CUI) level. The standard also provides minimum security requirements for international travel.

Training: As requested

Approvals			
Primary Office Owner		Signature	Date
	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)		
SWG Chair	Bill Bauer	/ RA /	11/27/2020
CISO	Jonathan Feibus	/ RA /	11/30/2020

TABLE OF CONTENTS

1 PURPOSE **1**

2 GENERAL REQUIREMENTS..... **2**

 2.1 APPROVED REMOTE ACCESS METHODS 2

3 SPECIFIC REQUIREMENTS..... **4**

 3.1 INTERNATIONAL TRAVEL 4

 3.1.1 *Recommended Remote Access Services/Connectivity*..... 5

 3.1.2 *PIV Credentials* 6

 3.1.3 *Long-Term International Travel* 6

 3.1.4 *Electronic Media Sanitization and Quarantine* 6

 3.2 NON-NRC COMPUTERS REMOTE ACCESS WITHIN THE UNITED STATES 6

 3.3 REMOTE ACCESS RESTRICTIONS PER DEVICE TYPE THROUGH PERMITTED METHODS 7

 3.4 USE OF REMOTE ACCESS METHODS 10

APPENDIX A. ACRONYMS **11**

APPENDIX B. GLOSSARY **12**

List of Tables

Table 2.1-1: Approved Remote Access Methods 2

Table 3.1-1: International Travel Permitted Services and Capabilities 5

Table 3.3-1: Remote Access Per Device Type through Permitted Methods 8

Computer Security Standard CSO-STD-2105

NRC User Remote Access and International Travel Security Standard

1 PURPOSE

CSO-STD-2105, “NRC User Remote Access and International Travel Security Standard,” provides the minimum security requirements that must be met by users for remote access to the Nuclear Regulatory Commission (NRC) systems (e.g., networks, applications, remote desktop). The standard also provides minimum security requirements for international travel.

This standard covers remote access to NRC systems that process information up to, and including, the Sensitive Unclassified Non-Safeguards Information (SUNSI) or Controlled Unclassified Information (CUI) levels.

NRC remote access services approved for NRC users (e.g., staff, contractors) are:

- Virtual Private Network (VPN): Users can access NRC networks, systems, and applications in a similar manner to what is accessible when connected onsite at an NRC facility by utilizing a remote VPN connection. Further details are provided in the *Mobile Desktop Users Guide*¹ through the NRC Service Catalog.
- Citrix Broadband Remote Desktop (BRD): Users can remotely access an NRC desktop and use NRC applications. The Citrix BRD provides access to the user desktop through NRC BRD. Further details are provided in *Remote Access: Citrix* site² through the NRC Service Catalog.
- Direct Access (DA) to NRC Applications over the Internet: Users can access other NRC resources, such as email, the NRC intranet, and shared files.

This standard applies to remote access through the following devices, under the terms and conditions identified in the NRC Service Catalog under *Loaner Devices and Mobile Solutions*³ and *Password and Identity Management > Remote Access: Citrix*⁴:

- NRC Mobile Desktops
- NRC Loaner Mobile Desktops – Domestic
- NRC Loaner Mobile Desktops – International

¹ NRC Service Catalog > Loaner Devices and Mobile Solutions provides link to *Mobile Desktop User Guide*: <https://drupal.nrc.gov/ocio/catalog/247>

² NRC Service Catalog > Password and Identity Management > Remote Access: Citrix: <https://drupal.nrc.gov/ocio/catalog/704>

³ NRC Service Catalog > Loaner Devices and Mobile Solutions: <https://drupal.nrc.gov/ocio/catalog/247>

⁴ NRC Service Catalog > Password and Identity Management > Remote Access: Citrix: <https://drupal.nrc.gov/ocio/catalog/704>

- Bring Your Own Device (BYOD) or Government Furnished Equipment (GFE) Smartphones and Tablets
- Non-NRC Computers⁵

2 GENERAL REQUIREMENTS

This section addresses the general requirements that all users must comply with as the minimum set of controls.

NRC Mobile Desktops are **not permitted** to be taken outside of the United States (Contiguous United States/Outside Contiguous United States [CONUS/OCONUS]).

For international travel, **all permitted devices** and applicable security requirements are specified in Section 3.1, International Travel.

The ability to print from remote devices (e.g. NRC issued laptops, NRC loaner laptops, personal computers) **is limited** to situations that involve legal requirements and are reviewed on a case-by-case basis.


All users must comply with requirements specified in the user's approved NRC Telework Program Participation Agreement (Form 624), in addition to the requirements specified in this standard.

Contractors may be subject to greater, more stringent requirements specified in their contract based upon direction provided by the Contracting Officer's Representative (COR) or Contracting Officer (CO).

2.1 Approved Remote Access Methods



All users must use one of the NRC approved remote access methods identified in Table 2.1-1 to access NRC systems remotely.

Table 2.1-1: Approved Remote Access Methods

Remote Access Method	Description
VPN 	<p>Preferred method for remote access while using NRC Mobile Desktops or NRC Loaner Mobile Desktop – Domestic. The NRC Mobile Desktop or NRC Loaner Mobile Desktop – Domestic is the NRC-assigned Government Furnished Equipment (GFE) laptop for an NRC user. Allows full access to the NRC network and systems. VPN access is initiated by the icon on the NRC Mobile Desktop. [Note: NRC Loaner Mobile Desktops – Domestic are also referred to as domestic loaner laptops.]</p> <p>VPN access must be set up in accordance with requirements specified in the <i>Mobile Desktop User Guide</i>.⁶</p>

⁵ Non-NRC computers include, but not limited to, home computers, non-NRC contractor laptops exceptions, etc.

⁶ NRC Service Catalog > Loaner Devices and Mobile Solutions provides link to *Mobile Desktop User Guide*: <https://drupal.nrc.gov/ocio/catalog/247>

Remote Access Method	Description
<p>Citrix BRD</p> 	<p>Preferred method for remote access while using NRC Loaner Mobile Desktops – International,⁷ or non-NRC computers. [Note: NRC Loaner Mobile Desktops – International are also referred to as International Loaner Laptops.]</p> <p>Enables access to an NRC Microsoft Windows desktop and access to the NRC network and applications through that environment.</p> <p>Citrix BRD access must be set up in accordance with requirements specified in <i>Remote Access: Citrix</i>.⁸</p>
<p>DA To NRC Applications Over the Internet</p>	<p>DA permits access to NRC applications, while using NRC Mobile Desktops, NRC Loaner Mobile Desktops – Domestic, NRC Loaner Mobile Desktops – International, non-NRC computers, and BYOD or GFE mobile devices (NRC-assigned and loaner devices).⁹</p>
<p> MaaS360</p>	<p>DA examples of NRC applications that can be accessed directly include:</p> <ol style="list-style-type: none"> 1. Microsoft 365 (M365), which was formerly referred to as Office 365 (O365): <ul style="list-style-type: none"> – Provides a collaboration platform in a cloud environment. These applications enable NRC users to collaborate and manage information in performance of their daily tasks.¹⁰ – Specific M365 apps are also permitted for use on Android and iOS devices as specified on the OCIO Mobility Services SharePoint site.¹¹ 2. MaaS360: <ul style="list-style-type: none"> – Provides access to user emails, calendar, contacts, and tasks while using NRC BYOD or GFE mobile device. To utilize MaaS360 and access Mobile Solutions contents, any user mobile device must be enrolled in the NRC Mobility Service program as defined in the NRC Service Catalog.¹² <p>The NRC Mobility Service program supports the latest Apple iOS and Google Android operating systems for BYODs, which permits NRC users not issued a GFE smartphone or tablet to access NRC productivity applications on the go.¹³</p> <p>M365 and other applications, such as, Webmail, Box for Enterprise File Synchronization and Sharing (EFSS), etc., must be accessed in accordance with the process identified in <i>E-mail, Meetings, and File Services</i>¹⁴ through the NRC Service Catalog. NRC applications (e.g., Talent Management System (TMS), iTravel, Training) are accessible through the NRC@Work Web page.¹⁵</p> <p>All use is subject to requirements specified in Section 3, Specific Requirements.</p>

⁷ NRC Service Catalog > Loaner Devices and Mobile Solutions – Provides information on Loaner Mobile Desktop – International / International Loaner Laptop devices: <https://drupal.nrc.gov/ocio/catalog/247>

⁸ NRC Service Catalog > Password and Identity Management > Remote Access: Citrix: <https://drupal.nrc.gov/ocio/catalog/704>

⁹ NRC Service Catalog > Loaner Devices - Provides information on loaner smartphones and tablets: <https://drupal.nrc.gov/ocio/catalog/31187>

¹⁰ Microsoft Office 365 (O365) for NRC staff and contractors: <https://drupal.nrc.gov/ocio/catalog/32634>

¹¹ OCIO Mobility Services – M365 Applications for Mobile Endpoints: https://usnrc.sharepoint.com/sites/ocio-mobility-public/SitePages/User_Guides/M365_Apps_for_Mobile_Endpoints/Overview.aspx

¹² NRC Service Catalog: <https://drupal.nrc.gov/ocio/catalog/247>

¹³ NRC Service Catalog > Loaner Devices and Mobile Solutions > Bring Your Own Device (BYOD): <https://drupal.nrc.gov/ocio/catalog/246>.

¹⁴ NRC Service Catalog > E-Mail, Meetings and File Services: <https://drupal.nrc.gov/ocio/catalog/831>

¹⁵ NRC@Work Web page: <https://drupal.nrc.gov>

3 SPECIFIC REQUIREMENTS

This section provides specific user security requirements for remote access to NRC systems and for international travel.

Requirements for the use of and NRC remote access using licensee wireless networks is addressed in the NRC Chief Information Officer (CIO) Memorandum “United States Nuclear Regulatory Commission Use of Licensee Wireless Technology,” issued on December 31, 2015.¹⁶

3.1 International Travel

NRC users travelling outside of the United States on official business are permitted to use the following devices subject to the requirements in this section:

- NRC Loaner Mobile Desktop – International (also referred to as International Loaner Laptops)
- International Loaner Smartphone
- International Loaner Tablet
- NRC-assigned GFE Smartphone
- NRC-assigned GFE Tablet
- Personal Mobile BYOD Mobile Device
- Disposable Phone

NRC Mobile Desktops or NRC Loaner Mobile Desktop – Domestic devices are **not permitted** to be taken outside of the United States (CONUS/OCONUS) due to security reasons, including the significant potential for a compromise of the device and sensitive information. The agency depends on counterintelligence elements/information to determine how devices may be used. Further information is available within the International Official Travel Frequently Asked Questions (FAQ) intranet site.¹⁷

Table 3.1-1, International Travel Permitted Services and Capabilities, below provides the permissible service and capabilities for these devices during international travel. Sensitive NRC information is not to be placed on devices taken on international travel.

¹⁶ NRC CIO [Memorandum: U.S. Nuclear Regulatory Commission Use of Licensee Wireless Technology \(ML14301A250\)](https://adamsxt.nrc.gov/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId=%7b2713C1C6-45F6-4614-8195-F2D97125C4A1%7d&ForceBrowserDownloadMgrPrompt=false): <https://adamsxt.nrc.gov/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId=%7b2713C1C6-45F6-4614-8195-F2D97125C4A1%7d&ForceBrowserDownloadMgrPrompt=false>

¹⁷ Refer to the Information Technology (IT) Security and Counter-Intelligence sections under the “Safety and Security” portion of the International Official Travel FAQ: <https://drupal.nrc.gov/oip/34444>

Table 3.1-1: International Travel Permitted Services and Capabilities

	NRC Loaner Mobile Desktop – International	International Loaner Smartphone	International Loaner Tablet	NRC- Assigned GFE Smartphone	NRC- Assigned GFE Tablet	Personal Mobile BYOD Mobile Device
Permitted Services / Connectivity						
Wireless (Wi-Fi) Connectivity	√	√	√	√	√	√
Cellular (Carrier) Connectivity	√	√	√	√	√	√
International Carrier Service		√	√	√	√	√
Permitted Capabilities						
MaaS360 PIM (Personal Information Management) and DNA (Direct Network Access)		√	√	√	√	√
One-Time Password App (Symantec VIP) ¹⁸		√	√	√	√	√
Microsoft 365 Access ¹⁹	√	√	√	√	√	√
Remote Access via Citrix BRD (Wi-Fi or carrier access via physically connected Mi-Fi cellular modem)	√	√	√	√	√	√

Any use of services and capabilities other than what is specified in Table 3.1-1 is ***not permitted***.

3.1.1 Recommended Remote Access Services/Connectivity

During international travel, NRC users should strive to use remote access connectivity in the following manner to provide greater security:

1. Use cellular connectivity as the preferred method to obtain connectivity for your device(s).

¹⁸ Symantec VIP mobile application: If the mobile app is expected to be available / in use during international travel, it should be installed before the travel occurs.

¹⁹ Per CISO direction, M365 mobile apps (Android, iOS) are only permitted for use within the United States: https://usnrc.sharepoint.com/teams/OCIO-CSO/CSO_FISMA_Repository/FISMA_Systems/OCIO-ITI/AO_CISO_Decisions/FY21_ITI_CISO_Approval_of_%20M365_Apps_on_Android_and_iOS_Mobile_Devices_from_Pilot_to_All_NRC_Users_20201028.pdf

2. If cellular connectivity does not exist or is not reliable, then NRC users may connect via Wi-Fi networks, such as via a hotel or other available network.

3.1.2 PIV Credentials

When using NRC Loaner Mobile Desktop – International / International Loaner Laptops for international travel, a local account must be provided in advance of travel, as Personal Identity Verification (PIV) cards are not used. The Yellow Announcement (YA), YA-20-0056, “Policy on the Use of Personal Identity Verification Credentials as Identification During International Travel,”²⁰ specifies that NRC employees and contractors are not to travel abroad with agency-issued PIV cards. User authentication for the NRC-issued International Loaner Laptops can be securely accomplished without the PIV card by using the hardware one-time password (OTP) fob or mobile app. This is done in a similar manner to how hardware OTP fob or mobile app authenticators are used with NRC-assigned, loaner, and BYOD mobile devices.

3.1.3 Long-Term International Travel

During long-term international travel (e.g., greater than one month), NRC personnel may purchase disposable phones in country for communicating with colleagues to minimize charges to NRC. Disposable phones are only permitted to use Wi-Fi and Cellular (Carrier) Connectivity for communication with peers via voice and text.

3.1.4 Electronic Media Sanitization and Quarantine

Electronic media sanitization and quarantine requirements, which apply following the completion of international travel, are specified in CSO-STD-2004, “Electronic Media and Device Handling Standard.”

3.2 Non-NRC Computers Remote Access within the United States

While non-NRC computers (e.g., home computers, contractor laptops exceptions) may be used in specific circumstances to remotely access NRC systems, users must comply with the following requirements:

- Use DA to connect with NRC applications over the Internet:
 - DA applications (e.g., M365, webmail) protect NRC information from potential breaches through implementing security features, such as restricting downloading of files from non-NRC computers.
 - NRC applications approved for remote access using a non-NRC computer by the NRC Authorizing Official (AO) or an AO delegate. If NRC applications have been approved for remote access by a non-NRC computer (e.g., M365, MaaS360), that approval should be specifically identified within the NRC Service Catalog.

²⁰[YA-20-0056, “Policy on the Use of Personal Identity Verification Credentials as Identification During International Travel:”
https://drupal.nrc.gov/announcements/yellow/policy/61359](https://drupal.nrc.gov/announcements/yellow/policy/61359)

- Refer specifically to the *Remote Access: Citrix* site through the NRC Service Catalog for services that can be used for remote access to NRC systems using a non-NRC computer.²¹
- Consider best practices for secure configuration of home computers, home networks, and use of public hotspots to help protect NRC information while performing NRC work remotely, such as the “National Security Agency (NSA) Cybersecurity Information (CSI) Best Practices for Keeping Home Networks Secure²².”

3.3 Remote Access Restrictions Per Device Type Through Permitted Methods

NRC users may remotely access NRC systems based upon specified network types and device types (i.e., NRC Mobile Desktops, NRC Loaner Mobile Desktops – Domestic, non-NRC computers, and BYOD or GFE smartphones and tablets) with NRC permitted methods used for access.

Remote access for NRC Mobile Desktops, NRC Loaner Mobile Desktops – Domestic, non-NRC computers, and BYOD or GFE smartphones or tablets must:

- Originate only from the network types listed in Table 3.3-1, Remote Access Per Device Type through Permitted Methods, below, within the United States, and
- Is contingent upon the use of an approved remote access method, as specified in Section 2.1, Approved Remote Access Methods.

NRC Mobile Desktops or NRC Loaner Mobile Desktop – Domestic are **not permitted** to be taken outside of the United States (CONUS/OCONUS).

All users must comply with the remote access restrictions per remote access method for each device type while establishing a connection through the network types specified in Table 3.3-1. Anything other than what is specified in Table 3.3-1 is **not permitted**.

²¹ NRC Service Catalog > Password and Identity Management > Remote Access: Citrix, specifically Description, Guidelines and FAQs tabs: <https://drupal.nrc.gov/ocio/catalog/704>

²² NSA CSI Best Practices for Keeping Home Networks Secure: <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf>

Table 3.3-1: Remote Access Per Device Type through Permitted Methods

Network Type (Within the United States)		Remote Access Per Device Type Through Permitted Methods (VPN, Citrix BRD=BRD, Direct Access=DA)				
		Mobile Desktop	Loaner Mobile Desktop- Domestic	Non-NRC Computer	BYOD Smartphones/ Tablets	GFE Smartphones/ Tablets
Home Networks	Wired Networks	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	Not Applicable	Not Applicable
	Wireless Networks	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
Cellular Networks	GFE Cellular Hotspot : Connection via Wi-Fi	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	GFE Cellular Hotspot: Connection via Wired port	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	GFE Cellular Hotspot: Connection via Universal Serial Bus (USB) tethering	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	Not Applicable	Not Applicable
	GFE Laptop Cellular Air Card (e.g., USB, Peripheral Component Interconnect (PCI) Express cellular modem)	VPN, BRD, DA	VPN, BRD, DA	Not Allowed	Not Applicable	Not Applicable
	Non-GFE Cellular Hotspot: Connection via WiFi	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	Non-GFE Cellular Hotspot: Connection via Wired port	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	Non-GFE Cellular Hotspot: Connection via USB tethering	Not Allowed	Not Allowed	BRD, DA	BRD, DA	Not Allowed
	Non-GFE Laptop Cellular Air Card (e.g., USB, PCI Express cellular modem)	Not Allowed	Not Allowed	BRD, DA	Not Applicable	Not Applicable
Travel Networks	Hotel/Lodging Networks: Wired	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	Not Applicable	Not Applicable
	Hotel/Lodging Networks: Wireless	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	Transit (e.g., Airplane, Airport, Rail, Bus) Networks: Wired	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	Not Applicable	Not Applicable
	Transit (e.g., Airplane, Airport, Rail, Bus) Networks: Wireless	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA

Network Type (Within the United States)		Remote Access Per Device Type Through Permitted Methods (VPN, Citrix BRD=BRD, Direct Access=DA)				
		Mobile Desktop	Loaner Mobile Desktop- Domestic	Non-NRC Computer	BYOD Smartphones/ Tablets	GFE Smartphones/ Tablets
Business Guest Networks	NRC Guest Wireless Network ²³	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
	Other Business Guest Wireless Networks	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
Licensee Networks	Licensee Wireless Networks ²⁴	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA
Other, Non-NRC Business Networks	Excludes Guest Networks	Not Allowed	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Other Publicly Accessible Wireless Networks	This refers to wireless networks that are specifically available for use by an organization/business' customers/visitors (e.g., libraries, telework centers). This does not include wireless networks if it is not clear that the network is available for purpose (e.g., unprotected wireless networks in an apartment/condominium building).	VPN, BRD, DA	VPN, BRD, DA	BRD, DA	BRD, DA	BRD, DA

²³ NRC Service Catalog > Network Operations > Guest Wireless Services: <https://drupal.nrc.gov/ocio/catalog/25028>

²⁴ NRC CIO Memorandum: U.S. Nuclear Regulatory Commission Use of Licensee Wireless Technology (ML14301A250): <https://adamsxt.nrc.gov/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId=%7b2713C1C6-45F6-4614-8195-F2D97125C4A1%7d&ForceBrowserDownloadMgrPrompt=false>

3.4 Use of Remote Access Methods

The following sequence of remote access methods should be used while connecting through the network types specified in Table 3.3-1, Remote Access Per Device Type.

- NRC Mobile Desktops or NRC Loaner Mobile Desktop – Domestic:
 - A VPN connection should be used as the primary/preferred remote access method.
 - If a VPN connection is not available (e.g., due to service inaccessibility, technical difficulties), the other permissible remote access methods (i.e., Citrix BRD or DA) may be used.
- NRC Loaner Mobile Desktop – International or Non-NRC Computers:
 - A Citrix BRD connection should be used as the primary/preferred remote access method.
 - If the Citrix BRD connection is not available (e.g., due to service inaccessibility, technical difficulties), DA to NRC applications over the Internet may be used; this is the only other permissible remote access method available.
- BYOD or GFE Smartphones and Tablets:
 - NRC users enrolled in MaaS360 are encouraged to use the MaaS360 mobile application as the preferred mechanism to access the provided services, such as email, calendar, and contacts.

APPENDIX A. ACRONYMS

ADM	Office of Administration
AO	Authorizing Official
BRD	Broadband Remote Desktop
BYOD	Bring Your Own Device
CONUS	Contiguous United States
CIO	Chief Information Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
CSI	Cybersecurity Information
CSO	Computer Security Organization
CUI	Controlled Unclassified Information
DA	Direct Access
EFSS	Enterprise File Synchronization and Sharing
FAQ	Frequently Asked Questions
GFE	Government Furnished Equipment
IT	Information Technology
M365	Microsoft 365
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
O365	Microsoft Office 365
OCIO	Office of the Chief Information Officer
OCONUS	Outside Contiguous United States
OTP	One-Time Password
PIV	Personal Identity Verification
PCI	Peripheral Component Interconnect
SUNSI	Sensitive Unclassified Non-Safeguards Information
STD	Standard
TMS	Talent Management System
USB	Universal Serial Bus
VPN	Virtual Private Network
YA	Yellow Announcement

APPENDIX B. GLOSSARY

Bring Your Own Device	Personally owned smartphones or tablets enrolled in an authorized NRC BYOD program that can be used to establish a remote access session with the NRC system.
Controlled Unclassified Information	Requires safeguarding or dissemination controls in accordance with applicable law, regulations, and government-wide policies but is not classified.
GFE Cellular Hotspot	Utilizes 3G/4G/5G cellular networks to allow data connection via Wi-Fi, Bluetooth, or USB, with a mobile desktop or Loaner mobile desktop-domestic.
MiFi Cellular Modem	A cellular modem and hotspot providing Internet access to other devices via capabilities that include physical connection and Wi-Fi.
NRC Mobile Desktop	Laptops provided to users by the Office of the Chief Information Officer (OCIO), allowing users to remotely connect to the NRC infrastructure to access NRC resources and process information up to, and including, the SUNSI level.
NRC Telework Program Participation Agreement (Form 624)	Defines terms and conditions for a user to voluntarily agree to participate in the telework program and adhere to the applicable guidelines and policies.
PCI Express	A high-speed serial computer expansion bus standard, used as common motherboard interface for connections to computer graphic cards, modems, hard drives, etc.
Remote Access	Authenticated access to a system by an authorized user or an NRC 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.
Sensitive Unclassified Non-Safeguards Information	Generally not publicly available information and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source).
USB Tethering	Process of sharing a phone's mobile data through a USB connection to access the Internet on an NRC Mobile Desktop, NRC Loaner Mobile Desktop – Domestic, or non-NRC Computer.
Virtual Private Network	Protected system connection (through Internet) utilizing tunneling and security controls.

Wired Network

Utilizes Ethernet cables to transfer data between connected computers, switches, routers, servers, and peripheral devices.

Wireless Network

Network set up by using a radio signal frequency to communicate between computers and other network devices.

CSO-STD-2105 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
29-Oct-14	1.0	Initial Issuance	Distribution at ISSO forum and posting on CSO Web page	Upon request
10-Dec-19	2.0	Broadened scope and updated with the latest requirements including international travel	Post to OCIO/CSO website	Upon request
20-Apr-20	2.1	Clarified requirements for printing from remote devices	Post to OCIO/CSO website	Upon Request
30-Nov-20	2.2	Updated to permit greater use of Citrix BRD during international travel. Added reference to YA-20-0056 regarding PIV card restriction on international travel. Additional updates to reflect permitted use of M365 mobile apps.	Post to OCIO/CSO website	Upon Request