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

Office Instruction:	**CSO-STD-2111**
Office Instruction Title:	**Remote Access Enterprise Security Architecture Standard**
Version Number:	**1.0**
Effective Date:	**September 15, 2021**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Description:	CSO-STD-2111 “Remote Access Enterprise Security Architecture Standard,” provides the minimum security requirements that must be met for remote access to NRC systems processing information up to, and including, the Sensitive Unclassified Nonsafeguards Information (SUNSI) or Controlled Unclassified Information (CUI) (excluding Safeguards Information [SGI]) level.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	8/17/2021
CISO (Acting)	Garo Nalabandian	/RA/	8/23/2021

TABLE OF CONTENTS

List of Tables

Computer Security Guidance
CSO-STD-2111
Remote Access Enterprise Security Architecture Standard

1 PURPOSE

CSO-STD-2111, "Remote Access Enterprise Security Architecture Standard," provides the minimum security requirements that must be met for remote access to Nuclear Regulatory Commission (NRC) systems (e.g., networks, applications, remote desktop) processing information up to, and including, the Sensitive Unclassified Nonsafeguards Information (SUNSI) or Controlled Unclassified Information (CUI) (excluding Safeguards Information [SGI]) level.

This standard is intended for system administrators, system and solution architects, information technology (IT) system managers (operational and project-related), system owners, and Information System Security Officers (ISSOs) who must ensure to apply and enforce the remote access security requirements.

Remote access requires endpoint-based identification and authentication to ensure access is only permitted to authorized endpoints. The endpoints can be either physical or logical in nature and are placed at the originating or terminating end of a communications channel. Examples of endpoints include, NRC Desktops, NRC Mobile Desktops, smartphones, tablets, servers, gateways, Platform as a Service (PaaS) devices, or System as a Service (SaaS) Application Program Interfaces (APIs) in a cloud environment.

This standard applies to remote access through the following endpoints, under the terms and conditions identified in the NRC Service Catalog under *Loaner Devices and Mobile Solutions*[1] and *Password and Identity Management > Remote Access: Citrix*[2]:

- NRC Mobile Desktops
- NRC Loaner Mobile Desktops
- Bring Your Own Device (BYOD) or Government Furnished Equipment (GFE) Smartphones and Tablets
- Non-NRC Computers[3]

CSO-STD-2111 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 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.

---

[1] *NRC Service Catalog > Loaner Devices and Mobile Solutions*: 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] Non-NRC computers include, but not limited to, home computers, non-NRC contractor laptop exceptions, etc.

Refer to CSO-GUID-2111, “Remote Access Enterprise Security Architecture Guidance,” which facilitates compliance with this standard.

This standard does **not** apply to:

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

2 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 NRC endpoints (e.g.,NRC Mobile Desktops, Loaner Mobile Desktops, GFE smartphones and tablets) 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.

NRC Mobile Desktops must not be permitted to be taken outside of the United States. Technical measures should be implemented to detect unauthorized usage of NRC Mobile Desktops outside the United States and report this usage to Office of the Chief Information Officer (OCIO) Security Operations.

2.1 NRC-Approved Hardware and Software

All NRC 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.

2.2 Approved Remote Access Methods

NRC systems processing information up to, and including, the SUNSI or CUI (excluding SGI) level must only allow NRC users (e.g., staff, contractors) to remotely access NRC resources using the approved remote access methods listed in Table 2.2-1.

Table 2.2-1: Approved Remote Access Methods

Remote Access Method	Description
Virtual Private Network (VPN)	Provides access to NRC networks, systems, and applications in a similar manner to what is accessible when connected onsite at an NRC facility.
Citrix Broadband Remote Desktop (BRD)	Allows users to remotely access desktop or NRC applications through Citrix (Receiver or Workspace).
Direct Access (DA) to NRC Applications over the Internet	Provides access to NRC resources, such as email, other office productivity applications, and shared files.

The remote access methods must be used in conjunction with the appropriate user identification and authentication methods, as specified in the *NRC Service Catalog*.[4] Further information related to remote access methods, authentication, and encryption is provided in the CSO-GUID-2111, "Remote Access Enterprise Security Architecture Guidance."

2.3 User Identification and Authentication

The following requirements apply regarding user identification and authentication for remote access to NRC systems:

- Valid digital identity credentials (e.g., Personal Identity Verification [PIV], One-time Password [OTP]) must be required from all users for remote access to NRC systems, in accordance with the requirements outlined in the Office of Management and Budget (OMB) memorandum (M), M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management."[5]
- Minimum digital Authenticator Assurance Levels (AAL), Identity Assurance Levels (IAL), and Federation Assurance Levels (FAL) must be used in accordance with the digital identity guidelines provided in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3,"Digital Identity Guidelines,"[6] and requirements outlined in the OMB M-19-17. These requirements must be met for all NRC users in accordance with CSO-PROS-2001, "CSO System Security Categorization Process."
- The NRC Improved Identity, Credential, and Access Management (ICAM) Authentication Gateway is the enterprise method for user authentication that must be used to remotely access NRC systems and applications.[7]

2.4 Data in Transit

All remote access sessions must encrypt data in transit in accordance with CSO-STD-2009, "Cryptographic Control Standard."

Additionally, network ports, protocols, and services (NPPS) used for remote access must be selected, configured, and secured in accordance with CSO-STD-2008, "Network Ports, Protocol, and Services Enterprise Security Architecture Standard."

3 SPECIFIC REQUIREMENTS

This section provides specific requirements for authorized endpoints to access sensitive information (e.g., SUNSI or CUI, excluding SGI) through a remote connection to NRC systems. Endpoint identification and authentication ensures that only authorized endpoints (e.g., NRC Mobile Desktops, NRC Loaner Mobile Desktops) can establish a connection to NRC systems and access is restricted based on the information sensitivity.

---

[4] NRC Service Catalog: https://drupal.nrc.gov/ocio/26331
[5] OMB M-19-17: https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[6] NIST SP 800-63-3: https://pages.nist.gov/800-63-3/sp800-63-3.html
[7] Refer to the NRC Service Catalog > Password and Identity Management page for additional information on the NRC ICAM Authentication Gateway: https://drupal.nrc.gov/ocio/catalog/26445

3.1 Endpoint Identification-Based Restrictions

In order to enforce appropriate remote access restrictions, NRC remote access solutions must meet the following two requirements. Please note that the second requirement is dependent upon the first.

1. To protect sensitive information (e.g., SUNSI or CUI, excluding SGI) against unauthorized remote access, the following endpoint identification-based restrictions must be applied:

    - Endpoints must be identified and authenticated as to whether they are authorized to access and store SUNSI or CUI (excluding SGI). Some endpoints may be authorized to access but not authorized to store SUNSI or CUI (excluding SGI).

        For example:

        - NRC Mobile Desktops that are used to remotely access NRC systems are authorized to access, download, and store SUNSI or CUI (excluding SGI) through the remote connection.
        - Non-NRC computers (e.g., home, contractor computers) would be allowed to access, but not store or download, SUNSI or CUI (excluding SGI) through DA or Citrix BRD remote access methods.

2. Based upon the results of the endpoint identification and authentication (as specified above), the following remote access restrictions apply:

    - Endpoints that are authorized to store SUNSI or CUI (excluding SGI) are ***permitted*** to store and process SUNSI or CUI (excluding SGI) through storing or downloading of SUNSI or CUI (excluding SGI).

        For example:

        - Users accessing NRC resources through Citrix BRD on an authenticated endpoint (e.g., NRC Mobile Desktop) are permitted to store or process SUNSI or CUI (excluding SGI) through transferring data/files to local drives for external storage services. This could be accomplished through drive mapping or use of cloud services, such as the Enterprise File Synchronization and Sharing (EFSS) service (i.e., BOX-EFSS[8]) or NRC Microsoft OneDrive (part of Microsoft 365 [M365]).
        - Endpoints that are authorized to connect, but are not authorized to store and process SUNSI or CUI (excluding SGI), are ***not permitted*** to store or download files containing SUNSI or CUI (excluding SGI).

            For example:

            NRC users accessing M365 on their home computer would not be allowed to store or download files containing SUNSI or CUI (excluding SGI) to that computer.

[8] NRC Service Catalog information for BOX-EFSS: https://drupal.nrc.gov/ocio/catalog/34956

3.2 Information Sensitivity Access Restrictions

To protect remotely accessed sensitive information (e.g., SUNSI or CUI, excluding SGI), the following requirements must be applied:

- Restrict creation, download, and storage of sensitive information to only NRC approved applications and NRC authenticated endpoints.

  For example:

  - A remote user can use NRC approved applications, such as M365, to create, download, and locally store a sensitive document while using an NRC authenticated endpoint, such as an NRC Mobile Desktop through DA, VPN, or Citrix BRD methods.
  - Similarly, a BYOD mobile endpoint can use an NRC approved application, such as MaaS360, through a DA method to remotely access, create, or edit an email with sensitive information.

- Restrict all NRC endpoints from:
  - Storing or sharing sensitive data through non-NRC tenants on storage services used by NRC (e.g., OneDrive, Box).
  - Storing or sharing sensitive data through unauthorized external storage services (e.g., Dropbox, Google Drive).
- Restrict all non-NRC endpoints (e.g., non-NRC computers, BYODs) from:
  - Local storage of sensitive data, unless authorized by Authorizing Official (AO) or designee.
  - Storing or sharing sensitive data through non-NRC tenants on storage services used by NRC or unauthorized external storage service (e.g., Dropbox, Google Drive).
  - Copying and pasting, printing, taking screenshots, or performing screen recording of the remote access session (where feasible) to prevent spills of sensitive data.
  - Transferring/sharing files from the remote access method (e.g., Citrix BRD) to the local, non-NRC endpoint (e.g., BYOD tablet). In this scenario, it would require that file transfers and drive mapping be disabled for non-NRC endpoint.

APPENDIX A. ACRONYMS

AAL	Authenticator Assurance Level
API	Application Program Interface
ADAMS	Agency-wide Documents Access and Management System
AO	Authorizing Official
BRD	Broadband Remote Desktop
BYOD	Bring Your Own Device
CSO	Computer Security Organization
CUI	Controlled Unclassified Information
DA	Direct Access
EFSS	Enterprise File Synchronization and Sharing
ESA	Enterprise Security Architecture
FAL	Federation Assurance Level
GFE	Government Furnished Equipment
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ISSO	Information System Security Officer
IT	Information Technology
M	Memorandum
M365	Microsoft 365
NIST	National Institute of Standards and Technology
NPPS	Network Ports, Protocols, and Services
NRC	Nuclear Regulatory Commission
OCIO	Office of Information Services
OMB	Office of Management and Bedget
OTP	One-time Password
PaaS	Platform as a Service
PIV	Personal Identity Verification
SaaS	System as a Service
SP	Special Publication
SGI	Safeguards Information
STD	Standard
SUNSI	Sensitive Unclassified Nonsafeguards Information
TRM	Technical Reference Model
VPN	Virtual Private Network

APPENDIX B. GLOSSARY

BOX-EFSS Service	BOX-EFSS is a cloud-based collaboration tool that provides a secure way to share information with external entities.
Controlled Unclassified Information	Information that requires safeguarding or dissemination controls in accordance with applicable law, regulations, and government-wide policies but is not classified.
Direct Access Applications	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 or CUI (excluding SGI) level while encrypting data in transit.
Digital Authentication	The process of establishing confidence in user identities electronically presented to a system.
Endpoint	A physical or logical entity, that is placed at the originating or terminating end of a communication channel.
External Network	Networks that interconnect with the NRC network or are used by individuals to connect to NRC networks, systems, and applications.
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.
NRC Loaner Mobile Desktop	Laptops provided by OCIO to users for presentations, travel on agency business, or for other work-related uses. The two types of NRC Loaner Mobile Desktops are: a. NRC Loaner Mobile Desktop - Domestic: Permitted for use within the NRC and while on domestic (United States) travel. b. NRC Loaner Mobile Desktop - International: Permitted for travel outside of the United States.
NRC Mobile Desktop	Laptops provided to users by the OCIO, allowing users to remotely connect to the NRC infrastructure to access NRC resources and process information up to, and including, the SUNSI or CUI (excluding SGI) level.
NRC Managed Networks	Networks that are managed or operated by NRC personnel at NRC facilities and include Infrastructure Support and Business/Application Networks, and NRC Extended Networks.
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.
Remote Access	Remote access is authenticated access to a system by an authorized user or an authorized endpoint communicating through the Internet.
Remote Access Method	The vendor and product agnostic means of providing remote access to an NRC system.
Safeguards Information	A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected.

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).
Tenant	Within the scope of cloud service, a tenant refers to a customer's instance of the cloud service. Thus, specifying "NRC tenant" would refer to NRC's specific instance of a cloud service and exclude instances of the cloud service for other customers, and vice versa.
Tunneling	A method to send data that is encapsulated and transmitted over the network using Point-to-Point Tunneling Protocol.
Virtual Private Network	Protected system link utilizing tunneling and security controls.

CSO-STD-2111 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
17-Aug-21	1.0	Initial release	Post to OCIO/CSO Standards SharePoint site	Upon request
3-Feb-22	1.0	Errata issuance to correct PDF conversion issue for posting.	Post to OCIO/CSO Standards SharePoint site	Upon request