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

Office Instruction:	**OCIO-CS-STD-4000**
Office Instruction Title:	**Network Infrastructure Standard**
Revision Number:	**1.2**
Issuance Date:	**Date of last signature below**
Effective Date:	**Upon Issuance**
Primary Contacts:	**Kathy Lyons-Burke, Senior Level Advisor for Information Security**
Responsible Organization:	**OCIO**
Summary of Changes:	OCIO-CS-STD-4000, "Network Infrastructure Standard," provides the minimum standard that must be applied to the NRC network-computing environment.
Training:	As requested
ADAMS Accession No.:	ML16302A389

Approvals			
Primary Office Owner	Office of the Chief Information Officer	**Signature**	**Date**
Enterprise Security Architecture Working Group Chair	Kathy Lyons-Burke	R/A	28-Nov-16
Chief Information Officer	David Nelson	R/A	29-Nov-16
Chief Information Security Officer	Tom Rich	R/A	10-Jan-17

TABLE OF CONTENTS

List of Figures

List of Tables

Computer Security Standard
OCIO-CS-STD-4000
Network Infrastructure Standard

1 PURPOSE

OCIO-CS-STD-4000, "Network Infrastructure Standard," provides the minimum security requirements that must be applied to the Nuclear Regulatory Commission (NRC) network-computing environment. This standard provides security considerations at the network level that are needed to provide an acceptable level of risk for NRC information processing. This standard introduces the concepts of network types; network trust level relationships; network segmentation; network structure; network devices and technology; and network resources.

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.

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."

OCIO-CS-STD-4000 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 maintenance of the NRC network infrastructure. The requirements are derived from the following high-level concepts and terminology associated with the NRC network.

2.1 Requirement Definitions and Identifiers

Throughout this standard different terms and terminology are used to describe whether a requirement is mandatory, an administrative or implementation choice, or a recommended best practice. The following terminology definitions are used:

- *Must* indicates a mandatory requirement.
- *May* indicates an administrative or implementation choice.
- *Should* indicates a recommendation or current best practice.

A behavior or condition that is allowed but not always required is described as *is permitted*. A behavior or condition that is never allowed is described as *not permitted*.

Within this standard, each requirement is assigned a unique identifier (e.g., NI-NSP-G1) that identifies the:

- Standard (i.e., NI);
- Requirement category (e.g., NSP, for Sections 3.9, Network Security Protections, and 4.1.2, Network Security Protections); and
- Type of requirement (i.e., "G" for General Requirements, "S" for Specific Requirements) and which requirement within a category that may contain multiple requirements (e.g., G1, G2, G3, etc. or S1, S2, S3, etc.).

2.2 Information Sensitivity

Information processed within NRC networks can be of different sensitivity levels. These sensitivity levels dictate specific trust levels between networks and specific security requirements.

- Sensitive Unclassified Non-Safeguards Information (SUNSI): NRC managed networks and networks managed on behalf of NRC are permitted to only process information up to, and including, the SUNSI level (aka SUNSI and below). SUNSI is divided into two categories, plaintext SUNSI and encrypted SUNSI:
  - Plaintext SUNSI: SUNSI that has no form of encryption.
  - Encrypted SUNSI: SUNSI that is encrypted in accordance with CSO-STD-2009, "Cryptographic Control Standard."
- SGI: Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant that are designed to protect special nuclear material or to protect the physical location of certain plant equipment that is vital to the safety of production/utilization facilities. SGI is divided into two categories, plaintext SGI and encrypted SGI:
  - Plaintext SGI: SGI that has no form of encryption.
  - Encrypted SGI: SGI that is encrypted in accordance with CSO-STD-2009.

- Classified Information: Restricted Data, Formerly Restricted Data, and National Security Information processed or produced by a system that requires protection against unauthorized disclosure in the interest of national security. Classified information is divided into two categories, plaintext classified information and encrypted classified information:
    - Plaintext Classified Information: Classified information that has no form of encryption.
    - Encrypted Classified Information: Classified information that is encrypted in accordance with CSO-STD-2009.

2.3 Security Categorizations and Impact Levels

The Federal Information Processing Standards (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and information Systems," defines security categories for unclassified information systems based on:

1. The potential impact on organizations, assets, or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability. FIPS PUB 199 divides impact levels into three categories:

    - Low: The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
    - Moderate: The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
    - High: The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

2. The formula for determining a security category (SC):

    SC = {(confidentiality, impact), (integrity, impact), (availability, impact)},
    where the acceptable values for potential impact are Low, Moderate, or High.

The SC is represented by the high water mark (e.g., the highest value assigned) of the three potential impacts, however, the levels for confidentiality, integrity, and availability are considered separately when determining required security controls.

Networks or systems may contain other smaller networks or subsystems with different information sensitivities and impact levels.

For more information regarding security categorizations and impact levels, refer to http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

2.4 Introduction to Basic Network Architecture

In order to apply the requirements defined within this standard, a basic understanding of networking and network architecture is needed. This section describes the basic principles found in network design and topology that can be applied to the networks described within this standard. Figure 2.5-1, Basic Network, illustrates how a basic network can be logically divided into two main parts, an intranet and a demilitarized zone (DMZ).

The intranet is the internal network that provides users with access to network resources and applications. The intranet can contain both workstation groups and server groups. A DMZ is located at the perimeter of a network and provides a buffer between the intranet and other networks. DMZs are used to protect the internal network by separating that network from other networks. In order to access the intranet, all communication passes through the DMZ. DMZs are externally facing and offer services to other networks. The NRC DMZ provides separation from the NRC intranet and the Internet and provides services such as the Web, mail, and Domain Name System (DNS) services. The NRC network consists of many smaller networks, each with an intranet and DMZ. The combination of all the networks within the NRC is considered the NRC intranet. The NRC network also has guest networks that allow non-NRC users to access the Internet.

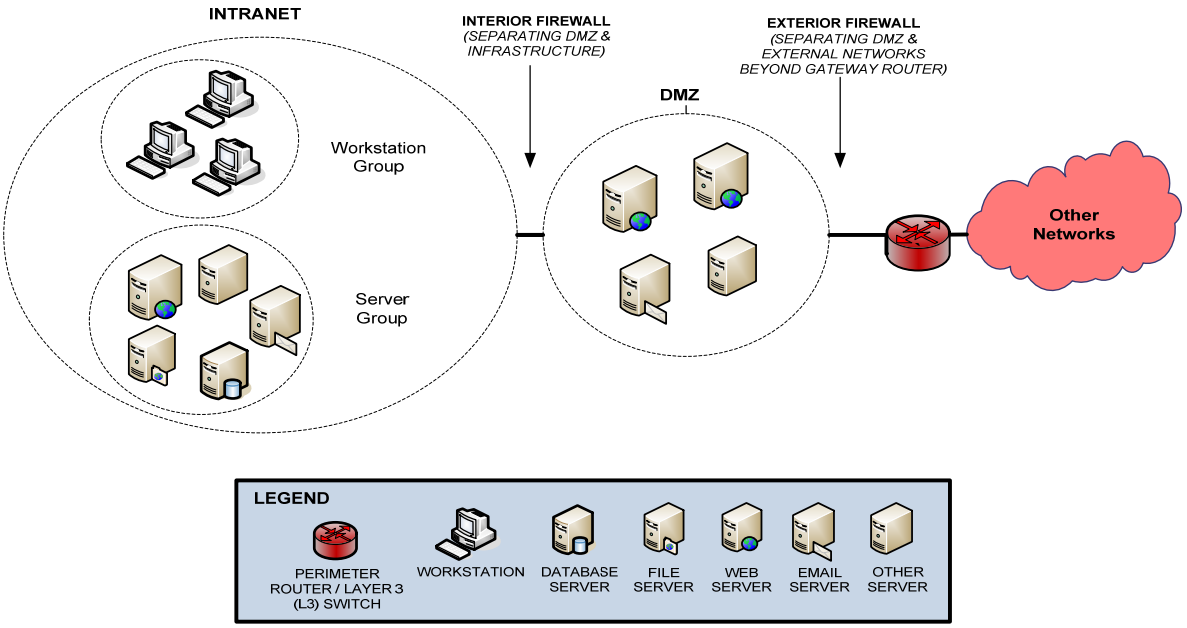


Figure 2.5-1: Basic Network

2.5 Network Types

The network type reflects the nature of the network in use. Network types allow for differing levels of information processing and controls to be associated with the different information types and permit construction of rule sets for interconnecting different networks.

NRC network types are organized from a logical standpoint into hierarchies (i.e., parent and child networks). There are three overarching NRC network categories to place specific parent and child network types:

- NRC managed networks
- Networks managed on behalf of NRC
- External networks

For NRC managed networks and networks managed on behalf of NRC, there are mission, business, and information technology (IT) function-oriented networks that can fall into both the NRC managed networks parent type and the networks managed on behalf of NRC parent type. Some child networks may also fall into several different parent network types and contain network subtypes.

The following sections identify the parent and child network types under each NRC network category. Security requirements and network trust levels are determined based on the parent and child network types.

2.5.1 NRC Managed Networks

NRC managed networks are networks that are managed by NRC and are operated and/or hosted by NRC. Table 2.6-1, NRC Managed Networks, identifies and describes all NRC managed networks.

Table 2.6-1: NRC Managed Networks

NRC Managed Networks	
Parent Network Type	**Child Network Type**
NRC Wide Area Network (WAN)	NRC uses a Multi-protocol Label Switching (MPLS) WAN to provide connectivity across NRC Headquarters (HQ) to different Regional Offices (ROs) and the Technical Training Center (TTC). This group of networks comprises the NRC WAN. The ROs and TTC connect back to HQ and utilize a Trusted Internet connection to access the Internet. NRC HQ consists of all NRC sites located within the Washington Metropolitan Area and provides the IT backbone and many of the infrastructure networks for each of the sites and to the WAN. ROs and the TTC are located outside the geographic boundaries of NRC HQ; however, these remote sites are also operated as part of the NRC managed networks. NRC WAN also includes the following child networks: • Infrastructure Networks – Also referred to as Infrastructure Support (IS) Networks, provide infrastructure support services (e.g., identity, access management, time, DNS) to other systems/networks. • Business/Application (BA) Networks – Networks hosting specific business area system(s) and application(s). These networks support the specific business and mission functions of the NRC and do not provide specific support for the NRC network core infrastructure.

Table 2.6-1: NRC Managed Networks

NRC Managed Networks	
Parent Network Type	**Child Network Type**
	• Resident Inspector Site Expansion (RISE) Networks – A remote worksite located at power plant licensee facilities for resident inspectors to access the NRC network and to perform assigned duties. The NRC internal network, managed by the NRC, contains the infrastructure and business/application networks that provide the resources NRC users need to accomplish the NRC mission.
NRC Extended Networks	Extended networks exist where the NRC network is connected to a specific remote facility. In these networks, NRC controls both endpoints. NRC extended networks include: • Extended Licensee (NRCEL) Networks – NRC provided equipment used at licensee sites to collect emergency data for emergency response purposes.
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. NRC special purpose networks include: • Management Network – An isolated network hosting Network Management Systems (NMS) that collect security event log information from any/all NRC managed networks and also provide command and control capabilities that are used for the operation, administration, maintenance, and provisioning of the NRC managed network. • Standalone Office Local Area Networks (LANs) – Offices can use a separate standalone LAN located outside the boundaries of the NRC WAN and use a Trusted Internet Connection (TIC) for Internet connectivity. RO LANs are considered Standalone Office LANs. • Guest Networks – Networks provided for use by individuals that do not have permission to access the NRC internal network. These individuals may include foreign assignees and NRC visitors. • Research and Development (Nuclear) – Networks used to conduct analyses to support the regulatory mission. • Research and Development (IT) – Networks used to conduct research and product development for IT-related activities. • High Performance Computing (HPC) – Specialized computing network or network cluster designed for performance and typically used to carry out complex calculations.

2.5.2 Networks Managed on Behalf of NRC

Networks managed on behalf of NRC are 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.

Table 2.6-2 identifies and describes all networks managed on behalf of NRC.

Table 2.6-2: Networks Managed on Behalf of NRC

Networks Managed on Behalf of NRC	
Parent Network Type	**Child Network Type**
Contractor/Government Hosted Networks Specifically for NRC	Contractor/government hosted NRC networks are networks hosted by another party specifically for NRC that are not used for any other party (e.g., other government agencies or contractors).
Contractor/Vendor/Government Hosted Cloud Service	Contractor/vendor/government hosted cloud service networks provide cloud services to several different parties (e.g., multiple federal agencies).
Internet Service Providers (ISPs)	The Department of Homeland Security (DHS) maintains a list of ISPs that can provide a TIC. Under the TIC initiative, the Managed Trusted Internet Protocol Service (MTIPS) provides federal agencies with managed cyber security services. The NRC MPLS ISP (or MPLS provider) provides connectivity to the networks at NRC sites to create the NRC WAN but does not provide Internet connectivity. The TIC/MTIPS provider provides Internet connectivity. The MPLS WAN and TIC/MTIPS providers are not necessarily the same ISP.

2.5.3 External Networks

External networks are networks that interconnect with the NRC network or are used by individuals to connect to NRC networks, systems, and applications. Table 2.6-3 identifies and describes all external networks.

Table 2.6-3: External Networks

External Networks	
Parent Network Type	**Child Network Type**
Contractor, Vendor, and Service Provider Networks	Networks used for general purposes by the NRC, other organizations, and the public. These networks include: • Phone/Satellite/Data Carriers – Provide Internet connectivity for NRC cellular phones and air cards. • Vendor Networks Providing Maintenance Services – Outside vendor networks connecting to the NRC IT infrastructure for administration, support, and maintenance purposes (e.g., vendors providing Tier 3 expert support).
Other Government Networks	Federal (not NRC), state, local, or tribal networks that interconnect with NRC managed networks and other networks managed on behalf of NRC.
Telework Networks	Networks for users accessing NRC internal resources and for working remotely. These networks include: • Home Networks – Networks in users' homes used to perform teleworking. • Public Access Networks – Public networks (wired or wireless hotspots) used for the purposes of teleworking. • State Government Telework Centers – State provided centers, which provide Internet access for the purposes of teleworking. • Other Organizations' Guest Networks – Networks established by an organization to permit guests to access the Internet and are used to perform teleworking.
Academia Networks	Networks owned and/or hosted by academia.
Industry Networks	Networks owned and/or hosted by industry.

Table 2.6-3: External Networks

External Networks	
Parent Network Type	**Child Network Type**
Licensee and Licensee Contractor Networks	Networks owned and/or hosted by licensees regulated by NRC. This also includes networks owned and/or hosted by licensee contractors. Also referred to as "Licensee Networks."
Foreign Government and International Organizations' Networks	Networks owned and/or hosted by foreign governments or by companies in foreign countries.
Internet	Internet as accessed via an Internet provider and not covered in any of the other network types defined in this standard.

2.5.4 NRC Network Interconnections

NRC must have the ability to interconnect with many organizations and requires different kinds of internal and external connections to meet the business needs of the agency. Figure 2.6-1 provides a conceptual image of network interconnections. As shown in the diagram, the NRC network interconnects (e.g., using virtual private networks [VPNs]) with other federal agencies, licensees, contractors, remote users, and public networks.

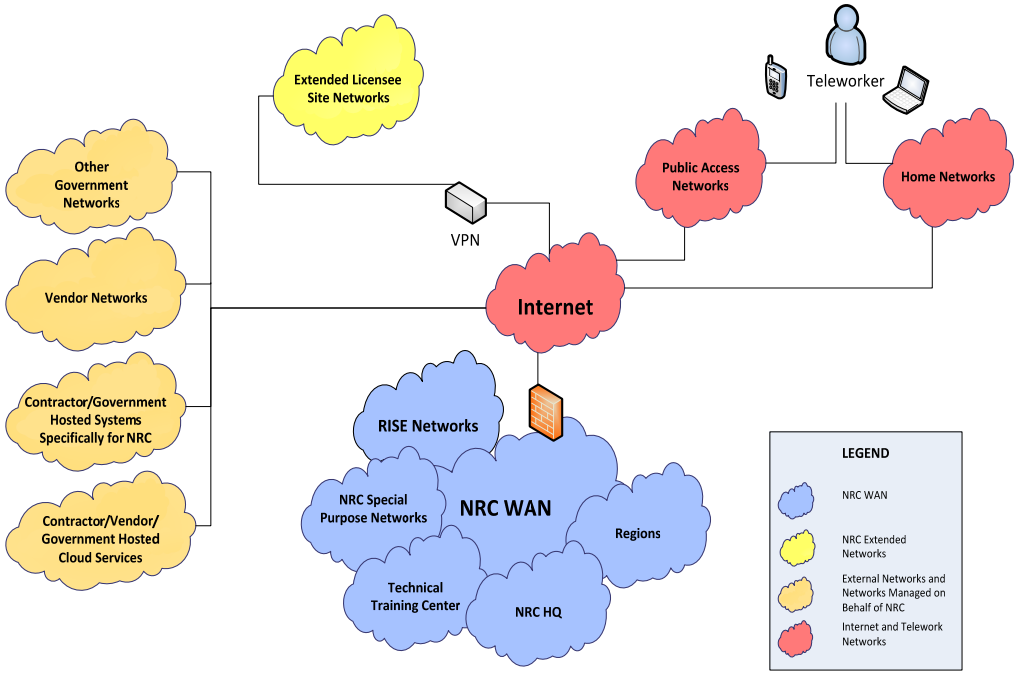


Figure 2.6-1: Conceptual NRC Network

2.5.5 NRC Network Types Summary

Table 2.6-4 compiles the NRC categories and associated parent/child network types described within Section 2.6, Network Types. The table also identifies the following networks that may be contained within each of the child network types:

- DMZ: Networks that are externally facing, typically at the perimeter of a network, and offer services to other networks or the Internet (e.g., web servers, mail servers, and DNS servers). DMZs are used to protect the internal network by separating that network from other networks.
- Intranet: A computer network used to share information, host applications, or provide network services within an organization.
- Guest: An open network provided by an organization to allow local users to connect to the Internet.

Table 2.6-4: NRC Network Type Summary

Networks (Categories & Parent/Child Network Types)		Networks Contained within Child Networks		
NRC Managed Networks		**DMZ**	**Intranet**	**Guest**
NRC WAN	*Infrastructure Networks*	X	X	X
	BA Networks	X	X	
	RISE Networks	X	X	
NRC Extended Networks	*NRCEL Networks*	X	X	
NRC Special Purpose Networks	*Management Network*	X	X	
	Standalone Office LANs	X	X	X
	Research and Development (Nuclear)	X	X	
	Research and Development (IT)	X	X	
	HPC	X	X	
Networks Managed on Behalf of NRC				
Contractor/Government Hosted Networks Specifically for NRC		X	X	X
Contractor/Vendor/Government Hosted Cloud Service		X	X	X
ISPs		X	X	X
External Networks				
Contractor, Vendor, and Service Provider Networks	*Phone/Satellite/Data Carriers*	X	X	X
	Vendor Networks Providing Maintenance Services	X	X	X
Other Government Networks		X	X	X
Telework Networks	*Home Networks*	X	X	X
	Public Access Networks	X	X	X

Table 2.6-4: NRC Network Type Summary

Networks (Categories & Parent/Child Network Types)		Networks Contained within Child Networks		
	State Government Telework Centers	X	X	X
	Other Organizations' Guest Networks	X	X	X
Academia Networks		X	X	X
Industry Networks		X	X	X
Licensee and Licensee Contractor Networks		X	X	X
Foreign Government and International Organizations' Networks		X	X	X
Internet		N/A	N/A	N/A

2.6 IT Network Environments

Within the network type hierarchies, there are different IT network environments. These IT network environments serve a specific purpose and have different security considerations. The NRC network environments include:

- IT Development Environment: This is the environment in which a system is created. Developers have significant privileges on the development systems they used to create and integrate software and hardware capabilities. The primary form of control associated with the development environment is a configuration management (CM) system that is used to control access to code and track changes to the code.
- IT Test Environment: This is the environment in which each system release is tested before being placed into an IT operational environment.
- IT Operational Environment: The working environment where day-to-day work, normal network functions, systems, and applications are used to achieve the mission. This includes pre-production zones, which can be used for assessments of system changes by independent auditors.

The IT development, test, and operational environments are all subject to NRC cyber security policy and controls. These environments are subject to different controls (e.g., in number and strength) based on the nature of the environment. The IT development environment has the least stringent security requirements because of the different needs for developing applications. The IT test environment has security requirements less stringent than the operational and test environments because of the need to perform development testing of applications and devices but should mimic the operational environment as closely as possible. The IT operational environment has the most stringent security controls. A possible scenario to illustrate the use of multiple environments is the creation of a business web application to fulfill a specific business need. After the creation of the application in the IT development environment, the application is tested within the IT test environment. Once the application is thoroughly tested, and functions as intended (including the security controls), the application is moved into the IT operational

environment. The IT operational environment is where the user performs the NRC mission and is subject to the most stringent security requirements.

2.7 Network Trust Levels

NRC requires that users and other organizations are able to remotely connect to the NRC network through a variety of network types (refer to Section 2.6, Network Types). Each of the identified network types present different considerations for interconnections in determining the overall level of trust:

- Trusted
- Semi-trusted
- Restricted

2.7.1 Trusted

Trusted networks are considered by the NRC to be the most secure because of the oversight and controls present. Networks with a trust level of "trusted" offer:

- A high level of assurance (i.e., the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the network);[1]
- A high expectation of security controls with a high degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct;
- A high strength of security functionality;
- Are hardened to meet NRC requirements; and
- Are subject to monitoring by the NRC.

2.7.2 Semi-Trusted

Semi-trusted networks are moderately secure and present an acceptable level of risk to connect to the NRC network. Networks with a trust level of "semi-trusted" offer:

- A moderate level of assurance;
- An expectation of adequate security controls, with a moderate degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct; and
- Are hardened.

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

These networks reside within or outside of the boundaries of the NRC managed networks and provide services that support NRC users.

2.7.3 Restricted

Restricted trust levels apply to networks where the NRC has:

- Minimal knowledge of the network's reputation, the security controls that the network has in place, or
- Suspicion that the network is not trustworthy.

Restricted networks present the greatest amount of uncertainty when establishing an interconnection with the NRC. There are two types of trust levels associated with the parent restricted trust level: untrusted and blacklisted.

2.7.3.1 Untrusted

Networks with a trust level of "untrusted" are networks that may not be hardened or have security controls in place. Typically, the NRC has little to no knowledge about an untrusted network's security posture. These networks may pose significant risk if they were permitted to connect to the NRC network. Untrusted networks generally:

- Have a low level of assurance;
- Reside outside the boundaries of the NRC managed network or networks managed on behalf of NRC;
- Fall outside the purview of NRC oversight;
- Have unknown security controls;
- May have a poor reputation; and
- NRC may suspect that the network is hostile or compromised.

2.7.3.2 Blacklisted

The NRC has determined that networks with a trust level of "blacklisted" represent a real and present danger to the NRC operating environment. These networks are prevented from connecting to the NRC network.

2.8 Network Segmentation

Network segmentation is the process of separating parts of the network and network traffic for performance, security, or reliability reasons. Segmenting networks also provides a degree of control and helps to meet requirements to protect sensitive information and IT assets. Networks can be physically or logically separated, depending on the specific network and security requirements, into different network segments, enclaves, network domains, subnets, and virtual LANs (VLANs). A network segment physically separates a subset of the larger network in which its boundaries are created by different network devices. NRC networks are composed of different environments and network domains with different requirements for access and

protection. Network domains are identified by the business, architectural, information sensitivity, and functional requirements, as well as by the type of network connectivity for the systems in each environment.

2.8.1 Network Segments

A network segment is a subset of the larger network in which its boundaries are created by different network devices (e.g., switches and routers). Segmenting the network environment in this manner is a way of grouping clients and systems, and can increase available bandwidth on the segment.

2.8.2 Enclaves

Within larger networks, there is a greater threat of compromise from within the networks and a greater degree of segmentation can be warranted. Networks can be further segmented into separate enclaves based on information sensitivity and specialized functions. An enclave is defined as a system connected by one or more internal networks under the control of a single authority and security policy that supports a specialized function. Enclaves typically have more stringent security and access controls and provide services to a smaller group of users that have specific roles or functions (e.g, software engineers in an engineering enclave, Human Resources [HR] personnel in an HR enclave, or an Internet Protocol version 4 [IPv4] enclave in an IPv6 network). The networks may be structured by physical proximity or by function, independent of location. A typical enclave security design includes constraints on communication between an enclave and the trusted NRC managed network, untrusted network, or a semi-trusted network as well as between network domains within the trusted managed network. Enclaves can contain several different network domains.

2.8.3 Network Domains

An NRC Network Domain (e.g., development, test, operational, training, guest, management network, DMZ) is a subset of the network composed of a group of devices, such as workstation/client and server devices. The devices included in the subset of the network are commonly centrally managed (e.g., through one central security database administered by a single authority).

The DMZ is a special purpose network but can serve a dual purpose as a network domain that provides resources to both internal and external users and does not necessarily reside on the internal network. Even though the DMZ interfaces with both internal and external networks, its main function is to provide resources to external users and add a layer of separation between the internal networks and external connections.

2.8.4 Subnets

Using subnets for logically segmenting the network environment can be an efficient way of grouping clients and systems into separate groups to share a specific network address space and broadcast domain. Subnets can be assigned based on various attributes, such as system functionality or user group. Multiple subnets can be created to logically separate different groups of devices attached to one network device, such as a switch.

Separate IP subnets can be applied to each security domain and trust zones within NRC to create logical separation and enforce routing and inspection of traffic between the different networks and server farms. Take the example of a primary network with an IPv4 address range of 123.45.0.0-123.45.255.255. In this example, the management network can be assigned to subnet number 67, which provides the IP address range of 123.45.67.0-123.45.67.255 for the subnet, and a training network can be assigned to subnet number 89, which provides the IP address range of 123.45.89.0-123.45.89.255 for the subnet. Subnet isolation can be implemented separate from or together with the use of VLANs to further segment a network.

2.8.5 VLANs

The Institute of Electrical and Electronics Engineers (IEEE) 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. A VLAN creates a logical boundary between devices, users, protocols and services to improve network functionality and security. The use of VLAN technology implements a security enforcement point in addition to physical security devices. VLAN segmentation can be used for users, devices, protocols, and services according to department, location, function, application, and both logical and physical address. This allows users and resources within the same VLAN to communicate with each other using Layer 2 switching. If there is an internal compromise, VLAN segmentation provides an additional layer of protection and makes it more difficult for a client to gain access to the information exchanged in other parts of the network.

2.8.6 Security Benefits of Segmentation

Segmenting different network types, environments, and domains from each other can assist administrators in meeting requirements for protecting sensitive information, links, and hosts.

Traffic segmentation can be used to restrict and control communication between network domains and security zones. Subnet isolation and VLANs can logically separate network traffic. This adds an additional layer of defense to the NRC network and can be used to enhance security controls, such as traffic filtering and monitoring. Figure 2.9-1, Conceptual View of Network Segmentation, demonstrates how networks can be segmented using different network devices and technology (e.g., routers and firewalls). The firewalls create separate security zones by restricting and controlling network traffic flowing from the Internet to the DMZ and the DMZ to the intranet.

Network types, trust levels, and information sensitivity (e.g., as reflected by system categorizations) are used as the basis for segmentation and communication restriction; however, the amount of communication restriction is based on network type and trust. For example, two separate trusted networks must still be segmented from each other but allowed to interconnect and share a large amount of network services (e.g., time, identity management, access, DNS) with a signed Interconnection Service Agreement (ISA). Networks and systems may segment different portions of the network or subsystems based on security categorization and information sensitivity. These networks or systems with varying impact levels that have been combined into a single network or system should have subnetworks or subsystems with the highest impact level segmented from other subnetworks or subsystems with a lower information sensitivity or impact level. Figure 2.9-2, Network Segmentation, provides an example of how network segmentation can be achieved.

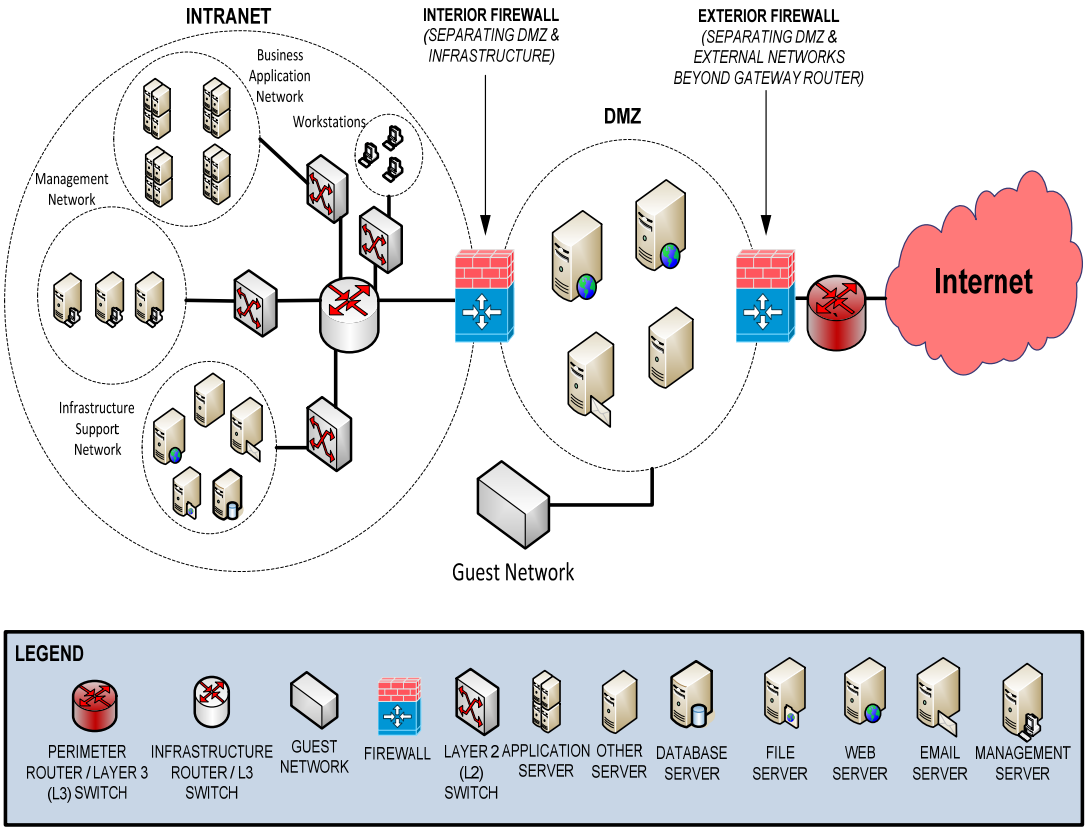


Figure 2.9-1: Conceptual View of Network Segmentation

Network segmentation can provide an opportunity to not just separate components into different network segments for the purposes of security, but can also assist with network performance. For example, segmenting management and managed networks can assist in isolating the specific traffic that is production traffic (e.g., between applications and users) and management traffic (whether for monitoring or performing administrative tasks). With that said, this can be used to isolate and prioritize traffic to ensure, for instance, that management network traffic does not degrade production traffic and thus performance of NRC applications. Figure 2.9-3, Network Segmentation of Management and Managed Networks, provides an example of a physical management LAN segment that is separated from the managed network with control of communication enforced by Layer 3 network devices, including routers and firewalls.

2.9 Network Structure

Network structure will be addressed in a future issuance of this document.

2.10 Network Devices and Technology

This section describes both security and non-security capabilities of devices as they relate to network architecture, topology, and segmentation in this standard. This section also describes core network device and technology capabilities, examples of current devices and technologies in use, and considerations for placement of network devices and technologies.

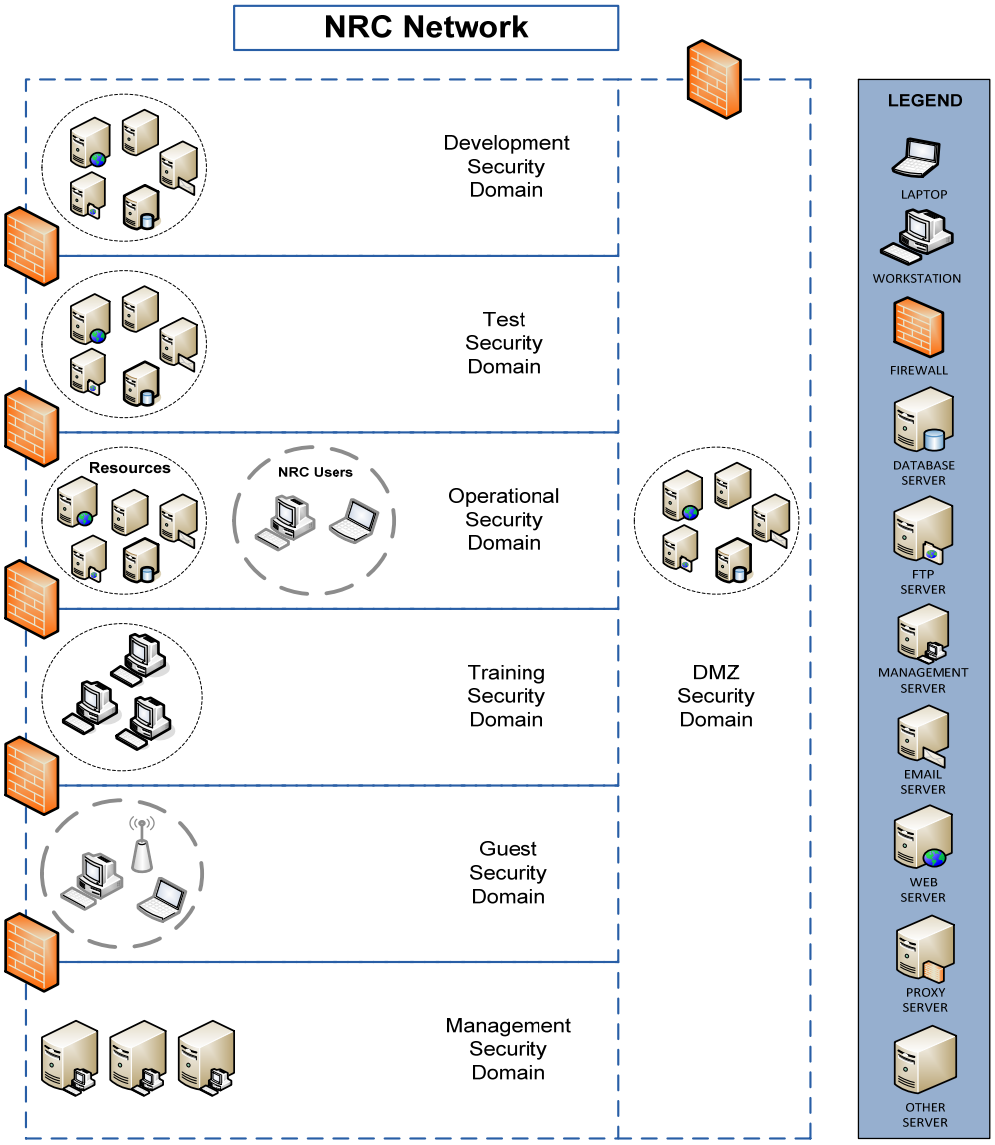


Figure 2.9-2: Network Segmentation

2.10.1 Core Network Capabilities

Through employing network devices and network technologies (e.g., software that provides networking services), networks have the capability to perform multiple functions and provide different services that facilitate network communications and security. This section identifies, groups, and describes network capabilities provided by network devices and technology. Some capabilities are introduced to provide context into how a network functions as opposed to other security capabilities that are associated with security requirements within the standard. Network security protections (NSPs), which are also referred to as security protections, are specifc types of network capabilities that relate to network security. Some NSPs are similar or related but serve different purposes in securing and facilitating network communication. The following subsections describe the core network capabilities both with regards to non-security functions and security protection.

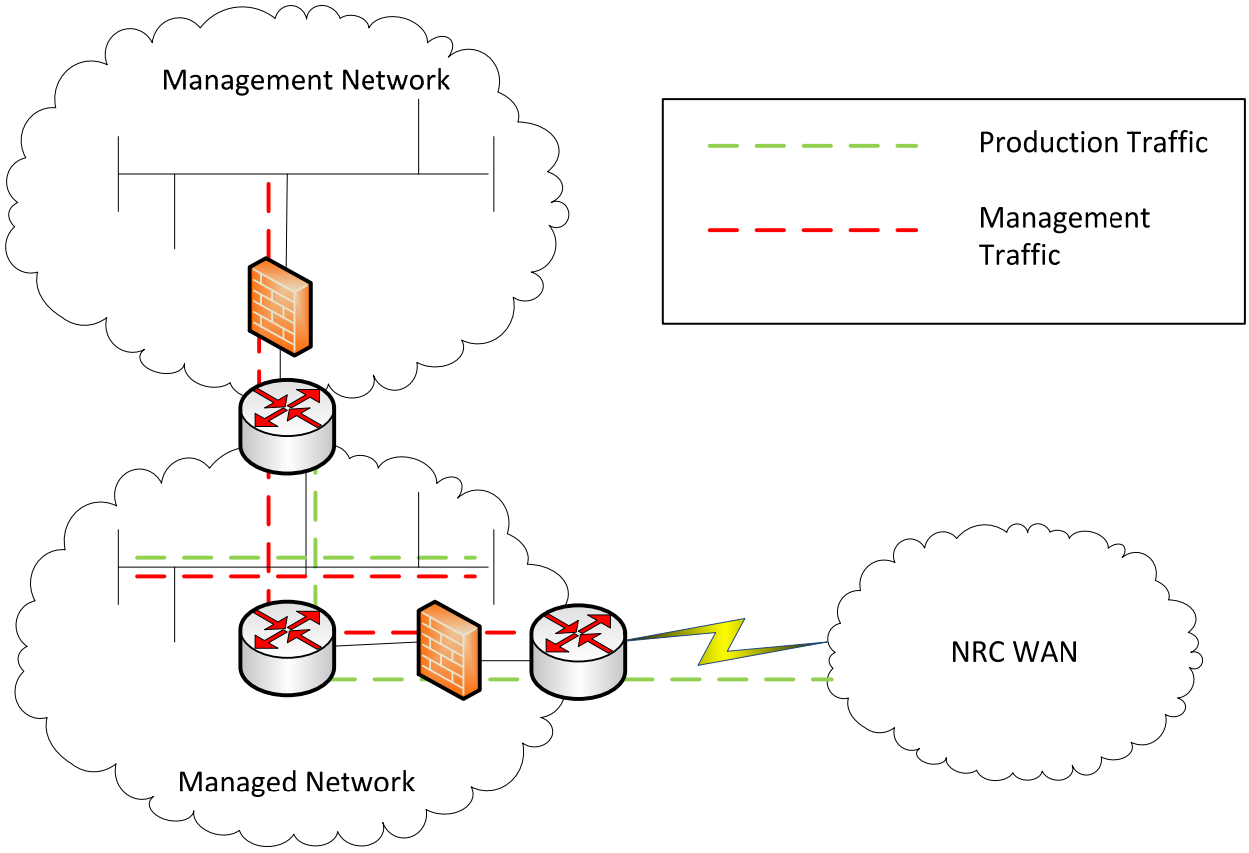


Figure 2.9-3: Network Segmentation of Management and Managed Networks

Please note that core network capabilities and NSPs are not intended to be strictly linked with just certain types of network device or technology. The core network capabilities and security protections are written to be flexible such that they can apply not only at the time that the standard is published to the existing state of network devices and technology, but also in several years time as network devices and technology continue to mature. Addressing all aspects of a specified network security protection may lead to the use of multiple network devices and technologies. Conversely, one network device or technology may address multiple specified NSPs.

2.10.1.1 Network Traffic Routing

Network traffic routing is the capability to control and direct the flow of information within the network/system and across network/system boundaries using the sources and destinations for each information flow. This allows network administrators and architects to control how information traverses the network from its source to its destination (e.g., directing traffic flow from one subnet to another subnet or one network segment to another network segment).

2.10.1.2 Data Format Translation

Data format translation is the capability of changing or translating one format of data to another (e.g., converting voice and fax calls from the public switched telephone network (PSTN) to an IP network or translating IPv4 to IPv6 so that IPv4 hosts may communicate with IPv6 hosts).

2.10.1.3 Network Boundary Protection

Network boundary protection (NBP) is the parent capability category of many different NSPs that are used to detect, prevent, and correct the flow of IP packets transiting networks based on security needs. To control the flow of traffic through network borders and monitor content by looking for attacks and evidence of compromised devices, boundary defenses can be multi-layered (e.g., several security protections used in conjunction or to augment each other).

2.10.1.3.1 Network Traffic Restriction and Network Traffic Filtering

The NSP of restricting and filtering traffic can be achieved by allowing only a portion or certain types of network communication to pass through a boundary device or to deny all communication entirely (e.g., blocking network traffic based on source, destination, and/or both). Another capability that boundary protection devices have is the capability to track the state of a connection (e.g., remembers packets that have come before or after and establishes a context). Stateful inspection tracks each connection traversing all interfaces of the boundary and ensures they are valid. A stateful inspection boundary device also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the boundary protection device.

2.10.1.3.2 Network Traffic Inspection and Monitoring

The network traffic inspection and monitoring capability covers monitoring and inspecting traffic as it traverses the network. This aides network administrators and those with network security responsibilities in identifying anomalous or unauthorized network activity and is typically based on the type of network traffic (e.g., source and destination, volume of traffic, or what protocols are used) but not an examination of the actual payload of each IP packet.

2.10.1.3.3 Network Intrusion Detection

The network intrusion detection security protection monitors for possible intrusions, malicious activity, and security policy violations. Intrusion detection systems (IDS) are passive in nature and only alert network security administrators to suspicious network activity (e.g., a device detects a policy violation and alerts a network administrator). Network intrustion detection differs from traffic monitoring because it looks for patterns within the network traffic associated with attacks or malicious behavior as network traffic passes through the sensors and is typically based on known attacks. Intrusion prevention may be extended to wireless networks and, if so, is known as a wireless intrusion detection system (WIDS).

2.10.1.3.4 Network Intrusion Prevention

The Network intrusion prevention security protection alters or changes the network environment based on possible intrusions, malicious activity, or security policy violations. Intrusion prevention systems (IPS) are active and typically do not require any network adminstrator intervention (e.g., a device that attempts to block or stop an attack by actively changing network communication, dropping/blocking communication, or modifying the network segment). Intrusion prevention may be extended to wireless networks and is known as a wireless intrusion prevention system (WIPS).

2.10.1.4 Content Inspection and Filtering

The content inspection and filtering security protection performs content inspection as network communication flows through an inspection point and may search for malware, spam, unauthorized communication (e.g., through use of data loss prevention technologies), key words, or other content level criteria of application protocols (e.g., a device that inspects web traffic for inappropriate content such as adult material or gambling). This inspection differs from network traffic inspection because it inspects actual content as opposed to individual or groups of IP packets (e.g., does not focus on IP packet source and destination addresses). Content inspection inspects the actual payload of the packet and other application protocols (e.g., deep packet inspection) but is not based on known network attacks. Content inspection supports content filtering. Once content inspection has been completed, the content may be filtered for viruses, spam, or other content level criteria.

2.10.1.5 Network Anti-Malware Protection

The network anti-malware security protection is detecting, alerting, quarantining, and cleansing viruses in data as it passes through ingress points to the network and may act as a gateway. Anti-malware protection protects against many different threats (e.g., be able to scan major protocols such as Hyper Text Transfer Protocol [HTTP], Hypertext Transport Protocol over Secure Sockets Layer [SSL] [HTTPS], Simple Mail Transfer Protocol [SMTP], and File Transfer Protocol [FTP]).

2.10.1.6 Network Encryption

This security protection covers the encryption and decryption of information as it transits network boundaries (e.g., Type 1 encryption devices used to protect classified U.S. Government information). For example, a network authorized for use with high sensitivity information may use a network encryption device to encrypt all data in transit when that information is transmitted using a network that is not authorized for use with cleartext data of that information sensitivity, such as the Internet. In this example, if the Internet is used to transport data from one network authorized for use with high sensitivity information to another (authorized to process information of the same/higher sensitivity), the receiving network would use another network encryption device to decrypt the information.

2.10.1.7 Virtual Private Networking

VPNs can extend the NRC managed network across other untrusted external networks such as the Internet. VPNs allow devices to transmit and receive data across untrusted external networks as if they were directly connected to the trusted NRC managed network while utilizing the functionality, security controls, and security policy of the trusted NRC managed network.

2.10.1.8 Network Authentication

The network authentication security protection verifies and approves a user or device access to a network and/or application system. Network authentication can allow specific users or devices to access specific networks (e.g., the management network) or enclave (e.g., the HR enclave).

2.10.1.9 Network Logging and Auditing

Network logging and auditing is the capability to log and audit network activity (e.g., a boundary protection device may record blocked connection attempts, which may be reviewed by a network administrator at a later date). Many network devices and technologies include this feature in addition to their primary capabilities (e.g., routers, intrusion detection systems [IDS], IPS, proxies, and firewalls include this logging and auditing capability).

2.10.2 Network Devices and Technologies

Network devices and technologies provide the capabilities as described in 2.11.1, Core Network Capabilities, and the necessary technology for network communications and security. Network devices and technologies include, but are not limited to, routers, switches, firewalls, various types of gateways (e.g., VPN or Voice over IP [VoIP]), IDS, and IPS. This section provides a high-level description of the various network devices, technologies,and the capabilities each provides. These capabilities include functionality, management, and security of network devices and systems. A single network device or technology may also provide several different capabilities and/or security protections. In order to facilitate the understanding of different device capabilities and security proections, this standard will reference the Open Systems Interconnection (OSI).

2.10.2.1 Open Systems Interconnection Model

The OSI model is theoretical but provides a basis for understanding how different network devices operate and communicate. The OSI model contains seven layers and includes the physical, data link, network, transport, session, presentation, and application. Each layer adds a different piece of information to the network communication and is known as network encapsulation. Figure 2.11-1 provides an example of how encapsulation occurs by demonstrating what each layer adds to the network communication.

2.10.2.2 Core Network Devices and Technologies

Table 2.11-1, Core Network Devices/Technologies, and Table 2.11-2, Network Security Devices/Technologies, describe commonly used network devices/technologies, their functions, and relates them to their core network capabilities. Please note that the list of devices and technologies within the tables is not intended to be all inclusive. The devices and technologies identified are based on commonly used network devices and technologies that are current as of the time when this standard was written. The devices/technologies listed within the tables may be able to fully satisfy or meet the objectives of the security requirements within Section 4.1.2, Network Security Protections, individually or as a group and may provide one or multiple NSPs and capabilities as described in Section 2.11.1, Core Network Capabilities.

This section also provides an overview of how some of the network devices/technologies with specific security protections and capabilities may be placed within an enterprise network. Many of the devices/technologies listed below are able to provide several different security protections and capabilities.

Table 2.11-1 lists and describes the core network device/technology types and provides images that are commonly used to represent the devices/technologies in network diagrams.

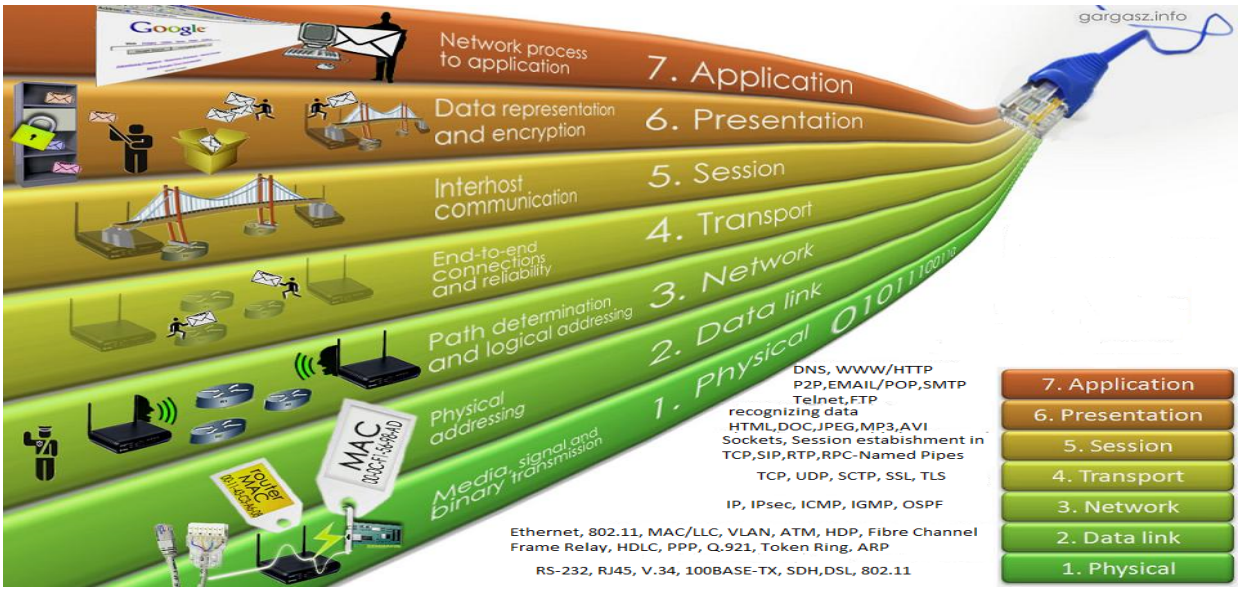


Figure 2.11-1: OSI Model[2]

Table 2.11-1: Core Network Devices/Technologies

Type	Image	Description
Application Delivery Controller (ADC)		An advanced load balancer, which often offers features including compression, cache, traffic shaping, and content switching in addition to basic server load balancing. Some offer security capabilities, including Distributed Denial of Service (DdoS) protection and application layer security.
Layer 2 (L2) Switch		A device that uses media access control (MAC) addresses from network host (computers or other network devices) network interface cards (NICs) to determine where to forward data. L2 switches use hardware application-specific integrated circuits (ASICs) as opposed to operating system software logic to create and maintain filter tables, which store MAC addresses for network hosts, and forward data. This is an example of a network device that provides network routing capabilities.

[2] Diagram from website gargasz.info.

Table 2.11-1: Core Network Devices/Technologies

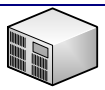
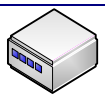
Type	Image	Description
Layer 3 (L3) Switch		A device that uses hardware ASICs as opposed to operating system software logic, which are used in routers, to forward data packets across networks. L3 switches establish connections to multiple networks. Like routers, L3 switches forwards data packets and direct traffic across the networks. L3 switches evaluate incoming packets from each network to determine the destination for the data, and then use the information in the routing table to either drop the packet or send the packet onto the next network or hop on the path. This is an example of a network device that provides network routing and boundary protection capabilities.
Private Branch Exchange (PBX)		A private branch exchange (PBX) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a limited number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.
Repeater		A device that regenerates incoming electrical, wireless, or optical signals. Ethernet or wireless data transmissions can only span a limited distance before the quality of the signal degrades. Repeaters preserve signal integrity and extend the distance over which data can safely travel. This is an example of a network device that provides network routing capabilities.
Router		A device that uses operating system logic to forwards data packets over networks. Routers establish connections to multiple networks, and evaluate incoming packets to determine the destination for the data. They then use information in the routing table to either drop the packet or send the packet onto the next network or hop on the path. This is an example of a network device that provides network routing, boundary protection, and logging and auditing capabilities.
Storage Area Network (SAN)		SANs allow storage devices (e.g., disk arrays and SAN switches), to be accessible to servers so that the storage devices appear as if they are locally attached to the operating system.
VoIP Gateway		A VoIP Gateway, which can be in the form a specialized network device or software technology on a server, that that converts voice and fax calls from a PSTN to an IP network. This is an example of a device/technology that provides data translation capabilities.
Wireless LAN Controller (WLC)		A WLC controller is used in combination with the Lightweight Access Point Protocol (LWAPP) to manage light-weight access points (APs) throughout an enterprise. This is an example of a network device that provides network routing capabilities.

Table 2.11-1: Core Network Devices/Technologies

Type	Image	Description
Wireless AP		A wireless AP is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) if it is a standalone device, or is part of a router itself. This is an example of a network device that provides network routing capabilities (when the AP is part of/performs routing services itself).

Table 2.11-2 lists and describes the network security device/technology types and images that are commonly used to represent the devices/technologies in network diagrams.

Table 2.11-2: Network Security Devices/Technologies

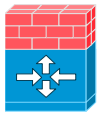
Type	Device	Description
Firewall		A device/technology with the capability to permit and/or deny network communications based upon a configured set of rules. Firewalls are used to protect networks from unauthorized access while also allowing legitimate communications and can log network traffic. This is an example of a device/technology that provides network boundary protection and logging and audit capabilities.
IDS/IPS		A device/technology with the capability to detect, log, and report unauthorized or malicious network communications. IPS also have the ability to prevent unauthorized network communication by dropping unauthorized network communications, including access attempts and network attacks. This is an example of a device/technology that provides network boundary protection and logging and audit capabilities.
Proxy Server		A server/application that “breaks” the connection between a client and a server. Specialized network devices can also be used as proxy servers as opposed to server technology used to provide this capability. The proxy can be configured to accept certain types of traffic entering or leaving a network, processes it, and forwards it. A proxy adds a layer of protection by effectively closing the direct path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Examples of proxy servers are: HTTP proxy used for web access, SMTP proxy used for e-mail, and DNS. This is an example of a device/technology that provides network boundary protection, content inspection and filtering, and logging and audit capabilities.
Encryption Appliance		A device with the capability to perform encryption and decryption of network traffic. This is an example of a device that provides network encryption capabilities.

Table 2.11-2: Network Security Devices/Technologies

Type	Device	Description
Authentication Server (AS)		A server/application used to verify and approve a user or device access to a network and/or application system. Specialized network devices can also be used as authentication servers as opposed to server technology used to provide this capability. Authentication servers can be used to authenticate user and devices on both wired and wireless networks. This is an example of a device/technology that provides network authentication capabilities.
Web Application Firewall (WAF)		A WAF is an appliance, server software, plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked. This is an example of a device/technology that provides network content inspection and filtering and boundary protection capabilities.
Data Loss Prevention (DLP)		A device used to analyze network traffic to detect data that is traversing the network that is in violation of information security policies. Servers may use DLP software by itself or to supplement network devices/appliances providing DLP capabilities. A DLP device is normally placed at the network's point of egress to help monitor and prevent the intentional or unintentional loss of sensitive data. This is an example of a device/technology that provides network content inspection and filtering capabilities.
Security Gateway		A device that augments a firewall by using customized filters for managing and filtering certain application layer "control/data" protocols. For example, security gateways can manage data by allowing client applications to use dynamic Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. For example, implementing a mail gateway in the DMZ to control SMTP traffic between the DMZ and the back-end mail server. This is an example of a device that provides data translation and network routing capabilities.
VPN Gateway		VPN Gateway is a device used to establish, manage, and terminate a virtual point-to-point connection, such as through the use of dedicated connections and encryption, and is used with network nodes or devices. This is an example of a device that provides virtual private networking capabilities.

2.10.3 Placement of Network Security Protections

This section describes examples of where and in what mode NSPs, which are provided by network devices and technologies, can be placed within various network types. Network devices and technologies, as defined within this standard can be placed between network domains, enclaves, and networks to manage/monitor network traffic, detect violations, and enforce security controls that cover both inbound and outbound connections supports the network security posture. This section also illustrates how some of the objectives for specific requirements as described in Section 4.1.2, Network Security Protections, may be met.

The perimeter of each domain can be secured with the appropriate devices to enforce network security controls which includes network device hardening, Layer 4-7 traffic filtering, logging, alerting, traffic surveillance, and, where appropriate, transport encryption.

Protecting the NRC managed network necessitates managing and monitoring the flow of traffic entering and leaving the NRC managed networks and networks managed on behalf of NRC and between network domains by employing specific security controls. Section 2.11.2, Network Devices and Technologies, introduced network devices and technologies that can be used to implement a defense-in-depth strategy to provide access control and security management of NRC's networks and systems.

The network devices and technologies provide some of the following security controls:

- Anti-Virus/Malware Protection
- Data Integrity (e.g., Transport Encryption)
- Layer 4-7 Detection and Prevention
- Layer 2-4 Traffic Filtering
- Network Authentication

Figure 2.11-2 is a conceptual representation of an implementation of a defense-in-depth strategy by leveraging and placing firewalls, routers, IDS/IPS, encryption technology, and various other security devices and software.

Network traffic flow control enforces policy that regulates where traffic is allowed to travel within the NRC managed network, between systems and what is allowed to leave the managed network. For example, enforcing traffic restrictions include, restricting web requests to the Internet that are not filtered through the internal web proxy server and limiting information transfers between logically separated networks based on content and destination.

2.10.3.1.1 Placement of Boundary Protection Devices/Technologies

Boundary protection devices such as firewalls, proxies, Intrusion Detection and Prevention System (IDPS) sensors, and web application firewalls provide effective and efficient means of protection for a network when they are placed at appropriate points within the network topology. The following subsections describe where these devices can be placed and what specific protections they can provide.

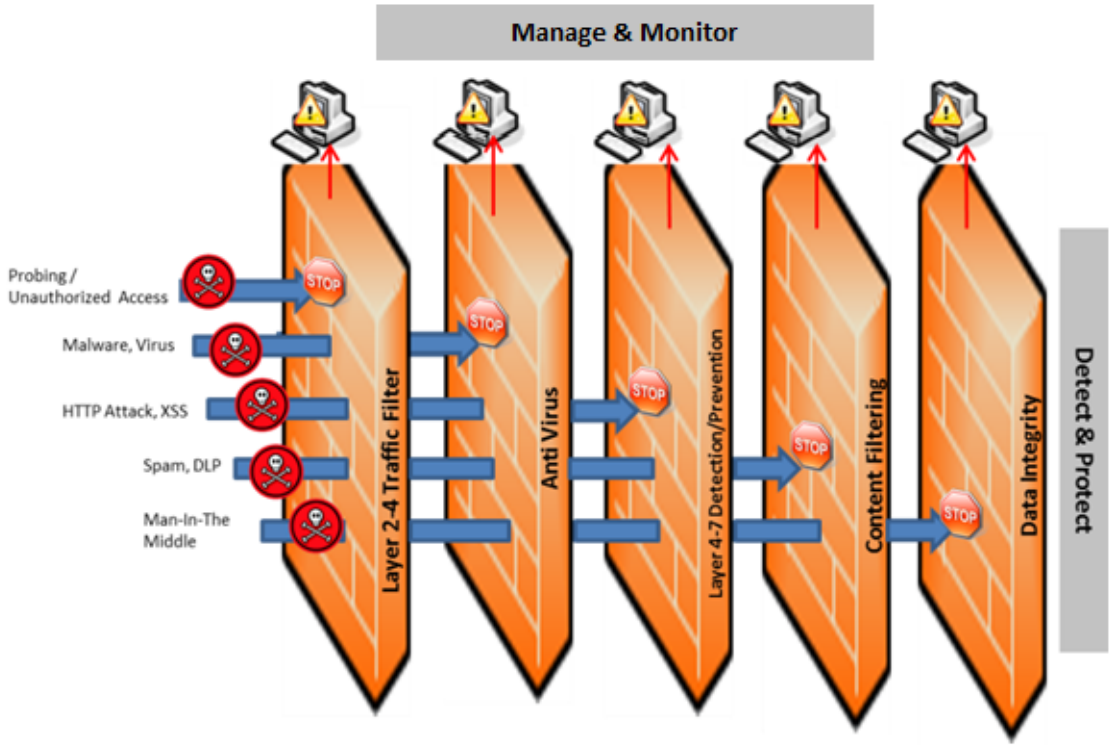


Figure 2.11-2: Defense-in-Depth

2.10.3.1.1.1 Firewall

The exterior firewall represents a stateful packet inspection firewall placed at the network perimeter, which operates at Layer 3 and up.

Firewalls are used to provide a layer of protection to the network by using custom rules to enforce NRC security policy. Firewalls vary in purpose, function, and capability. Each firewall type and implementation will vary according to the network, the network infrastructure, and the type of network traffic. Firewalls can be used to protect the boundaries of network domains and provide separation between networks.

Firewalls are typically found at the edge of logical network boundaries; meaning, firewalls may be positioned either as a node where the network splits into multiple paths, or inline along a single path.

When firewalls are used to separate networks such as a DMZ, they are typically deployed in one of the following ways:

- Single firewall (three-homed perimeter network): In a single firewall design, the firewall has three network adapters:
  - First network adapter connects to the NRC internal network.
  - Second network adapter connects to the DMZ network.
  - Third network adapter connects to the Internet.

- Dual firewall: In a dual firewall design, a firewall is located on either side of the DMZ network:
  - One firewall connects to the Internet, and
  - One firewall connects to the NRC intranet.

  This is considered to be a more secure approach. To circumvent a dual firewall design, an attacker would need to leverage flaws/misconfigurations in multiple devices (perhaps from different vendors that could complicate such efforts) to get through both firewalls in order to get to the internal network. On the other hand, an attacker would only need to take advantage of flaws/misconfigurations with one device (with no possible firewall vendor diversity) to get to the internal network.

The use of multiple layers of security is considered to be a necessary practice to provide defense-in-depth strategy for protecting network domains.

2.10.3.1.1.2 Proxy Servers

A proxy server can be configured and deployed to provide two functions:

- Act as a dedicated device with firewall capabilities providing application proxy gateway services, and/or
- Act as an intermediary between the clients and other networks to intercept traffic entering and leaving the network; virtually hiding the real network computing device and destination addresses of the network traffic.

A dedicated proxy server may be placed in conjunction with packet filter firewall devices to perform more specialized filtering and logging that otherwise is not performed on the lower layer firewall.

Dedicated proxy servers are typically positioned to filter and inspect inbound traffic destined for SMTP and HTTP servers. Inbound traffic is defined as any traffic originating from an external system requesting NRC resources to include SMTP and web application services located in the DMZ and the internal network. For example, a dedicated proxy server can be used to inspect and forward inbound World Wide Web (WWW) connections to an internal web server or inspect and filter e-mail traffic for file attachments that do not comply with NRC security policy such as attachments with .exe extensions. This also applies to NRC users connecting to NRC managed networks via remote access.

Dedicated proxy servers have the capability to manage and filter all outbound SMTP and HTTP traffic. They may be configured to allow or block outbound traffic and requests to external resources in accordance with NRC network security policy and applicable National Institute of Standards and Tecnology (NIST) guidelines. The proxy server can be placed in-line with outbound traffic directly from internal systems, filter and log the traffic, and then pass it to the upstream firewall for outbound delivery. An example would be an HTTP proxy deployed behind the firewall; users would need to connect to this proxy before connecting to external web servers.

2.10.3.1.1.3 IDPS Sensors

An IDPS sensor has the capability to inspect, detect, and prevent both IPv4 and IPv6 traffic on public facing servers. The acronym IDPS is considered to be synonymous with IPS. IDPS devices can be placed throughout the NRC managed network to inspect and filter traffic between trusted, untrusted, and semi-trusted networks.

IDPS devices can be deployed in the following locations:

- Behind all tunnel endpoints to monitor all traffic (IPv4 and IPv6) entering the NRC managed network and networks managed on behalf of NRC.
- On DMZ networks that host public servers (e.g., web, Secure File Transfer Protocol [SFTP], DNS, e-mail gateways)
- Behind VPN gateways to monitor unencrypted VPN traffic.

  Note: The use of encrypted protocols can impact the deployment of network sensors. For example, the use of VPNs encrypts network traffic making it difficult for sensors to inspect the traffic. It is important to place IDPS devices prior to VPN traffic being encrypted (for egress traffic) and after the VPN traffic is unencrypted (for ingress traffic). Otherwise, malicious traffic will likely go unnoticed in the encrypted data stream.

- In front of network domains that host sensitive services and/or critical resources (e.g., Server Farms segments containing databases, application, private backend servers, management network).
- On segments that host network and security management systems to include Out-of-Band (OOB) management links.

2.10.3.1.1.4 Web Application Firewalls

WAFs are considered to be a specialized application aware firewalls. A WAF is an advanced firewall that has the capability to inspect traffic at Layer 7, the Application Layer; protecting against web application threats, such as SQL injection, XSS, session hijacking, parameter or Uniform Resource Locator (URL) tampering, and buffer overflows.

The firewall rules on these devices are based on applications being used within the trusted NRC managed network or specific network domain; all non-required ports and services can be blocked by using the most restrictive rules possible. Inbound application firewalls can be placed in front of any application server that does not have sufficient security features to protect it from application-specific attacks and can also supplement existing application/web server protections.

A WAF can be positioned to inspect any protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data is not otherwise inspected at another point in the traffic flow.

A WAF has the capability to:

- Inspect web application input and respond appropriately based on NRC policy.

- Prevent data leakage.
- Enforce both positive (white list) and negative (black list) security models.
- Inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as HTTP and HTTPS.
- Defend against threats that target the WAF itself.
- Support Transport Layer Security (TLS) termination, or be positioned so encrypted traffic is decrypted before being inspected by the WAF.

2.11 Wireless LAN Security

Wireless LANs (WLANs) allow networks to be extended and allow a user to connect to a network without physically connecting a device. Wireless networks have many more considerations than a wired LAN. WLANs are susceptible to eavesdropping (e.g., wireless sniffers) and other forms of signal interference not found on wired LANs. A WLAN also has a dynamic topology (e.g., endpoints and access points can easily be moved based on needs or convenience). WLANs, unlike wired LANs, do not have easily determined boundaries. This section will reference and expand upon Section 2.11.2.2, Core Network Devices and Technologies, in regard to Wireless components and architecture. WLANs typically employ the IEEE 802.11 standard, which has two basic modes of operation:

- Infrastructure mode: Allows a device to connect to the network through a wireless AP (refer to Section 2.11.2.2 for more information on wireless APs).
- Ad hoc mode: Allows for wireless devices to directly communicate with each other in wireless networks. It allows the wireless devices in the network that are within range of each other to discover and communicate in peer-to-peer (P2P) fashion without involving central APs. Ad-hoc mode does not allow for centralized security management. Ad hoc networks are typically temporal in nature and usually have a limited range.

There should be adequate controls, including physical security, for the wireless architecture components listed in the sections below. Physical security measures should include locks, barriers, and proper placement of wireless devices.

2.11.1 Service Set Identifier

A Service Set Identifier (SSID) is a 1 to 32 byte string that is typically easily readable by users and usually refered to as the network name. SSIDs should be created so that they do not contain recognizable strings such as agency or department names, street, building, or other identifiable information. Some SSIDs may be hidden based on the security considerations for the WLAN. There are typically many APs within an enterprise WLAN, and the SSID is the network that all APs within the WLAN are on. Many users are familiar with how a wireless network is setup within a home or small office (e.g., one AP). Within an enterprise architecture, there is different terminology used to describe the WLAN implementation. The following sections introduce several other terms relating to the implementation of an enterprise WLAN.

2.11.1.1 Basic Service Set

A Basic Service Set (BSS) is a specific AP and its clients. A user setting a home wireless network will typically have one BSS because they have one wireless AP (e.g., a wireless router).

2.11.1.2 Basic Service Set Identifier

The BSS Identifier (BSSID) identifies the BSS and is a MAC address of the wireless AP for the BSS.

2.11.1.3 Extended Service Set

The Extended Service Set (ESS) contains a group of combined BSSes that share the same Layer 2 network and the same SSID. An ESS is a more technical way of describing a WLAN that has multiple APs. A large enterprise wireless network will typically have an ESS or multiple ESSes based on how many different wireless networks there are and the desired wireless coverage area of each network. The ESS also allows a client to roam from AP to AP.

2.11.1.4 Extended Service Set Identifier

The ESS Identifier (ESSID) identifies the ESS. Figure 2.12-1 depicts how an enterprise network with multiple APs and BSSes come together to form an ESS.

2.11.2 Wireless Components

The following components are used to create and secure a WLAN. Please note that the list of wireless components within this section may not be all inclusive. The wireless components listed are commonly used as of the time when this standard was written.

2.11.2.1 Stations

Stations (STAs) are wireless endpoint devices. Typical examples of STAs are mobile devices (e.g., laptops, tablets, and cell phones) and desktop systems with wireless Network Interface Cards (NICs).

A STA also describes the origin or destination of a message. STAs may learn about each other by sending beacon or probe requests.

2.11.2.2 Access Points

APs are wireless devices that are used to logically connect STAs to wired networks and/or other wireless STAs. An example of an AP is a wireless router.

2.11.2.3 Wireless LAN Controller

A WLC manages one or more APs by providing configuration settings and firmware upgrades. As mentioned above, an enterprise wireless network will have multiple APs and WLCs may also be used for load balancing, channel interference, and authentication.

Figure 2.12-1: BSS, ESS, BSSID, and SSID[3]

2.11.2.4 Authentication Server

An AS determines whether a user and/or STA is authorized to access network services based on the credentials provided by the user and/or STA and is used for network access control.

2.11.2.5 Wireless Bridges

A WLAN bridge is a device that allows APs to communicate and join multiple LANs.

2.11.2.6 Wireless Repeater

Wireless repeaters act as range extenders.

[3] Diagram from website Juniper.net.

2.11.2.7 Wireless Intrusion Detection Sensors

WLANs have an NSP of intrusion detection by using sensors to monitor traffic and detect attacks against WLANs similar to the function of an IDS/IPS as described in Section 2.11.1.3.3, Network Intrusion Detection (refer to Section 2.12.9, Wireless Intrusion Detection and Prevention, for more information on NSP in regards to wireless).

2.11.3 Wireless Device Authentication

Best practices for authentication include STAs authenticating to wireless networks using 802.1x and device certificates. Additionally, best practices for WLAN configurations include supporting protocols such as Extensible Authentication Protocol-TLS (EAP-TLS) or Protected Extensible Authentication Protocol (PEAP), Public Key Infrastructure and Authentication Authorization Accounting (AAA) infrastructure, and using AS as necessary. For more detailed information regarding Network Access Control (NAC), please refer to CSO-STD-2007, "Network Access Control Standard."

2.11.4 Wireless Ranges and Frequencies

Within the 802.11 wireless framework there are several different standards that have different frequencies, speeds, and ranges. These standards include 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ad. Each of these standards may be used based on needs or convenience but present different security considerations. Higher frequency bands will lower the range of the WLAN but can also increase the data rate and amount of bandwidth. Depending on how many APs are in use, a wireless network can provide a large coverage area. Table 2.12-1 depicts the different wireless standards and their respective frequency bands, bandwidth, maximum data rates, and ranges. Please note that the list of wireless standards is not all inclusive and is based on current wireless standards as of the time when this standard was written. Each range is based on a single broadcasting AP.

Table 2.12-1: Comparison of Wireless Standards

Standard	Frequency Band	Bandwidth	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	2 Mb/s	~150 feet
802.11b	2.4 GHz	20 MHz	11 Mb/s	~150 feet
802.11a	5 GHz	20 MHz	54 Mb/s	~150 feet
802.11g	2.4 GHz	20 MHz	54 Mb/s	~150 feet
802.11n	2.4 GHz	24 MHz, 40 GHz	600 Mb/s	~300 feet
802.11ac	5 GHz	20, 40, 80, 80+80, 160 MHz	6.93 Gb/s	~<100
802.11ad	60 GHz	2.16 GHz	6.76 Gb/s	~30 feet

WLANs may use a combination of these 802.11 standards, and with devices that support the standards. STAs may roam and connect to different wireless standards depending on how the WLAN is implemented (e.g., a STA may use an 802.11 ad hoc network in a conference room and walk back to their office).

2.11.5 Wireless Area Coverage

The different wireless standards have different data rates, ranges, amount of APs, and therefore do not have network borders that are clearly defined within wired LANs. The WLAN should be designed so that:

- The wireless signal only provides coverage for its intended area, and
- There is minimal signal leakage (e.g., the signal may extend 10-15 feet outside the building, but not so far that an attacker could sit in a parking lot across the street and be able to discover the network).

There are several ways of limiting the range of a WLAN (without regard to physical obstructions, such as trees or walls) that include using either different types of antennas or decreasing an antennas' transmission power (e.g., gain).

2.11.5.1 Antenna Types and Placement

APs may use different types of antennas and placement. The different types and placement of wireless antennas should be used to limit the coverage of the WLAN. These antenna types include omnidirectional, semi-directional, and highly directional. Each antenna type provides a different coverage area and may be tuned to provide the desired coverage by adjusting the gain. Increasing or decreasing the gain may provide the intended wireless coverage with minimal signal leakage and should be used in conjunction with the appropriate antenna type.

2.11.5.1.1 Omnidirectional Antennas

Omnidirectional antennas provide 360° wireless coverage and are often used in point-to-multipoint connections. These antennas broadcast in all directions and are the easiest to deploy but typically provide the least amount of customization to limit the coverage of the wireless network. Omnidirecional antennas should only be used when absolutely necessary, such as for large auditoriums or conference rooms. Semidirectional antennas using the appropriate gain will provide the same wireless area coverage but will decrease signal leakage outside the intended wireless coverage area. Figure 2.12-2 depicts an omnidirectional antenna broadcasting a wireless signal.

2.11.5.1.2 Semidirectional Antennas

Semidirectional antennas provide wireless coverage in a more limited area, sometimes referred to as sectors or patches. Semidirectional antennas may provide coverage for specific sections of a building. These antennas may be placed in corners or walls of a building so that there is minimal signal leakage. This antenna type provides the ability for wireless network architects to provide adequate wireless coverage for intended users while limiting the signal leakage. These antennas should be used in concert to create an overlapping wireless coverage area that covers the intended area but makes the WLAN difficult for unauthorized users to discover. Figure 2.12-3 depicts a semidirectional antenna placed on a wall to provide limited wireless area coverage.

Figure 2.12-2: Omnidirectional Antenna Broadcast[4]

Figure 2.12-3: Semidirection Antenna Broadcast[5]

[4] Diagram from website 4gon.co.uk.
[5] Diagram from website 4gon.co.uk.

2.11.5.1.3 Highly Directional Antennas

Highly directional antennas are typically used where broad wireless area coverage is not necessary, and the wireless network needs to be broadcast across larger distances. These antennas are used for point-to-point connections and for bridging wireless networks. A major concern for using these types of antennas are physical obstructions that would interfere with the wireless signal. Figure 2.12-4 depicts a highly directional antenna broadcasting a wireless signal to create a wireless bridge between two sites.

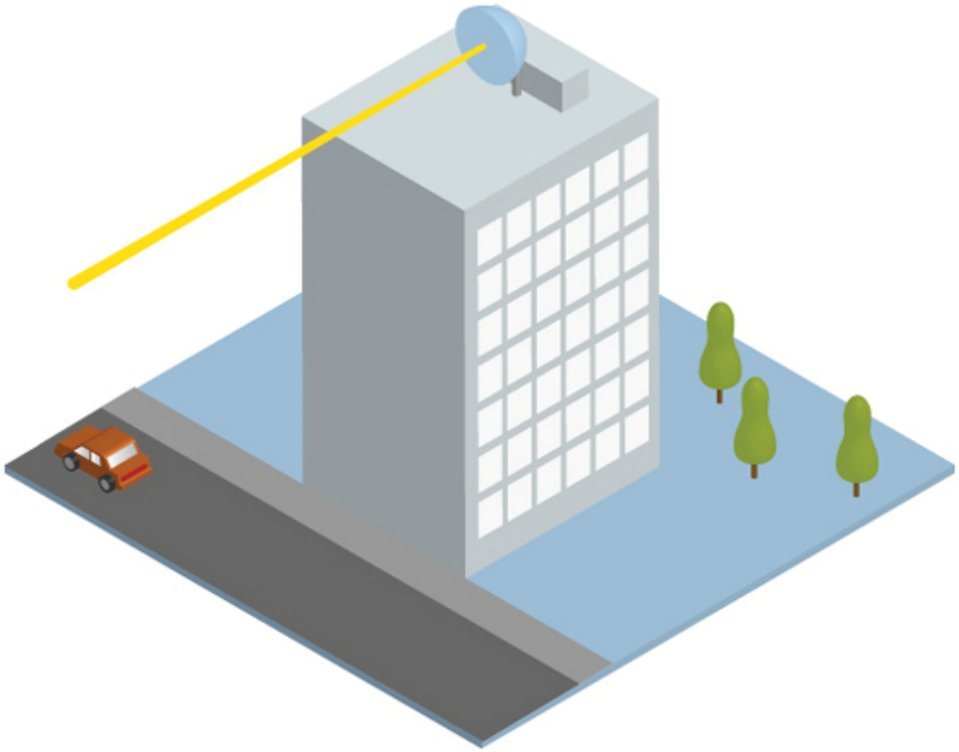


Figure 2.12-4: Highly Directional Antenna Broadcast[6]

2.11.6 Guest Wireless Networks

Guest wireless networks may provide Internet access to guests and non-NRC personnel in addition to NRC users without requiring authentication. Guest wireless networks, however, should use some form of registration and method of collecting information on the devices that are connecting to the guest wireless network. Captive web portals are an effective means of accomplishing this task. Captive portals may use a login page or route users to a page that requires them to accept the terms of service before granting Internet access. This Internet access should be granted for a specified amount of time. Guest wireless networks should not

[6] Diagram from website 4gon.co.uk.

allow direct communication between users and may use encryption so that network traffic cannot be intercepted by other users. Guest wireless networks should also be segregated from the trusted NRC managed network, which can be accomplished by creating a separate guest wireless VLAN.

2.11.7 Overlapping WLANs

There may be several WLANs present in the same coverage area (e.g., guest wireless and NRC WLAN). WLANs may overlap with each other as long as they do not operate on the same or overlapping channels. For example, there are 14 channels within the 2.4 GHz frequency band. If the two WLANs are on the same channel or neighboring channels, they may interfere with each other and reduce the availability of that WLAN. The neighboring WLANs should employ both encryption and authentication so that users do not associate or access the neighboring WLAN.

2.11.8 Rogue Devices

While a WLAN offers users the freedom to connect to the trusted NRC managed network, it can also be exploited by attackers. Users and STAs will typically associate with the wireless network or AP that has the greatest signal strength. Users may choose to manually connect to a wireless network with a SSID that appears familiar or has the strongest signals. Attackers can place a fake AP to launch a man-in-the-middle attack and potentially steal login credentials.

“Evil twins” are rogue APs that broadcast the same or similar SSID as an authorized AP to trick users into connecting to the rogue AP. The rogue AP can also use this connection for man-in-the-middle attacks.

STAs may associate with rogue access points if the signal-to-noise ratio (SNR) is high with the AP that the host typically associates with, and if the rogue AP has a stronger signal. Attackers can flood channels with illegitimate traffic so that the SNR is sufficiently high enough to cause the host to search for a new wireless AP (e.g., the rogue AP).

The proper use of 802.1x also makes it extremely difficult for rogue APs to connect to the trusted NRC managed network. The use of wireless intrusion detection and prevention is an effective means for detecting and stopping the use of rogue devices.

2.11.9 Wireless Intrusion Detection and Prevention

The wireless intrusion detection systems, WIDS and WIPS, differ from wired IDS in that they can specifically analyze 802.11 protocols and should have a signature database with specific wireless attack signatures with an alert console. These signatures will differ from the wired IDS and will focus on known wireless attacks. The WIDS/WIPS also monitor or actively search for the presence of rogue APs, rogue STAs, spoofed STAs, and STA ad hoc connections.

2.11.10 Other WLAN Security Controls for Standalone WLANs

There are a few less commonly used security controls that apply to standalone wireless networks (e.g., standalone wireless office LANs) and include using MAC address filtering and protocol filtering. These security controls are used at times in standalone networks or closed

systems where other more formal authentication methods (e.g., 802.1x and device certificates) are not possible. The MAC addresses can easily be captured by sniffing wireless traffic and the use of them for authentication is not considered secure.

2.11.11 Other Wireless Network Types

There are several different types of “wireless” networks that are used within enterprises that are not based on the 802.11 standard. For the purpose of this standard, these networks are not considered WLANs. The following sections describe other wireless technologies (e.g., IEEE 802.15 and IEEE 802.16) that are not subject to the same requirements as 802.11 WLANs and will not be addressed within this standard. Figure 2.12-5 depicts how the different wireless technologies compare to each other in power and overall range.

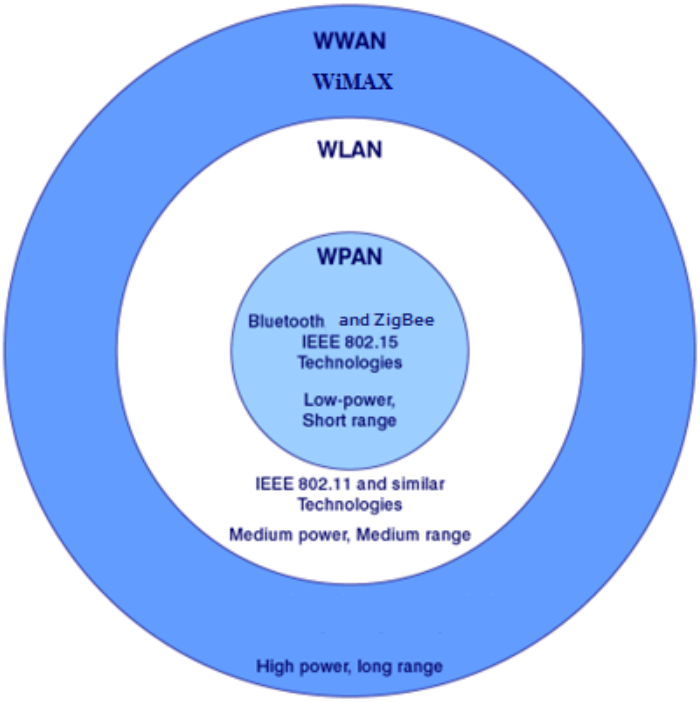


Figure 2.12-5: Wireless Technologies

2.11.11.1 Line-of-Sight Wireless Networks

Traditional 802.11 wireless networks were intended to be used indoors because of the range and other factors that may interfere with the wireless network. A wireless network can be extended to other buildings via a line-of-sight (LOS) wireless connection. Two semidirectional or highly directional wireless antennas are mounted on top of the buildings and broadcast to each other. The use of this network requires a clear line of sight so that the signal will not be obstructed from reaching the other antenna.

2.11.11.2 Wireless Wide Area Networks and Metropolitan Area Networks

Wireless Wide Area Network (WWAN) or Wireless Metropolitan Area Network (WMAN) is a wireless networking technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links (bridge) to portable and fully mobile WMAN subscriber (client) access to Internet services.

WMAN systems are designed for medium range and are primarily used as wireless bridges to connect two sites or buildings.

2.11.11.2.1 WiMAX

Worldwide Interoperability for Microwave Access (WiMAX) (IEEE 802.16) is similar to a WLAN but can accommodate many more users over a much greater range than a typical WLAN. For example, a WLAN could provide network services and Internet access for a single building while a WiMAX wireless network could provide network services and Internet access for an entire city.

2.11.11.3 Wireless Personal Area Networks

Wireless Personal Area Networks (WPAN)s are used to transmit information over a small distance to a limited number of users in an ad hoc manner.

2.11.11.3.1 Bluetooth

Bluetooth devices connect and communicate wirelessly in ad hoc networks called piconets and are typically used with human interface devices (e.g., mice, keyboards, and headsets).

2.11.11.3.2 ZigBee

ZigBee is a low-cost, low-power, low rate wireless networking technology. ZigBee is typically used for device-to-device communications as opposed to Bluetooth, which is used frequently for human interface devices.

2.12 Network Resources

Network resources (i.e., network ports, protocols, and services [NPPS]) will be addressed in a future issuance of this document.

2.13 Interconnections

An interconnection is a connection between one network's node and another separate network's node for the purpose of network communication. Each network provides the NRC resources for various users, vendors, and affiliates (e.g., contractors, other private organizations, or interested parties) by allowing interconnections through direct connection or network gateways. These interconnections include:

- Connectivity of general laptops to the various network types.

- Non-NRC devices that connect with the NRC infrastructure or another network's infrastructure (e.g., has access to network resources or services such as FTP).
- Devices that access public interfaces, publicly available information, and the Internet (e.g., general laptop accessing a public web site or application).
- NRC systems or networks that connect with other NRC systems or networks for the purpose of sharing services or information.

The key considerations for an interconnection are:

- Network/System Information and Data Sensitivity Level
- Level and Method of the Interconnection
- Services Offered
- Information Exchange Security

Each of these considerations is described in detail in Section 2.15.2, Key Considerations for an Interconnection.

2.13.1 Types of Interconnections

This section describes the different types of interconnections at the NRC but does not describe the permissibility of the interconnection.

2.13.1.1 NRC Network-to-NRC Network

NRC Network-to-NRC Network (N2N) interconnections are any NRC managed networks or networks managed on behalf of NRC that connect for the purpose of sharing data or services. These can include interconnections between two different network types (e.g., NRC-DMZ and NRC intranet). Generally, these are interconnections between two trusted NRC managed networks.

2.13.1.2 Telework-to-NRC Network

Telework-to-NRC Network (T2N) interconnections are telework networks (e.g., home networks, public access networks, state telework centers, and other organizations' guest networks) that interconnect with NRC networks/systems for the purposes of accessing NRC network resources (e.g., an NRC employee that connects from a semi-trusted home network to the NRC). NRC laptops may also be used for remote access to another NRC network or system.

2.13.1.3 NRC Device-to-Telework Network

NRC Device-to-Telework Network (D2T) interconnections are mobile devices (e.g., NRC laptops, smart phones, and tablets) that interconnect to a telework network for the purpose of accessing the Internet (e.g., an NRC laptop interconnects to a home network). Generally, these are interconnections between an NRC device and an untrusted network.

2.13.1.4 Government-to-Government

Government-to-Government (G2G) interconnections are local, state, tribal, and other federal agency networks that interconnect with NRC networks/systems for the purpose of providing services and/or sharing data with NRC networks/systems (e.g., another Federal network interconnecting with the NRC or government entities acting as users to applications on NRC networks). Generally, these are interconnections between a trusted NRC managed network and a network managed on behalf of NRC semi-trusted network or external semi-trusted government network.

2.13.1.5 Non-Government/Private Organizations/Business-to-Government

Non-Government/Private Organizations/Business-to-Government (B2G) interconnections are commercial and private entities that connect with NRC networks/systems for the purpose of providing services and/or sharing data with NRC networks/systems (e.g., a private organization's network connecting to the NRC or non-government entities acting as users to applications on NRC networks). These B2G interconnections also include private academia networks (e.g., a private university). Generally, these are interconnections between a trusted NRC managed network and an external untrusted network.

2.13.1.6 Licensee-to-Government

Licensee-to-Government (L2G) interconnections are connections between the NRC and specific licensee sites for the purposes of sharing emergency data (e.g., a power plant connecting with the NRC to provide emergency data) or a general laptop connecting to a licensee site (e.g., for an emergency response exercise). Generally, these are interconnections between a trusted NRC managed network and an external untrusted network.

It is permissible to use Licensee network technologies when conducting day-to-day duties and during emergencies given the following mandatory conditions:

- NRC staff shall use only NRC issued hardware and software or personally owned hardware and software that use an NRC Designated Approving Authority (DAA) authorized access solution (e.g., NRC Citrix, Licensee Citrix, Bring Your Own Device [BYOD]) to access the Licensee network technologies.
- NRC issued hardware and software meet NRC requirements for configuration control, security scans, and patches.
- NRC staff shall report the loss or perceived misappropriation of NRC hardware or software immediately to cs_irt@nrc.gov

The following activities are expressly forbidden:

- NRC staff under no circumstance may receive or use Licensee furnished IT hardware or software for individual use. Licensee workstations designated for walkup access by NRC staff may be used for NRC authorized and official purposes only.
- NRC staff under no circumstances are allowed to use personally owned information technology hardware or software to connect to Licensee network technologies unless

using an NRC DAA authorized access solution (e.g., NRC Citrix, Licensee Citrix, Bring Your Own Device [BYOD]) to access the Licensee network technologies.

- NRC access to Licensee network technologies are for NRC authorized and official purposes only. Personal use of Licensee network technologies is prohibited.
- NRC staff are forbidden from requesting or receiving additional access privileges or technical support on Licensee networks other than those typically provided by the Licensee to the NRC.

2.13.1.7 Citizen-to-Government

Citizen-to-Government (C2G) interconnections are the general user population not associated with a government or commercial entity (e.g., authenticated or unauthenticated) and does not provide network services for NRC systems (e.g., an interested citizen or party that connects to the NRC). These are interconnections between an external untrusted network and a trusted NRC managed network.

2.13.1.8 International Entities/Organizations-to-Government

International Entities/Organizations-to-Government (I2G) interconnections are international governments or organizations that connect with the NRC for the purpose of sharing data or services (e.g., the International Atomic Energy Association connecting to the NRC). Generally these are interconnections between a trusted NRC managed network and an external untrusted network.

2.13.2 Key Considerations for an Interconnection

Establishing an interconnection can introduce new risks and possible vulnerabilities to the NRC; therefore, there are several key considerations that must be understood prior to establishing an interconnection. These key considerations address the information that is necessary to better understand the possible impacts caused by the interconnection both from a business standpoint and for possible risks and vulnerabilities. Table 2.15-1 describes these key considerations for an interconnection.

Table 2.15-1: Key Considerations for an Interconnection

Key Consideration for Interconnection	Description
Network/System Information and Data Sensitivity Level	Each network/system, including network type, network trust level, network/system purpose, and overall network/system data sensitivity level.
Level and Method of the Interconnection	Level of interconnectivity that is established between the IT networks or systems, ranging from limited connectivity (limited data exchange) to enterprise-level connectivity (active sharing of data and applications), and defines the direction of information flows (e.g., one or two-way data flows). Method of interconnection should also be specified (e.g., VPN or leased lines).

Table 2.15-1: Key Considerations for an Interconnection

Key Consideration for Interconnection	Description
Services Offered	Specific services offered by each network/system. Examples of services include e-mail, FTP, Remote Authentication Dial-In User Service (RADIUS), Kerberos, database query, file query, and general computational services.
Information Exchange Security	Specific security controls implemented for the interconnection (e.g., method of protection, including required cryptographic module validation, certificates, and algorithms).
Topological Diagram of the Interconnection	Topological diagram illustrating the interconnectivity from one system to another system (end-point to end-point). Diagram should include all communication paths, circuits and other components used for the interconnection and should identify the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).

2.13.3 Interconnection Security Agreement and Memorandum of Understanding / Agreement

The Interconnection Security Agreement (ISA) is a companion document to a Memorandum of Understanding or Agreement (MOU/A) used to document and formalize the arrangements made between organizations for connecting networks or systems and to specify any details that may be required to provide overall security controls for the interconnection. The key considerations of an interconnection as described in Section 2.15.2, Key Considerations for an Interconnection, provide the basis for the information documented in the ISA:

- Information sensitivity
- Level of interconnection
- Method of interconnection
- Information flows
- Specific services provided

The MOU/A defines the responsibilities of both parties in establishing, operating, and securing the interconnection. The general purpose of an MOU includes:

- Addressing mutual areas of responsibility;
- Providing interface guidelines;
- Providing more effectively coordinated inspections,
- Addressing oversight and enforcement matters; and
- Avoiding duplication when agency areas of responsibility are not clearly defined.

The goal of an MOU is to optimize utilization of agency resources and to prevent overlap while allowing agencies to carry out their respective responsibilities.

3 GENERAL REQUIREMENTS

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

This standard provides a set of overarching requirements that must be used in concert with:

- CSO-STD-2105, “Remote Access Security Standard.” This standard provides the authorized remote access methods to access NRC resources and systems.
- CSO-STD-1004, “Laptop Security Standard.” This standard provides users with guidance in following security requirements for laptops.
- CSO-STD-2108, “Endpoint Protection Security Standard.” This standard provides the minimum security settings required for endpoint protection technologies on all NRC systems.
- CSO-STD-0020, “Organization Defined Values for System Security and Privacy Controls.” This standard defines the required NRC values for specific computer security controls identified in federal computer security control standards and guidance.

Computer security standards can be found at http://www.internal.nrc.gov/CSO/standards.html.

3.1 Cryptography

All cryptography used must comply with CSO-STD-2009.

3.2 Information Sensitivity

General requirements apply to SGI and classified information. Section 3.2.1, SGI, and Section 3.2.2, Classified, provide requirements for SGI and classified information. Expanded requirements associated with information sensitivity will be incorporated into a future issuance of this standard.

3.2.1 SGI

The following requirements apply to SGI:

NI-SGI-G1 Plaintext SGI is not permitted to traverse a public or SUNSI network.

NI-SGI-G2 Plaintext SGI must be processed by a physically separate network that has no connectivity with SUNSI networks.

NI-SGI-G3 Encrypted SGI is permitted to traverse SUNSI and public networks[7].

3.2.2 Classified

The following requirements apply to classified information:

NI-C-G1 Plaintext classified information is not permitted to traverse a public, SUNSI, SGI, or lower classification level network.

NI-C-G2 Plaintext classified information must be processed by a physically separate network that has no connectivity with lower level networks.

NI-C-G3 Encrypted classified information is permitted to traverse lower level networks using very specific requirements provided by the National Security Agency (NSA) or in the case of sensitive compartmented information (SCI), by the Director of National Intelligence.

Classified information must be protected in accordance with all applicable NSA and Committee for National Security Systems (CNSS) requirements.

3.3 Network Monitoring

Network monitoring will be addressed in a future issuance of this document.

3.4 Network Ports, Protocols, and Services

All network protocols utilized by the network infrastructure must comply with CSO-STD-2008, "Network Ports, Protocols, and Services Standard."

3.5 Network Access Control

Network access control (NAC) must comply with CSO-STD-2007.

3.6 Network Types and Trust Levels

Each of the network types present different considerations in determining the overall level of trust.

NI-NTTL-G1 All applicable network types must be identified for each network.

NI-NTTL-G2 Each network must be assigned a trust level based on the network's associated type(s) and specific attributes.

[7]See Management Directive (MD) 12.5, "NRC Cyber Security Program" and NUREG/BR-0168, Revision 4 Policy for Processing Unclassified Safeguards Information on NRC Computers for further information on processing sensitive information.

3.7 Interconnections

The following requirements must be addressed regarding network interconnections:

NI-I-G1 The network types and trust levels, as defined in Section 2.6, Network Types, and Section 2.8, Network Trust Levels, must be applied to networks that interconnect with the NRC.

NI-I-G2 It must be determined whether a DAA signed ISA is required for each interconnection (see Section 4.1.8.4, Interconnections Requiring a DAA Signed ISA).

NI-I-G3 Use of Licensee network technologies when conducting day-to-day duties and during emergencies must follow the mandatory conditions specified in Section 2.15.1.6, Licensee-to-Government.

NI-I-G4 Appendix C, NRC Network Interconnection Diagrams, and Appendix D, Interconnection Matrices, provide point-to-point representations of interconnections that are and are not permitted based upon the network types associated with the interconnecting networks. The information concerning permitted and not permitted interconnections specified in these appendices must be applied to all NRC interconnections.

3.8 Network Segmentation

The NRC managed networks and networks managed on behalf of NRC must have the following segmentation:

NI-NTS-G1 Each child network must be segmented from another child network regardless of child network type and trust level.

NI-NTS-G2 Network domains must be segmented from each other (i.e., development, test, operational, training, guest, management, DMZ, and HPC).

NI-NTS-G3 Communication between domains must be controlled. Details on the specific requirements and controls are provided in Section 4.1.1, Network Segmentation.

NI-NTS-G4 The use of multiple layers of security must be used to provide defense-in-depth strategy for protecting networks, enclaves, and domains.

NI-NTS-G5 Systems with different categorization levels (e.g., low, moderate, or high) must be segmented from each other. Details on the specific requirements and controls are provided in Section 4.1.1, Network Segmentation.

NI-NTS-G6 All network traffic from the NRC intranet destined for the Internet must be routed through a boundary protection device.

3.9 Network Security Protections

In Section 2.11.1, Core Network Capabilities, the NSPs and core network capabilites are introduced. This section provides general requirements associated with those capabilities and NSPs. One or many devices/technologies can be used in conjunction to satisfy the requirements as discussed within this section. For a list of specific network devices and technologies, and NSPs that each provides, please refer to Section 2.11.2.2, Core Network Devices and Technologies.

NRC managed networks and networks managed on behalf of NRC, through the use of network devices and technologies, must meet the following NSP requirements:

NI-NSP-G1 Boundary protection devices must be able to inspect, restrict, and filter both inbound and outbound traffic between networks, enclaves, network domains, Subnets, and VLANs.

NI-NSP-G2 Network devices used to segment networks, enclaves, and domains should be from different vendors (e.g., in a dual firewall design in which the perimeter firewall that connects to an untrusted external network should be from a different vendor from the interior firewall that connects to the DMZ).

3.10 Wireless LAN Security

Wireless LANs that store, process, or transmit information up to, and including, the SUNSI level have the following requirements:

NI-WLS-G1 WLANs must use network ports, protocols, and services in accordance with CSO-STD-2008 (e.g., EAP-TLS or PEAP when used for authentication and key distribution services).

NI-WLS-G2 WLANs must use authentication methods in accordance with CSO-STD-2007 (e.g., wireless devices must use certificate-based PKI authentication to connect to trusted NRC managed WLANs).

NI-WLS-G3 WLANs used to transmit, store, or process non-public/non-sensitive information or higher (e.g., SUNSI and SGI) must use encryption.

NI-WLS-G4 Cryptographic algorithms used for securing the communication between an endpoint and an AP or between APs must be in accordance with CSO-STD-2009 (e.g., the cryptographic requirements that apply when WiFi Protected Access 2 [WPA2] is used).

NI-WLS-G5 All other standards for wireless security listed on the Computer Security Standards web page, http://www.internal.nrc.gov/CSO/standards.html, must apply.

3.11 Transitioning to IPv6

Federal agencies must transition to and support IPv6 in accordance with the Office of Management and Budget (OMB) IPv6 Memorandum M-05-02, "Transition Planning for Internet Protocol Version 6 (IPv6)" and a follow-up OMB memorandum titled "Transition to IPv6" issued on September 28, 2010.[8]

4 SPECIFIC REQUIREMENTS

This section provides specific requirements for NRC managed networks.

4.1 SUNSI and Below

This section provides requirements for processing information up to, and including, the SUNSI level.

4.1.1 Network Segmentation

There are a wide variety of NRC networks within the overall NRC infrastructure, with NRC managed networks and networks managed on behalf of NRC providing the broad network types that these networks fall under. NRC networks also perform a variety of functions including guest networks that provide visitors access to the Internet at NRC facilities, management networks supporting management and monitoring of NRC networks, and development and test networks that may not be authorized to house production data. Section 2.6, Network Types, provides more information on the network types referenced above. Section 2.9, Network Segmentation, provides a more in-depth explanation and examples of network segmentation, both conceptually and how network segmentation can be implemented.

The number, varied roles, and complexity of these networks within the NRC would put the NRC at significant risk if the networks were laid out in a flat network architecture, with all networks being able to communicate openly with other networks. To mitigate that risk, this section provides requirements to segment NRC networks to restrict network communication and access between different networks and network components.

4.1.1.1 NRC Endpoints

Networks providing connectivity to NRC user endpoints (e.g., laptops, desktops, virtual desktops) are at risk of compromise due to many attacks that target NRC users, including phishing, drive-by-download, and social engineering attacks. Due to this risk, segmentation of networks providing connectivity to NRC user endpoints may reduce the risk of a compromise spreading from the initial compromised user endpoint, such as a laptop, to backend servers. The following requirement applies:

[8] OMB Memorandum, "Transition to IPv6," September 28, 2010 - http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf

NI-NS-S1 Networks providing connectivity to NRC user endpoints must be segmented from other NRC networks, such as those for applications and key business services including voice and video.

Supplemental Information: Network segments (e.g., specific subnets and VLANs) that provide connectivity to NRC user endpoints can employ a default deny approach and restrict communications outside of the segments to the Internet (e.g., through proxy servers) and internally to authorized applications and key business services (e.g., voice and video for unified communications software) based on the specific NPPS used.

4.1.1.2 Dedicated Voice and Video

Dedicated voice (e.g., Voice over IP [VoIP] phones) and video (e.g., video teleconferencing [VTC]) devices and services within enterprise networks commonly pose challenges to organizations. This is due to the sensitivity of their network communication to latency as well as the complexity of the hardware and software used, which can delay or sometimes eliminate the possibility of patching devices (e.g., backend VoIP infrastructure) against known threats to the underlying software used. Segmenting the networks used for dedicated voice and video services can provide a greater ability to prioritize traffic over other communications that may be less susceptible to being degraded due to lower latency and can reduce the risk of compromise. The following requirement applies:

NI-NS-S2 Networks providing connectivity to dedicated voice and video devices and services (e.g., VoIP phones, VTC equipment) must be segmented from other networks.

Supplemental Information: This only applies to dedicated voice devices, which may be referred to as endpoint instruments and include VoIP phones, and VTC equipment, which can include separate physical VTC codecs with their own cameras, microphones, and screens commonly used in conference and training rooms. This does not apply to unified communication technology that is solely employed through software, such as Microsoft Lync.

4.1.1.3 Guest Networks

Guest networks at NRC facilities provide limited access to individuals at NRC facilities in order to assist those individuals with doing business with the NRC. The guest networks are available to visiting NRC personnel, foreign assignees, licensees, and other visitors that are given access to the Internet. To protect the agency and to manage the risks associated with permitting visitor's access to this type of NRC special purpose network, the following specific requirements apply:

NI-NS-S3 Guest networks must be segmented and isolated with no access (ingress/egress) to any network other than the Internet. Access to the Internet can be provided directly or indirectly through perimeter security devices, such as a proxy server.

Supplemental Information: To secure the guest networks from other internal networks a VLAN can be used to segment guest networks from other networks. This also excludes connectivity between different guest networks (e.g., since a

guest network within an NRC headquarters facility can only access the Internet, it would not be permitted to communicate with any other guest networks, such as those in NRC ROs).

NI-NS-S4 Wired and wireless guest networks must be segmented from each other.

Supplemental Information: Consider an NRC site, such as a RO, that provides guest network connectivity using either wired or wireless connections. The endpoints residing on wired and wireless guest networks would be considered to be on separate guest networks. Thus, the wired and wireless guest networks would not be permitted to communicate with one another. That said, the wired and wireless guest networks would be permitted to access the Internet using the same proxy server.

NI-NS-S5 Within each guest network, each endpoint device (e.g., smartphone, tablet, laptop) must be isolated from one another where technically feasible.

Supplemental Information: For example, wireless client isolation is a common feature available in both consumer and enterprise wireless network equipment that can be enabled to prevent direct communication between endpoint devices connected to the same wireless network.

4.1.1.4 Management Networks

A management network is a segmented special purpose network that hosts for the purpose of monitoring, collecting event log information, and to provide command and control capabilities for the operation, administration, maintenance, and provisioning of managed networks. Management networks may host:

- Console servers;
- Network management stations;
- AAA servers;
- Network Time Protocol (NTP) servers;
- Syslog servers;
- Log correlation and analysis tools;
- Network compliance management; and
- Other management and control services.

Management networks can be in-band, with management communication flowing over the same routers and switches as production traffic (e.g., between users and applications), or OOB, with management communication occurring over different, dedicated networking equipment that is not used for production traffic.

The use of in-band and OOB management networks are not mutually exclusive, meaning that it is possible to employ just one or both types of management networks. When in-band management is the primarily managed approach used, OOB management networks are

suggested for use as a back-up. An OOB management network can provide access to network devices (e.g., routers, switches) through serial console connections. This approach is frequently used to provide network/security operations personnel access even if there is no in-band production network connectivity to a device.

The following sections provide requirements that apply to in-band and OOB management networks.

4.1.1.4.1 In-Band Management Networks

In-band management networks are used when management traffic takes the same data path as production (non-management) traffic on managed networks. Production traffic refers to communication over the IT operational network environment between users and NRC applications for normal day-to-day user activities (e.g., use of e-mail). More information on the IT operational network environment is provided in Section 2.7, IT Network Environments.

Both management and production traffic use the same physical network. Thus, network management traffic is intermixed with user traffic.

The following requirement applies to in-band management networks:

NI-NS-S6 In-band management networks must be segmented from managed networks. Access to in-band management networks must be restricted to only authorized users and devices (e.g., to those located within the NRC Network Operations Center [NOC] or Security Operations Center [SOC]).

Supplemental Information: In-band management networks are commonly logically separated from managed networks, such as through the use of a dedicated VLAN for management traffic. Figure 2.9-3, Network Segmentation of Management and Managed Networks, provides an example of how an in-band management network can be segmented from a managed network.

4.1.1.4.2 Out-of-Band Management Networks

OOB management networks are used when management traffic takes a different data path compared with production (non-management) traffic on managed networks. Management and production traffic use different physical networks. Thus, network management traffic is logically and physically separated from user traffic.

Common examples of OOB management technology include, but are not restricted to:

- Console servers
- Keyboard Video Mouse (KVM) over IP
- Power Distribution Units (PDUs), which can be networked
- Intelligent Platform Management Interface (IPMI) built-in and add on functionality (e.g., for servers)

OOB management networks are sometimes referred to as “overlay management networks.” Collectively, OOB management technology uses dedicated communication channels (e.g., a separate network that is physically separated). Some OOB management technology, such as IPMI, does not rely on whether the device being managed (e.g., network switch, router, server) is powered on or if the operating system is functional. Examples of IPMI technology include Hewlett-Packard (HP) Integrated Lights Out (iLO) and integrated Dell Remote Access Card (iDRAC).

The following is a list of specific requirements that apply to OOB management networks:

NI-NS-S7 OOB management networks must be physically segmented from other NRC networks.

Supplemental Information: OOB management networks are in a separate band from the data or voice stream, or on an entirely separate, dedicated channel. OOB management networks are implemented using dedicated switches that are independent of the managed network(s). Access to in-band management networks must be restricted to only authorized users and devices (e.g., to those located within the NRC NOC or SOC).

NI-NS-S8 OOB management traffic must not traverse over the same data path as production (non-management) traffic. OOB management traffic must use different network interfaces than what is used for production traffic to avoid OOB management traffic intermixing with user traffic.

Supplemental Information: Network devices (e.g., routers, switches, firewalls, IDPS, and other network devices) connect to the OOB management network through dedicated management interfaces.

NI-NS-S9 The network devices (e.g., routers, switches) used within the OOB management network should be from a different networking vendor compared to the network devices used in the managed production network.

Supplemental Information: Using products from a different networking vendor reduces the likelihood that a critical flaw in the network operating system used in the network devices in the managed production network can affect the management network.

If the managed production network has been compromised or is affected by a major operational issue due to a critical flaw in the network operating system used, it is likely that the management network may also be affected. Resolving issues with managed networks is significantly more difficult if the management network is also affected.

4.1.1.5 IT Development, Test, and Operational Networks

NRC management networks and networks managed on behalf of the NRC may include IT development, test, and operational (e.g., production) network environments. Within the NRC managed network, the IT operational environment provides access to BA networks,and other infrastructure services including e-mail, calendar, contacts, file sharing, and collaboration

applications (e.g., Microsoft SharePoint). IT development network environments are used to construct applications and hardware and software configurations for future deployment. Prior to production, newly developed applications and configurations are deployed to test networks that may have slightly less stringent security requirements due to the need to expedite testing of new or enhanced applications and devices for functionality and performance.

Permitting open, unrestricted communication between these different network environments would very likely expose the NRC to unacceptable risk. Network segmentation of these different network environments is needed to isolate and restrict communications between the environments. Of the three IT network environments, the IT operational network environment is the most trusted and the IT development network environment is the least trusted. More information on the IT operational network environment is provided in Section 2.7, IT Network Environments.

The following is a list of specific requirements that applies to the IT development, test, and operational network environments:

NI-NS-S10 The IT development, test, and operational network environments within NRC managed networks and networks managed on behalf of NRC must be segmented from one another.

Supplemental Information: One important reason to segment these networks is to prevent data spills (e.g., unauthorized transfer of production data from the operational environment to a development environment). Physical or logical segmentation can be used. Firewalls can be used to define separate zones for IT development, test, and operational environments. A mix of physical and logical segmentation can also be employed if desired, such as the logical separation of IT test and operational environments coupled with the physical separation of the IT development environment.

NI-NS-S11 IT development network environments must be isolated from IT operational (production) network environments. No network communication is permitted between IT operational and development network environments.

Supplemental Information: IT development network environments are not typically secured to the same level as IT operational network environments. Due to this disparity in the presumed security levels of each environment, isolating the IT development network environment is an important step to take to reduce the likelihood of compromise of the IT operational network environment.

NI-NS-S12 Network connections may only be established from a more trusted IT network environment to a less trusted IT network environment (not vice versa).

Supplemental Information: Communication between the IT operational network environment and the IT test environment must be initiated by a system within the IT operational environment. In the same manner, communication between the IT test environment and the IT development environment must be initiated by a system within the IT operational environment.

4.1.1.6 Training Networks

Training networks are networks supporting the training needs of NRC personnel, contractors, licensees, and designated visitors at NRC. Security requirements are necessary to prevent the possibility of unauthorized access to the training network and other NRC managed network resources (e.g., to prevent visitors to the NRC that only authorized to access network resources on a training network from accessing resources on other networks).

The security requirements that apply to a training network depend on the training being performed for the specific training network (e.g., for a specific training room). The ISSO for systems that include training networks is responsible for ensuring that the applicable requirements specified in this section are implemented for each specific training class that is presented.

Different types of training may involve significantly different security considerations and corresponding security requirements. Factors that influence the required security requirements include the information that will be presented, stored, or processed on the training network during the training; the software and tools that will be used during training classes; whether access to other NRC or external networks is needed; and who is attending and presenting the training.

Training networks do not necessarily have to be set up and secured in the same manner permanently. Consider the following example of one training network (e.g., for a specific training room), which could be used for a variety of different types of training over a year that could result in requiring differing network segmentation requirements.

- One part of the year (e.g., for one or multiple weeks), the training network could be used by NRC personnel and contractors to learn how to use an application hosted within an internal NRC network. Thus, for this to occur, the training network could not be physically segmented without access to other NRC networks. The training network would need access to resources on the internal NRC network for the specified application.
- Another portion of the year, the training network might be used for training, such as for network penetration testing or malware analysis training, where there is significant risk that such activities could adversely affect other NRC networks if the training network was not fully isolated. In this case, physically segmenting the network would provide significant protections to reduce the likelihood of the training activity adversely affecting other network activities (e.g., for production communication on IT operational network environments within NRC managed networks).

One example of a method that an ISSO of a system with training networks can employ to assist in complying with the requirements stated is to use a questionnaire or checklist to obtain information about future training courses to determine the applicable security requirements. Such a questionnaire or checklist may request information including, but not restricted to:

- Whether the course requires Internet access or internal network access (e.g., to an internal NRC application, such as ADAMS).
- If the training involves the use of tools or software that present a risk to other networks, such as malware, vulnerability assessment, or penetration testing tools.

- The highest sensitivity of information will be involved in the class.
- Whether the training is conducted by a third-party as opposed to a cleared NRC resource.

This section presents the minimum requirements for network segmentation for training networks. Training networks may be segmented to a greater degree than is specified by the requirements within this section if desired (e.g., for a training class including lab activities examining or testing simulated network security protections employed at nuclear power plants).

The following is a list of specific requirements identified to segment the training networks:

NI-NS-S13 Training networks must be segmented from other networks. Training networks must also be segmented and isolated from other training networks based upon the sensitivity of information processed on the training network and if training (e.g., network penetration testing, malware analysis) includes the use of cybersecurity assessment, exploitation tools, or involves malicious software.

Supplemental Information: Since these networks are used for a variety of training courses; such as penetration testing that involves network discovery, it is essential to isolate the traffic from the NRC managed networks and other network resources. This segmentation (and in the case of a course for penetration testing, isolation) could be accomplished logically, such as through the modification of access control lists (ACLs), or physically to prevent any ingress or egress communication from the training network and any other network.

NI-NS-S14 Non-NRC network devices, such as a laptop used by an instructor that is a contractor, must either have network communications restricted to just the training network for the specific training that is underway (e.g., if the training must employ the use of non-NRC laptops for the instructor and learners), which would fully isolate the training network for the class, or be provided access to the NRC guest network (e.g., if only Internet access is necessary).

NI-NS-S15 Training networks may be provided access to external networks (e.g., the Internet) or to NRC managed networks as needed for training.

NI-NS-S16 Training networks may be used to support other purposes aside from training if authorized by the NRC DAA.

Supplemental Information: For example, the NRC Professional Development Center (PDC) includes training networks and may not always have all training networks in use at all times. The NRC Headquarters Operations Center (HOC), which is used to support the Office of Nuclear Security and Incident Response (NSIR), is located in the Three White Flint North (3WFN) building, the same building as the NRC PDC. If the NRC DAA provided authorization to do so, one or more training networks in the NRC PDC could be used to support NRC HOC activities if needed for incident response or operational activities (e.g., for extra capacity or perhaps if there was an issue with the HOC).

NI-NS-S17 Training networks must be controlled and segmented based upon the sensitivity of information used in the training. Only users and devices authorized to access the information may be connected.

4.1.1.7 Network Printers, Scanners, and Multi-Function Devices

Network printers, scanners, and multi-function devices contain onboard memory, processors, and storage devices. Network multi-function devices are devices that provide a combination of printing, scanning, copying, and/or fax functions and are available to endpoints (e.g., laptops, desktops) over NRC networks.

Network printers, scanners, and multi-function devices (MFDs) commonly run scaled down, yet powerful operating systems and firmware that if compromised may assist attackers with performing network reconnaissance and launching attacks against other computers. Due to this, network segmentation of network printers, scanners, and MFDs permits the restriction of communication traffic between these devices and authorized endpoints (e.g., laptops, desktops) to only those NPPS that are known to be associated with the primary function of the devices. Thus, if network segmentation is employed and NPPS are restricted, then that may reduce the likelihood of a successful attack against the device and the compromised device then being used to scan or attack other NRC networks.

The following requirement applies to network printers, scanners, and multi-function devices:

NI-NS-S18 Network printers, scanners, and MFDs connected to the NRC managed networks or external networks managed on behalf of NRC must be placed on networks that are logically segmented from other networks. Access to networks with network printers, scanners, and MFDs must be restricted solely to NPPS associated with the printing, scanning, copying, faxing, and other functions of the devices.

NI-NS-S19 Access to networks with network printers, scanners, and multi-function devices must be restricted solely to NPPS associated with the printing, scanning, copying, faxing, and other functions of the devices.

4.1.1.8 DMZ Segmentation by Applications and Application Tiers

DMZ networks may provide access to remote NRC users, authorized parties (e.g., of other government organizations), and members of the public to a variety of hosted applications. Since DMZ networks are accessible externally, there is a potential that applications and components within DMZ networks may be compromised. Network segmentation within DMZ networks can reduce the likelihood that the compromise of one component or application hosted in the DMZ will lead to the compromise of another component or application within the DMZ. This is a significant risk especially with a flat DMZ where many/all devices associated with multiple applications can have open communication.

The following requirements apply to network segmentation by applications and application tiers within DMZ networks:

NI-NS-S20 DMZ networks must be segmented based on the applications hosted within the DMZ.

Supplemental Information: For example, if a DMZ network hosts three applications, then each application must be segmented from each other.

NI-NS-S21 Within each application network segment in a DMZ, each application tier (e.g., application, database, web) must also be segmented if technically possible. Communication between network segments associated with each application tier must be restricted to only necessary NPPS.

4.1.2 Network Security Protections

In Section 2.11.1, Core Network Capabilities, the NSPs and core network capabilities are introduced. This section provides specific requirements associated with those capabilities and NSPs. One or many devices/technologies can be used in conjunction to satisfy the requirements as stated within this section. This section also includes several requirements that apply to specific NSPs and the objectives the NSP (through the network devices and technologies used) must be able to achieve in a specific situation. For a list of specific network devices and technologies, and the NSPs that each device provides, please refer to Section 2.11.2.2, Core Network Devices and Technologies.

4.1.2.1 Network Boundary Protection

NBP is a category of NSPs and has several NSPs that fall within it. The following specific NSP requirements, which can be met through use of network devices and technology, apply for detecting, preventing, or correcting network traffic as it transits the perimeter of networks, enclaves, and network domains.

4.1.2.1.1 Network Traffic Restriction

The following specific NBP requirements apply to network traffic restriction.

NI-NSP-S1 NBP devices/technologies that perform traffic restriction and filtering devices must, at minimum, be placed at the perimeter of the network (e.g., ingress and egress points within the network).

NI-NSP-S2 NBP devices/technologies that restrict and filter network traffic must be placed at the boundaries of different functional network domains (e.g., provide segmentation between development, test, operational domains).

NI-NSP-S3 NBP devices/technologies that have the capability to restrict and filter traffic should be placed in front of network domains that host critical services and/or resources (e.g., network segments containing databases, application, private backend servers, management network).

NI-NSP-S4 NBP devices/technologies that have the capability to restrict and filter traffic must be placed between networks and systems that have different levels of data sensitivity.

Supplemental Information: Network encryption devices can also be placed at the perimeter of the network with the higher data sensitivity so that the information is

encrypted once it exits the network and only encrypted information transits over a network of a lower sensitivity level. The placement of NBP devices/technologies in this scenario must occur before the information is encrypted. Another NBP sensor may be used after the data has been encrypted to ensure that no unencrypted sensitive data transits over the network with a lower data sensitivity level.

NI-NSP-S5 System owners must ensure systems prevent public access into NRC managed networks except where managed interfaces and NBP devices/technologies are used to permit specific system owner and DAA-approved access.

NI-NSP-S6 Servers located within the boundaries of the trusted NRC managed network that request services from an untrusted or semi-trusted network must pass through an NBP device/technology that monitors, restricts, and logs network traffic.

Supplemental Information: Application gateways should be used to augment the NBP device/technology (e.g., used in conjunction with a firewall). Application gateways can shield the identity (e.g., network address) of a client when sending requests through the gateway and allow specific types of communication (e.g., file sharing, database, and mail protocols) to be inspected.

4.1.2.1.2 Network Intrusion Detection and Prevention

The following specific network intrusion detection and prevention requirements to detect possible intrusions, malicious activity, security policy violations, and alter the network environment apply.

NI-NSP-S7 NBP devices/technologies that detect possible intrusions, malicious activity, security policy violations, or alter the network environment must, at a minimum, be placed at the perimeter of the network (e.g., ingress and egress points within the network).

NI-NSP-S8 Network traffic from interconnections originating from an untrusted or semi-trusted network transiting into the trusted NRC managed network must pass through an NBP device/technology that detects possible intrusions, malicious activity, and security policy violations (e.g., an IDPS sensor).

Supplemental Information: The network traffic should be decrypted so that the NBP devices/technologies can detect possible malicious activity. If the network traffic cannot be decrypted, the NBP devices/technologies (e.g., IDPS or network anti-malware protection) are less likely to detect attacks and malware within the network traffic.

NI-NSP-S9 NBP devices/technologies that detect possible intrusions, malicious activity, and security policy violations (e.g., IDPS sensors) must be placed behind VPN gateways to monitor decrypted VPN traffic.

NI-NSP-S10 NBP devices/technologies that detect possible intrusions, malicious activity, and security policy violations to include unauthorized or transmission of information of a higher sensitivity than is authorized on the network must be placed at the

perimeter of enclaves that contain information categorized as having a high confidentiality or integrity information sensitivity.

Supplement Information: NBP devices/technologies that detect possible intrusions, malicious activity, and security policy violations should be placed in front of network domains that host sensitive services and/or critical resources (e.g., Server Farms segments containing databases, application, private backend servers, management network).

NI-NSP-S11 NBP devices/technologies that detect possible intrusions, malicious activity, and security policy violations must inspect, modify, or block both IPv4 and IPv6 traffic.

Supplemental Information: With the transition to IPv6, instances of networks employing dual stack transition methods will become more common (e.g., network traffic will use both IPv4 and IPv6 address schemes simultaneously). In order to provide the appropriate protection, NBP devices/technologies must be able to inspect, modify, and block both types of network traffic.

NI-NSP-S12 Network traffic originating from external (may be untrusted or semi-trusted) networks to trusted NRC managed networks must pass through an NBP device/technology (e.g., an IDPS sensor) that can alter or change the network environment or session (e.g, terminate network communication, modify or drop IP packets) once an attack has been detected.

Supplemental Information: For example, licensee networks transmit emergency response information to the trusted NRC managed network. This network traffic must be inspected so that malware or unauthorized commands are not transmitted to/executed on the trusted NRC managed network or this interconnection is not used as a point of attack on the NRC managed network.

4.1.2.1.3 Content Inspection and Filtering

The following specific requirements for content inspection and filtering of network communication as it flows through inspection points on a network apply.

NI-NSP-S13 NBP devices/technologies that have the capability to perform content inspection and filtering must, at minimum, be placed at the perimeter of networks (e.g., ingress and egress points of the network).

Supplemental Information: Content inspection and filtering is most commonly done in modern networks through a proxy server which can either be an actual hardware device or software installed on a server. Proxy servers are placed within the DMZ so that there is not a direct connection from devices in the intranet, such as user workstations, to an external network while also providing the opportunity to inspect, modify, and block specific network communications.

NI-NSP-S14 Networks with externally facing servers (e.g., web, SFTP, DNS, and e-mail servers), which provide services to external networks, must have network traffic pass through an NBP device/technology that can inspect, modify, drop, and block application content/requests.

Supplemental Information: In many instances, a WAF should be placed in front of the web server. The WAF adds an extra layer of security and can prevent the web application and web server from being attacked. This can complement the use of proxy servers, which can be used (for example with reverse proxies) to inspect traffic from web servers to application or database servers.

NI-NSP-S15 Application protocol requests (e.g., HTTP or HTTPS) originating from untrusted or semi-trusted networks (e.g., the Internet) must pass through an NBP device/technology that performs application specific content inspection.

Supplemental Information: Web requests originating from the Internet should use a reverse proxy server to pass the request on from the web server to the destination web application server.

NI-NSP-S16 NBP devices/technologies that perform content inspection and filtering of web application specific content must be placed in front of externally facing web servers and must inspect web application input from untrusted networks, such as the Internet and modify, drop, or block malicious requests.

NI-NSP-S17 NBP devices/technologies that perform content inspection and filtering of externally facing web applications specific content must also filter web application threats, such as SQL injection, XSS, session hijacking, parameter or URL tampering, and buffer overflows.

Supplemental Information: For example, a WAF may be used to inspect traffic for an externally facing web application, such as Electronic Information Exchange (EIE) that permits authorized and authenticated users to provide input for electronic submittals, before that user input or application transactions are passed to the destination web, application, or database server. For critical internal web applications, WAFs should be used to protect internal web servers and may also be used to protect associated application and database servers.

NI-NSP-S18 Web traffic for NRC user network endpoints connected to NRC managed networks must pass through an NBP device/technology that performs content inspection and filtering of application content to inspect, modify, and drop network communication, such as for communication with blacklisted and malicious web sites. This may include user laptops, desktops, mobile devices, or virtual desktops through Virtual Desktop Infrastructure [VDI] connected to NRC managed networks.

Supplemental Information: All NRC network endpoints that allow NRC users to browse the Web, not just those connected to NRC managed networks, should have web traffic pass have through an NBP device/technology that performs content inspection and filtering of application content to inspect, modify, and drop network communication. To hide network addresses of NRC devices, an NBP device/technology (e.g., a forwarding proxy server) should be used to forward requests onto external untrusted or semi-trusted networks.

4.1.2.1.4 Network Anti-Malware Protection

The following specific network anti-malware protection requirements to detect, alert, quarantine, and cleanse malware in data as it passes through ingress points to the network apply.

NI-NSP-S19 Network anti-malware devices/technologies must detect, alert, quarantine, and cleanse viruses in data as it passes through ingress points to the network.

Supplemental Information: Anti-malware protection should be able to protect against many different threats (e.g., be able to scan major protocols such as HTTP, HTTPS, SMTP, and FTP).

NI-NSP-S20 Network anti-malware devices/technologies, such as mail gateways, must examine mail protocol (e.g., SMTP) traffic and filter out blacklisted addresses and malicious e-mail attachments.

Supplemental Information: Network anti-malware protection and mail (e.g., SMTP) gateway filtering may be accomplished using the same network device/technology. This allows the mail gateway to effectively scan e-mail attachments for malware and take the appropriate action (e.g., strip the attachment from the e-mail, possibly blacklist the sender or domain associated with the sender).

4.1.3 Wireless LAN Security

The following specific requirements must be placed on WLANs that are managed by NRC or managed on behalf of NRC.

NI-WLS-S1 A WLAN coverage area must be reasonably sized and constrained to the areas intended for WLAN signals (e.g., wireless signals must not extend far past their intended coverage area).

Supplemental Information: Depending on the frequency and gain of the antenna, wireless signals can extend far outside the area that they are intended to provide service for. For example, a site WLAN must not have a signal that is strong enough for a user to connect to that WLAN from a parking lot across the street from the site.

NI-WLS-S2 All wireless networks (including associated peripheral devices) must be approved by the approval authority prior to connection and use for processing NRC information.

NI-WLS-S3 Each WLAN must identify and authenticate authorized devices and have the ability to determine and enforce any restrictions placed on that device.

NI-WLS-S4 Wireless APs and bridges must, at a minimum, be logically segmented from the wired portion of the network by placing them in dedicated subnets or dedicated VLANs.

NI-WLS-S5 Wireless APs and bridges must be logically or physically segmented from the wired infrastructure networks (e.g., placing APs or controllers in a screened subnet or DMZ separating intranet and wireless network).

NI-WLS-S6 Workstations (e.g., desktops and general laptops) or mobile devices (e.g., smartphones and tablets) must not be used as APs or to create wireless network bridges.

NI-WLS-S7 Any unauthorized wireless device or peripheral connected by users to the trusted managed NRC network must be considered rogue devices (e.g., a user trying to set up a WLAN using a wireless router brought from home).

NI-WLS-S8 Personal hotspots (e.g., smartphone hotspots and personal hotspot devices provided by phone carriers) must not use SSIDs similar or identical to NRC SSIDs, or they will be considered rogue devices.

NI-WLS-S9 WLANs must be logically separated from wired LANs (e.g., through the use of VLANs). Network communication between WLANs and wired LANs must be controlled to only permit authorized traffic, such as through permitting communications between specific devices associated with explicitly identified network ports, protocols, and services. This could be through the use of a gateway (e.g., a network firewall) with stateful or proxy firewall capabilities to control and inspect traffic.

Supplemental Information: A WLAN and a wired LAN can be logically separated through being assigned to different network zones of a firewall. In this scenario, network communication between the two network zones could be controlled to only permit traffic that has been specifically authorized (e.g., firewall rules that explicitly identify allow communication between zones for identified network devices and network ports, protocols, and services employed).

NI-WLS-S10 WLAN SSIDs must be changed from the manufacturer's default to a SSID that does not include any reference to NRC.

Supplemental Information: The WLAN should not include any reference that the AP is an NRC asset, location, or have any other indication that it is associated with the NRC except in the case of wireless guest networks.

NI-WLS-S11 WIDS sensor(s) must be installed and placed to monitor all wireless network transmissions for possible attacks and unauthorized traffic.

NI-WLS-S12 NRC WLANs must be able to detect unauthorized devices and must deny that device access to the network.

NI-WLS-S13 Guest wireless networks must be segmented from all other networks (e.g., the trusted NRC managed network and semitrusted networks managed on behalf of NRC).

NI-WLS-S14 WLANs and APs must be run in infrastructure mode, not in ad hoc mode. Any device connected to WLAN must not be run in ad hoc mode.

NI-WLS-S15 Wireless management devices such as AS, APs, WIDS/WIPS, and WLCs must be placed in a wireless management network (e.g., separate VLAN or subnet).

NI-WLS-S16 Wireless communication must be encrypted in accordance with CSO-STD-2009, "Cryptographic Control Standard."

4.1.4 Network Monitoring

Network monitoring will be addressed in a future issuance of this document.

4.1.5 Physical Network Security

Physical network security will be addressed in a future issuance of this document.

4.1.6 Interconnections

Specific requirements apply to interconnections. This section includes several requirements that apply to specific interconnections relating to authentication, encryption, and documentation. Due to the large variation and differences between individual interconnections, further specific requirements and restrictions will vary based on the actual interconnection itself and will need to be developed, proposed, documented within the ISA, and signed off on subject to Section 4.1.8.4, Interconnections Requiring a DAA Signed ISA prior to the interconnection being established. The only exception are interconnections identified in Section 4.1.8.3, Interconnections Not Requiring a DAA Signed ISA.

4.1.6.1 Interconnection Data Sensitivity and Information Exchange Security

Interconnections that access or process non-public or more sensitive information will require authentication and/or encryption in accordance with applicable computer security standards:

NI-I-S1 Interconnections that access non-public data must use authentication.

NI-I-S2 Interconnections that process or exchange information that is SUNSI or more sensitive must use authentication and encryption in accordance with applicable computer security standards. Interconnections between two networks or systems not authorized to process the same information sensitivity level must ensure that the information from the network with the higher sensitivity level is always encrypted as it transits through the network with the lower sensitivity level.

Supplemental Information: Consider the example of one network ("Network A"), which processes SUNSI, that interconnects with another network ("Network B"), which is only authorized to process public or non-public information, to use Network B's network connectivity to gain access to other networks that are authorized to process SUNSI (e.g., communication between different NRC facilities and sites). SUNSI transmitted or received by Network A using Network B's network connectivity must always be encrypted as it transits Network B. Since SUNSI is always encrypted, it is considered Plaintext SUNSI per Section 2.1, Requirement Definitions and Identifiers.

4.1.6.2 Interconnections Transiting over External Networks

The following requirement applies to interconnections that transit over external networks, such as the Internet:

NI-I-S3 Interconnections transiting over an external network, such as the Internet, must:

- Originate from a DMZ
- Terminate in a DMZ

Supplemental Information: Requiring all interconnections that transit over an external network to originate from and terminate in a DMZ provides the ability for perimeter network security protections to inspect, provide alerts on, and drop malicious or unauthorized network traffic. Otherwise, there is potential risk that an interconnection transiting over an external network that connects directly with an NRC internal network may not have network traffic monitored and malicious or unauthorized traffic blocked.

4.1.6.3 Interconnections Not Requiring a DAA Signed ISA

Only a few interconnections do not require an ISA. This is due to the characteristics of these interconnections that may make having an ISA infeasible or unnecessary. The full list of interconnections that do not require an ISA are identified in the requirement below.

NI-I-S4 The only interconnections that do not require an ISA are:

- Interconnections to telework networks and government and commercial guest networks, if they are used for the sole purpose of accessing the Internet.
- Interconnections to public interfaces (e.g., a website hosting an application) and accessing publicly available information (e.g., a public website). This includes interconnections between NRC networks and the Internet.
- Interconnections to non-public interfaces originating from an authorized private citizen or party (e.g., C2G interconnection where the citizen obtains a credential for authenticated access).
- Interconnections between two NRC systems with the same system owner.

4.1.6.4 Interconnections Requiring a DAA Signed ISA

The overwhelming majority of interconnections, whether they involve internal NRC networks or external networks associated with other organizations, do require a DAA signed ISA in accordance with the requirement below.

NI-I-S5 All interconnections, other than those specified in Section 4.1.8.3, Interconnections Not Requiring a DAA Signed ISA, require a DAA signed ISA. This includes, but is not restricted to:

- Interconnections that access another network types' infrastructure and network resources that are not publicly available (e.g., another government network interconnecting with the NRC for the purposes of sharing information or services such as SFTP or other general computational services).
- Interconnections between two networks, which are associated with separate systems, either internal or external to NRC.

4.1.6.4.1 Required Interconnection Information in an ISA

An ISA requires that the following be documented:

NI-I-S6 Information sensitivity must be documented within the ISA and specific restrictions must be placed on the interconnection based on the overall information sensitivity.

NI-I-S7 The level of interconnection must be documented within the ISA and specific restrictions must be placed on the interconnection based on how much access is granted (e.g., limited to a single application, system, network, or full enterprise).

NI-I-S8 The method of interconnection must be documented within the ISA and placement of specific restrictions are based on how the networks interconnect (e.g., VPN or direct connection).

NI-I-S9 Information flows (e.g., one or two way) must be documented within the ISA and placement of specific restrictions are based on how the information flows between the systems or networks.

NI-I-S10 The specific services provided by the interconnection must be documented within the ISA and the specific service(s) dictate the specific restrictions for the interconnection (e.g., an SFTP server providing file sharing services).

Once the required information is documented within the ISA, the following is required:

NI-I-S11 The specific requirements, restrictions, and security controls documented in the ISA must be reviewed and approved by the DAA.

NI-I-S12 The ISA must be signed by the DAA before an interconnection is established.

4.1.7 Network Trust Levels

Network trust levels can be differentiated from one another based upon their attributes. The following requirement applies to the identification of a network trust level to a specific network.

NI-NTL-S1 Each network must be assigned a network trust level. To be assigned a network trust level (e.g,. trusted, semi-trusted), the network must have the attributes specified in the sections below for the corresponding trust level.

- Section 4.1.9.1, Trusted
- Section 4.1.9.2, Semi-Trusted
- Section 4.1.9.3.1, Untrusted
- Section 4.1.9.3.2, Blacklisted

For example: For a network to be assigned the network trust level of "trusted," the network needs to have the attributes specified in Section 4.1.9.1, Trusted.

4.1.7.1 Trusted

Networks determined to be "trusted" by NRC have the following attributes:

- Employ sufficient information assurance measures to allow the network's use for processing NRC sensitive information;
- Be authorized to operate by the NRC DAA;
- Have all the required controls in place, operating as intended, and having the desired result in compliance with NRC cyber security policy;
- Be under NRC oversight, including NRC governing the facility, management, operational, and technical security controls; and
- There is an expectation of strong security controls and hardening of the network.

4.1.7.2 Semi-Trusted

Networks determined to be "semi-trusted" by NRC have an expectation of adequate security controls and hardening of the network and have the following attributes:

- DAA authorization to operate or a DAA signed ISA for external networks.
- All the NRC required controls are in place, operating as intended, and have the desired result.
- The network is under NRC partial or full control, including oversight of the facility, management, operational, and technical security controls.

The specific network dictates which of the above attributes apply as specified in Table 4.3-1, Baseline for Network Type Trust Levels.

4.1.7.3 Restricted

The two types of trust levels associated with the parent restricted trust level are untrusted and blacklisted.

4.1.7.3.1 Untrusted

Networks determined to be "untrusted" by NRC do not meet the requirements to be considered "trusted" or "semi-trusted" and generally have the following attributes:

- The network does not have an expectation of any security controls and hardening of the network.
- The network is potentially compromised.
- The network has no NRC oversight, including control of the facility, management, operational, and technical security controls.
- The network does not have a DAA signed ISA in place.

The following requirement applies to networks that are assigned the network trust level of "untrusted."

NI-NTL-S2 NRC infrastructure devices (e.g., firewall or VPN gateway) must not establish an interconnection to networks determined to be "untrusted" (excluding the Internet) that are not publicly available without a DAA signed ISA. Refer to CSO-STD-1004 for specific guidance on the use of laptops.

4.1.7.3.2 Blacklisted

Networks determined to be "blacklisted" are considered hostile at a given point in time and generally have the following permanent or temporary attributes:

- Networks permanently "blacklisted"
  - Connectivity with networks that are legally prohibited (e.g., related to criminal organizations, gambling, or pornography).
- Networks "blacklisted" at a given point in time
  - The network is hostile or suspected to be hostile (e.g., based upon information identified through network monitoring, information provided by the United States Computer Emergency Readiness Team [US-CERT]).
  - NRC suspects that the network is a threat vector for malicious attacks on the NRC's networks and systems.

The following requirements are associated with networks determined to be "blacklisted."

NI-NTL-S3 The NRC SOC must distribute or otherwise make available the list of networks blacklisted on a monthly basis to ISSOs of NRC systems that are not part of and do not use NRC Managed Networks for Internet connectivity. This is intended to reduce redundant efforts and take advantage of ongoing work by the NRC SOC to gather threat intelligence for greater effienciency and effectiveness of NRC network security.

NI-NTL-S4 ISSOs must ensure that blacklisted networks are reviewed at least twice per year to identify networks for possible removal (e.g., if a previously blacklisted network is determined to no longer represent a threat to NRC).

NI-NTL-S5 Networks determined to be “blacklisted” must be restricted from establishing an interconnection with NRC devices.

4.2 SGI

Networks that process plaintext SGI have specific requirements that go beyond the requirements for networks that process information determined to be SUNSI or below. These requirements are defined below.

4.2.1 Network Security Protections

Network security protections will be addressed in a future issuance of this document.

4.2.2 Wireless LAN Security

Wireless LAN security will be addressed in a future issuance of this document.

4.2.3 Network Monitoring

Network monitoring will be addressed in a future issuance of this document.

4.2.4 Physical Network Security

Physical network security will be addressed in a future issuance of this document.

4.2.5 Interconnections

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

4.3 Network Trust Levels Baseline

Each NRC network type, as described in Section 2.6, Network Types, are associated with a baseline trust level. This baseline network trust level is determined based on the characteristics of the network and security controls that the network type is expected to have in place.

Specific NRC networks are associated with NRC network types and associated with a trust level. The following requirement applies to the identification of network trust levels for each NRC network:

NI-NTL-S6 Each NRC network, which may be associated with one or more network types, must be associated with a network trust level. The network trust level is determined based on the characteristics of the network and the security controls the network has in place.

Table 4.3-1, Baseline for Network Type Trust Levels, identifies the baseline trust level for each network type and the rationale for the associated trust level.

The following defines the information contained within the columns of Table 4.3-1:

- Network Type: Identifies whether or not the network is an NRC managed network, network managed on behalf of NRC, or an external network. This also includes parent and child network type relationships.
- Trust Level: Identifies trust level for identified network.
- Rationale: Provides the justification for the identified network's trust level.

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
NRC Managed Networks			
NRC WAN	*Infrastructure Networks*	Trusted	• Authorized to operate by the NRC DAA • Under NRC oversight • Has required NRC security controls in place to comply with NRC cyber security policy.
	BA Networks	Trusted	• Authorized to operate by the NRC DAA • Under NRC oversight • Has required NRC security controls in place to comply with NRC cyber security policy
	RISE Networks	Semi-trusted	• Authorized to operate by the NRC DAA • Has all required controls in place to comply with NRC cyber security policy • Under NRC partial control and oversight of facility, management, operational, and technical security controls • Has an expectation of adequate security controls and hardening of network • Does not have strong physical security controls.
NRC Extended Networks	*NRCEL Networks*	Semi-trusted	• Has required controls in place to comply with NRC cyber security policy • Has an expectation of adequate security controls and hardening of the network
NRC Special Purpose Networks	*Management Networks*	Trusted	• Authorized to operate by the NRC DAA • Under NRC control and oversight of facility, management, operational, and technical security controls • Has required NRC security controls in place to comply with NRC cyber security policy
	Standalone Office LANs	Semi-trusted	• Authorized to operate by the NRC DAA • Have all required controls in place to comply with NRC cyber security policy • As standalone networks, there is not an expectation of strong security controls and hardening of the network
(NRC Special Purpose Networks	*Guest Networks*	Untrusted	• Authorized to operate by the NRC DAA • Does not have an expectation of strong security controls and

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
Cont'd.)			hardening of the network • Allows users without an NRC account to access the Internet
	DMZs	Semi-trusted	• Authorized to operate by the NRC DAA • Under NRC control and oversight of facility, management, operational, and technical security controls • Expectation of adequate security controls and hardening of network
	Research and Development (Nuclear)	Semi-trusted	• Authorized to operate by the NRC DAA • Under NRC control and oversight of facility, management, operational, and technical security controls • Has an expectation of adequate security controls and hardening of network
	Research and Development (IT)	Semi-trusted	• Authorized to operate by the NRC DAA • Under NRC control and oversight of facility, management, operational, and technical security controls • Has an expectation of adequate security controls and hardening of network
	HPC	Semi-trusted	• Authorized to operate by the NRC DAA • Under NRC control and oversight of facility, management, operational, and technical security controls • Has an expectation of adequate security controls and hardening of network
Networks Managed on Behalf of NRC			
Contractor/Government Hosted Networks Specifically for NRC		Semi-trusted with DAA signed ISA	• Authorized to operate by the NRC DAA • Has all required controls in place to comply with NRC cyber security policy • Under NRC partial control and oversight of facility, management, operational, and technical security controls • Has an expectation of adequate security controls and hardening of network

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
Contractor/Vendor/Government Hosted Cloud Service		Semi-trusted	• Authorized to operate by the NRC DAA • Has required controls in place to comply with NRC cyber security policy • Has an expectation of adequate security controls and hardening of the network
ISPs		Semi-trusted with DAA signed ISA	• Has an expectation of adequate security controls and hardening of the network
External Networks			
Contractor, Vendor, and Service Provider Networks	*Phone/Satellite/Data Carriers*	Semi-trusted	• Has an expectation of adequate security controls and hardening of the network
Contractor, Vendor, and Service Provider Networks	*Vendor Networks Providing Maintenance Services*	Semi-trusted with DAA signed ISA	• Has required controls in place to comply with NRC cyber security policy • Has an expectation of adequate security controls and hardening of the network
Other Government Networks		Semi-trusted with DAA signed ISA	• Has required controls in place to comply with NRC cyber security policy • Has an expectation of adequate security controls and hardening of the network
Telework Networks	*NRC Compliant Home Networks*	Semi-trusted	• Home networks are configured in accordance with CSO-STD-1801 or CSO-STD-1802 • Has required controls in place to comply with NRC cyber security policy • Does have expectation of adequate security controls and hardening of the network
	Non-compliant Home Networks	Untrusted	• Home networks are not configured in accordance with CSO-STD-1801or CSO-STD-1802 • Does not have all required controls in place to comply with NRC cyber security policy • Does not have an expectation of adequate security controls and hardening of the network
	Public Access Networks	Untrusted	• Fall outside the purview of NRC oversight and have unknown security controls
	State Government Telework Centers	Untrusted	• Fall outside the purview of NRC oversight and have unknown security controls

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
	Other Organizations' Guest Networks	Untrusted	• Fall outside the purview of NRC oversight and have unknown security controls
Licensee and Licensee Contractor Networks		Untrusted	• Fall outside the purview of NRC oversight and have unknown security controls
Academia Networks		Untrusted	• Resides outside the boundaries of the NRC managed network and networks managed on behalf of NRC • Fall outside the purview of NRC oversight and have unknown security controls
Industry Networks		Untrusted	• Resides outside the boundaries of the NRC managed network and networks managed on behalf of NRC • Fall outside the purview of NRC oversight and have unknown security controls
Foreign Government and International Organizations' Networks		Untrusted	• Resides outside the boundaries of the NRC managed network and networks managed on behalf of NRC • Fall outside the purview of NRC oversight and have unknown security controls
Internet		Untrusted	• Resides outside the boundaries of the NRC managed network and networks managed on behalf of NRC • Falls outside the purview of NRC oversight

APPENDIX A. ACRONYMS

3WFN	Three White Flint North
AAA	Authentication Authorization Accounting
ACL	Access Control List
ADC	Application Delivery Controller
AP	Access Point
AS	Authentication Server
ASIC	Application Specific Integrated Circuits
B2G	Non-Government/Private Organizations/Business-to-Government
BA	Business/Application
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
C2G	Citizen-to-Government
CM	Configuration Management
CNSS	Committee for National Security Systems
CSS	Cascading Style Sheets
D2T	Device-to-Telework
DAA	Designated Approving Authority
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DHTML	Dynamic Hypertext Markup Language
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol

EIE	Electronic Information Exchange
ESA	Enterprise Security Architecture
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FTP	File Transfer Protocol
G2G	Government-to-Government
GHz	Gigahertz
HOC	Headquarters Operations Center
HP	Hewlett-Packard
HPC	High Performance Computing
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol/Secure
I2G	International Entities/Organizations-to-Government
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention System
iDRAC	integrated Dell Remote Access Card
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
iLO	Integrated Lights Out
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS	Infrastructure Support

ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISSO	Information System Security Officer
IT	Information Technology
KVM	Keyboard-Video-Mouse
L2G	Licensee-to-Government
LAN	Local Area Network
LOM	Lights-out Management
LOS	Line-of-Sight
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control
MFD	Multi-function Device
MHz	Megahertz
MOU/A	Memorandum of Understanding or Agreement
MPLS	Multi-protocol Label Switching
MTIPS	Managed Trusted Internet Protocol Service
N2N	NRC Network-to-NRC Network
NAC	Network Access Control
NBP	Network Boundary Protection
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operations Center
NPPS	Network Ports, Protocols, and Services
NRC	Nuclear Regulatory Commission
NRCEL	NRC Extended Licensee

NSA	National Security Agency
NSIR	Office of Nuclear Security and Incident Response
NSP	Network Security Protection
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OGC	Office of General Counsel
OMB	Office of Management and Budget
OOB	Out-of-Band
OSI	Open Systems Interconnection
P2P	Peer-to-Peer
PaaS	Platform as a Service
PBX	Private Branch Exchange
PDC	Professional Development Center
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PII	Personally Identifiable Information
PROS	Process
RADIUS	Remote Authentication Dial-In User Service
RISE	Resident Inspector Site Expansion
RO	Regional Office
SaaS	Software as a Service
SAN	Storage Area Network
SCI	Sensitive Compartmented Information
SFTP	Secure File Transfer Protocol
SGI	Safeguards Information
SMTP	Simple Mail Transfer Protocol

SNR	Signal-to-Noise Ratio
SOC	Security Operations Center
SP	Special Publication
SSID	Service Set Identifier
SSL	Security Sockets Layer
STA	Station
STD	Standard
SUNSI	Sensitive Unclassified Non-safeguards Information
T2N	Telework-to-NRC Network
TCP	Transmission Control Protocol
TEMP	Template
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TRM	Technical Reference Model
TTC	Technical Training Center
UDP	User Datagram Protocol
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAN	Wide Area Network
WIDS	Wireless Intrusion Detection System

WiMAX	Worldwide Interoperability for Microwave Access
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WWW	World Wide Web
XSS	Cross-Site Scripting

APPENDIX B. GLOSSARY

Academia Networks	Networks owned and/or hosted by academia.
Blacklisted Networks	Forbidden networks that NRC computing devices are prohibited from connecting to unless there is a specific need to access such a network in an isolated fashion in which prior approval has been granted.
Boundary Protection Device	Devices used to detect, prevent, and correct the flow of IP packets transiting networks based on security needs.
Contractor/Government Hosted Networks Specifically for NRC	Networks hosted by another party specifically for NRC, and are not used for any other party (e.g., the network is not used for other government agencies or contractors).
Contractor/Vendor/Government Hosted Cloud Service	Networks provide cloud services to several different parties (i.e., multiple federal agencies). Common cloud service models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), or Platform as a Service (PaaS).
Contractor, Vendor, and Service Provider Networks	Networks that provide general services to the NRC.
Deep Packet Inspection	An inspection of the payload of an IP packet.
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.
Enclave	A system connected by one or more internal networks under the control of a single authority and security policy that supports a specialized function.
Evil Twin	A rogue AP that uses a SSID that matches or is very similar to the SSID of an authorized AP.
External Networks	Networks that interconnect with the NRC network or are used by individuals to connect to NRC networks, systems, and applications.
Externally Facing	A device or capability that is accessible from outside the network. Externally facing capabilities must reside in the DMZ.
File Transfer Protocol	A standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

Foreign Government and International Organizations' Networks	Networks owned and/or hosted by foreign governments or by companies in foreign countries.
Hardened	A network or system that has been secured by reducing its overall vulnerability through the use of cyber security controls and security best practices.
Highly Directional Antennas	Antennas that have a very limited coverage area and are used for covering larger distances, point-to-point connections, and for bridging wireless networks.
Hotspots	A location that offers wired or wireless broadband network services to visitors. Hotspots are often located in places such as airports, train stations, libraries, marinas, conventions centers, restaurants, and hotels.
Inbound Network Traffic	Network traffic entering into a network at an ingress point.
Industry Networks	Networks owned and/or hosted by industry.
Infrastructure Support Networks	Networks providing infrastructure support services (e.g., identity, access management, time, DNS) to other systems/networks.
Interconnection	An interconnection is a connection between two separate network nodes for the purpose of network communication.
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 MOU/A between the organizations.
Internet Service Providers	A service provider that provides access to the Internet and may provide other services such as MPLS connectivity.
Licensee	A company, organization, institution, or other entity to which the NRC or an Agreement State has granted a general license or specific license to construct or operate a nuclear facility, or to receive, possess, use, transfer, or dispose of source material, byproduct material, or special nuclear material.
Multi-protocol Label Switching	A method that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system or ISP in order to simplify and improve IP-packet exchange.
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 Boundary Protection	A parent category of many different network capabilities and NSPs that are used to detect, prevent, and correct the flow of IP packets transiting networks based on security needs.

Network Domain	A domain that implements a cyber security policy and is administered by a single authority.
Network Gateways	Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
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.
Network Management System	A combination of hardware and software used to monitor and administer computer networks.
Network Segment	A separated subset of the larger network in which its boundaries are created by different network devices.
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.
Omnidirectional Antennas	An antenna that broadcasts in all directions.
Open Systems Interconnection	The OSI model defines Internet working in terms of a vertical stack of seven layers. The upper layers of the OSI model represent software that implements network services like encryption and connection management. The lower layers of the OSI model implement more primitive, hardware-oriented functions like routing, addressing, and flow control.
Out-of-Band Management	The exchange of call control information in a separate band from the data or voice stream, or on an entirely separate, dedicated channel. In this case, control information for the management network is completely separate from the rest of the network traffic.
Packet	Logical grouping of information that includes a header containing control information and user data.
Payload	The data portion of a packet.
Plaintext	Information that has no form of encryption.
Point-to-point Connection	A connection between two network nodes.

Restricted Network	Any network that is not a trusted network or semi-trusted network. This includes all networks originating from a foreign country and publicly accessible networks (e.g., public hotspots) or networks otherwise accessible to members of the public through commercial businesses (e.g., hotel networks).
Safeguards Information Network	Network used to process sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant that are designed to protect special nuclear mateal or to protect the physical location of certain plant equipment that is vital to safety of production/utilization facilities, known as Safeguards Information.
Semidirectional Antennas	Antennas that broadcast in sectors or patches and have a limited coverage area.
Semi-trusted Network	Semi-trusted networks are networks where security controls have been applied; limiting risks of system compromise and breaches.
Sensitive Unclassified Non-Safeguards Information	Information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.).
Stateful Inspection	Stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall.
Telework Networks	Networks used for remotely accessing NRC internal resources and to conduct work.
Trusted Internet Connection	This is the NRC term used when referencing the organizations ISP; synonymous with service provider.
Trusted Network	A network that employs sufficient hardware and software assurance measures to allow its use for processing SUNSI. For the purposes of this standard, NRC managed networks are the only trusted networks.
Untrusted Network	A category of restricted networks. Network where security controls are limited or have not been applied; increasing risks of system compromise and breaches. Use of untrusted networks puts laptops, information, and users at risk of possible compromise or breach due to an assumed lack of verified, effective network security controls.

APPENDIX C. NRC NETWORK INTERCONNECTION DIAGRAMS

This appendix clarifies requirement NI-I-G3 in Section 3.7, Interconnections. The appendix specifies whether an interconnection is permitted based upon the respective network types.

The NRC network interconnection diagrams contained within this appendix provide a conceptual representation of possible interconnections based on the previously defined network types and trusts. The diagrams present whether an interconnection is permitted (X = No, √ = Yes), but does not define the specific conditions or requirements for the interconnection. For the purpose of these diagrams, an interconnection is depicted as two networks transmitting data to each other.

The interconnections make the following assumptions:

1. The interconnections are based on a point-to-point connection (e.g., a business/application network interconnecting with a home network would have to interconnect with the NRC-DMZ and then pass through the Internet to reach the home network).
2. The NRC-DMZ is on the network border and the only perimeter DMZ. All other DMZs (e.g., Infrastructure Networks DMZs) are internal.
3. The permissibility of an interconnection is based on whether a network interconnection currently occurs or may occur based on future needs.
4. The diagrams do not list external networks interconnecting with other external networks or the Internet (e.g., telenetwork connecting to the Internet) since the NRC does not manage or control these connections.
5. The ISP may provide Internet connectivity (i.e., TIC/MTIPS) and/or the connectivity (i.e., MPLS) for the NRC WAN.

The NRC network interconnection diagrams can be accessed via the following link:

OCIO-CS-STD-4000 NRC Network Interconnection Diagrams.docx

APPENDIX D. INTERCONNECTION MATRICES

The following matrices identify whether interconnections based on the previously defined network types and trusts are permitted, but do not define the specific conditions or requirements for the interconnection. These matrices depict an interconnection as two networks transmitting data to each other. Each potential network interconnection is mapped and bi-directional (i.e., the connection may originate at either network).

The interconnections make the following assumptions:

1. The interconnections are based on a point-to-point connection (e.g., a business/application network interconnecting with a home network would have to interconnect with the NRC-DMZ and then pass through the Internet to reach the home network).
2. The NRC-DMZ is on the network border and the only perimeter DMZ. All other DMZs (e.g., Infrastructure Networks DMZs) are internal.
3. The permissibility of an interconnection is based on whether a network interconnection currently occurs or may occur based on future needs.
4. The matrix does not list external networks interconnecting with other external networks or the Internet (e.g., telenetwork connecting to the Internet) since the NRC does not manage or control these connections.
5. The ISP may provide Internet connectivity (i.e., TIC/MTIPS) and/or the connectivity (i.e., MPLS) for the NRC WAN.

Each matrix identifies the parent and child network types under each NRC network category and the interconnections permitted between the parent/child network types. The following defines the information contained within the columns of each matrix in this appendix:

- Network Type: This refers to the type of network as defined in Section 2.6, Network Types, that each specific network may potentially interconnect with.
- Interconnection Permitted (Yes/No): This describes if an interconnection is permitted.

Table D-1: NRC Managed Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
NRC WAN		
NRC-DMZ	Yes	ISP
NRC-DMZ	Yes	NRC-DMZ
IS	Yes	IS-DMZ
BA	Yes	BA-DMZ
IS	No	IS
BA	No	BA
BA-DMZ	Yes	BA-DMZ
IS-DMZ	Yes	BA-DMZ
IS-DMZ	Yes	IS-DMZ
IS-DMZ	Yes	NRC-DMZ
BA-DMZ	Yes	NRC-DMZ
IS	No	BA
IS	No	ISP
BA	No	ISP
IS-DMZ	No	ISP
BA-DMZ	No	ISP
NRC EXTENDED NETWORKS		
RISE	Yes	RISE-DMZ
RISE	No	NRC Licensee
RISE	No	NRC Licensee-DMZ
RISE	No	NRC Licensee-DMZ
RISE	No	ISP
RISE	No	IS-DMZ
RISE	No	BA-DMZ
RISE	No	IS
RISE	No	BA
NRCEL	No	NRC Licensee
NRCEL	Yes	NRCEL-DMZ
NRCEL	No	NRC-DMZ
NRCEL	No	ISP
NRCEL	No	IS-DMZ
NRCEL	No	BA-DMZ
NRCEL	No	IS
NRCEL	No	BA

Table D-1: NRC Managed Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
NRCEL	No	RISE-DMZ
NRCEL-DMZ	Yes	NRC-DMZ (via ISP)
NRCEL-DMZ	Yes	NRCEL-DMZ
NRCEL-DMZ	Yes	ISP
NRCEL-DMZ	No	IS-DMZ
NRCEL-DMZ	No	BA-DMZ
NRCEL-DMZ	No	IS
NRCEL-DMZ	No	BA
NRCEL-DMZ	No	RISE-DMZ
RISE-DMZ	Yes	RISE-DMZ
RISE-DMZ	Yes	ISP
RISE-DMZ	No	NRCEL
RISE-DMZ	Yes	NRC-DMZ (via ISP)
RISE-DMZ	No	IS-DMZ
RISE-DMZ	No	BA-DMZ
RISE-DMZ	No	IS
RISE-DMZ	No	BA
NRC SPECIAL PURPOSE NETWORKS		
Guest	No	Guest
Guest	Yes	NRC-DMZ
Guest	No	ISP
Standalone Office LANs	Yes	Standaone Office LANs-DMZ
Standalone Office LANs	No	Standalone Office LANs
Standalone Office LANs	No	Guest
Standalone Office LANs	No	ISP
Standalone Office LANs-DMZ	No	NRC-DMZ
Standalone Office LANs-DMZ	Yes	Standalone Office LANs-DMZ
Standalone Office LANs-DMZ	Yes	ISP
Standalone Office LANs-DMZ	No	Guest

Table D-2: Networks Managed on Behalf of NRC

Network Type	Interconnection Permitted (Yes/No)	Network Type
Contractor/Government Hosted Networks Specifically for NRC (GCNRC)	No	NRC-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service (CVGCS)	No	NRC-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Contractor/Government Hosted Networks Specifically for NRC-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Contractor/Vendor/Government Hosted Cloud Service-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	NRC-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	NRC-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC	No	Contractor/Government Hosted Networks Specifically for NRC
Contractor/Government Hosted Networks Specifically for NRC	No	IS
Contractor/Government Hosted Networks Specifically for NRC	No	BA
Contractor/Government Hosted Networks Specifically for NRC	No	IS-DMZ
Contractor/Government Hosted Networks Specifically for NRC	No	BA-DMZ
Contractor/Government Hosted Networks Specifically for NRC	No	RISE
Contractor/Government Hosted Networks Specifically for NRC	No	NRC Licensee
Contractor/Government Hosted Networks Specifically for NRC	No	NRC Licensee-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	IS
Contractor/Vendor/Government Hosted Cloud Service	No	BA
Contractor/Vendor/Government Hosted Cloud Service	No	IS-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	BA-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	Contractor/Vendor/Government Hosted Cloud Service
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	IS
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	BA

Table D-2: Networks Managed on Behalf of NRC

Network Type	Interconnection Permitted (Yes/No)	Network Type
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	IS-DMZ
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	BA-DMZ
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Contractor/Vendor/Government Hosted Cloud Service-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	RISE
Contractor/Vendor/Government Hosted Cloud Service	No	RISE-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	NRC Licensee
Contractor/Vendor/Government Hosted Cloud Service	No	NRC Licensee-DMZ
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	RISE
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	RISE-DMZ
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	NRCL
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	NRC Licensee-DMZ
Contractor/Government Hosted Networks Specifically for NRC	No	RISE
Contractor/Government Hosted Networks Specifically for NRC	No	RISE-DMZ
Contractor/Government Hosted Networks Specifically for NRC	No	NRC Licensee
Contractor/Government Hosted Networks Specifically for NRC	No	NRC Licensee-DMZ
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	RISE
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	RISE-DMZ
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	NRC Licensee
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	NRC Licensee-DMZ
Contractor/Government Hosted Networks Specifically for NRC	No	Telework Networks
Contractor/Government Hosted Networks Specifically for NRC	No	Academia

Table D-2: Networks Managed on Behalf of NRC

Network Type	Interconnection Permitted (Yes/No)	Network Type
Contractor/Government Hosted Networks Specifically for NRC	No	Industry Networks
Contractor/Government Hosted Networks Specifically for NRC	No	Contractor, Vendor, and Service Provider Networks
Contractor/Government Hosted Networks Specifically for NRC	No	Other Government Networks
Contractor/Government Hosted Networks Specifically for NRC	No	Licensee and Licensee Contractor Networks
Contractor/Government Hosted Networks Specifically for NRC	No	ISP
Contractor/Government Hosted Networks Specifically for NRC	No	Foreign Government and International Organizations' Networks
Contractor/Government Hosted Networks Specifically for NRC	No	Contractor/Vendor/Government Hosted Cloud Service
Contractor/Government Hosted Networks Specifically for NRC	Yes	Contractor/Government Hosted Networks Specifically for NRC-DMZ
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Telework Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Academia
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Industry Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Contractor, Vendor, and Service Provider Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Other Government Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Licensee and Licensee Contractor Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	ISP
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Foreign Government and International Organizations' Networks
Contractor/Government Hosted Networks Specifically for NRC-DMZ	No	Contractor/Vendor/Government Hosted Cloud Service
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Academia-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Industry Networks-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Contractor, Vendor, and Service Provider Networks-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Other Government Networks-DMZ (via ISP)

Table D-2: Networks Managed on Behalf of NRC

Network Type	Interconnection Permitted (Yes/No)	Network Type
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Licensee and Licensee Contractor Networks-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	ISP
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Foreign Government and International Organizations' Networks-DMZ (via ISP)
Contractor/Government Hosted Networks Specifically for NRC-DMZ	Yes	Contractor/Vendor/Government Hosted Cloud Service-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service	No	Telework Networks
Contractor/Vendor/Government Hosted Cloud Service	No	Academia
Contractor/Vendor/Government Hosted Cloud Service	No	Industry Networks
Contractor/Vendor/Government Hosted Cloud Service	No	Contractor, Vendor, and Service Provider Networks
Contractor/Vendor/Government Hosted Cloud Service	No	Other Government Networks
Contractor/Vendor/Government Hosted Cloud Service	No	Licensee and Licensee Contractor Networks
Contractor/Vendor/Government Hosted Cloud Service	No	ISP
Contractor/Vendor/Government Hosted Cloud Service	No	Foreign Government and International Organizations' Networks
Contractor/Vendor/Government Hosted Cloud Service	No	Contractor/Vendor/Government Hosted Cloud Service
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Telework Networks
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	Academia
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	Industry Networks
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	Contractor, Vendor, and Service Provider Networks
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	Other Government Networks
Contractor/Vendor/Government Hosted Cloud Service -DMZ	No	Licensee and Licensee Contractor Networks
Contractor/Vendor/Government Hosted Cloud Service -DMZ	Yes	ISP
Contractor/Vendor/Government Hosted Cloud Service-DMZ	No	Foreign Government and International Organizations' Networks

Table D-2: Networks Managed on Behalf of NRC

Network Type	Interconnection Permitted (Yes/No)	Network Type
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Contractor/Vendor/Government Hosted Cloud Service
Contractor/Vendor/Government Hosted Cloud Service	No	Academia-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	Industry Networks-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	Contractor, Vendor, and Service Provider Networks-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	Other Government Netoworks-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	Licensee and Licensee Contractor Networks-DMZ
Contractor/Vendor/Government Hosted Cloud Service	No	ISP
Contractor/Vendor/Government Hosted Cloud Service	No	Foreign Government and International Organizations' Networks-DMZ
Contractor/Vendor/Government Hosted Cloud Service	Yes	Contractor/Vendor/Government Hosted Cloud Service-DMZ
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Academia-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Industry Networks-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Contractor, Vendor, and Service Provider Networks-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Other Government Networks-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Licensee and Licensee Contractor Networks-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	ISP
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Foreign Government and International Organizations' Networks-DMZ (via ISP)
Contractor/Vendor/Government Hosted Cloud Service-DMZ	Yes	Contractor/Vendor/Government Hosted Cloud Service-DMZ (via ISP)

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
Other Government Networks	No	NRC-DMZ
Other Government Networks	No	IS
Other Government Networks	No	BA
Other Government Networks	No	IS-DMZ
Other Government Networks	No	BA-DMZ
Other Government Networks-DMZ	Yes	NRC-DMZ (via ISP)
Other Government Networks-DMZ	No	IS
Other Government Networks-DMZ	No	BA
Other Government Networks-DMZ	No	IS-DMZ
Other Government Networks-DMZ	No	BA-DMZ
Telework Networks	Yes	NRC-DMZ (via ISP)
Telework Networks	No	IS
Telework Networks	No	BA
Telework Networks	No	IS-DMZ
Telework Networks	No	BA-DMZ
Academia	No	NRC-DMZ
Academia	No	IS
Academia	No	BA
Academia	No	IS-DMZ
Academia	No	BA-DMZ
Industry Networks	No	NRC-DMZ
Industry Networks	No	IS
Industry Networks	No	BA
Industry Networks	No	IS-DMZ
Industry Networks	No	BA-DMZ
Academia-DMZ	Yes	NRC-DMZ
Academia-DMZ	No	IS
Academia-DMZ	No	BA
Academia-DMZ	No	IS-DMZ
Academia-DMZ	No	BA-DMZ
Industry Network-DMZ	Yes	NRC-DMZ
Industry Networks-DMZ	No	IS

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
Industry Networks-DMZ	No	BA
Industry Networks -DMZ	No	IS-DMZ
Industry Networks-DMZ	No	BA-DMZ
Licensee and Licensee Contractor Networks	No	NRC-DMZ
Licensee and Licensee Contractor Networks	No	IS
Licensee and Licensee Contractor Networks	No	BA
Licensee and Licensee Contractor Networks	No	IS-DMZ
Licensee and Licensee Contractor Networks	No	BA-DMZ
Licensee and Licensee Contractor Networks-DMZ	Yes	NRC-DMZ (via ISP)
Licensee and Licensee Contractor Networks-DMZ	No	IS
Licensee and Licensee Contractor Networks-DMZ	No	BA
Licensee and Licensee Contractor Networks-DMZ	No	IS-DMZ
Licensee and Licensee Contractor Networks-DMZ	No	BA-DMZ
Foreign Government and International Organizations' Networks	No	NRC-DMZ
Foreign Government and International Organizations' Networks	No	IS
Foreign Government and International Organizations' Networks	No	BA
Foreign Government and International Organizations' Networks	No	IS-DMZ
Foreign Government and International Organizations' Networks	No	BA-DMZ
Foreign Government and International Organizations' Networks-DMZ	Yes	NRC-DMZ (via ISP)
Foreign Government and International Organizations' Networks-DMZ	No	IS
Foreign Government and International Organizations' Networks-DMZ	No	BA
Foreign Government and International Organizations' Networks-DMZ	No	IS-DMZ
Foreign Government and International Organizations' Networks-DMZ	No	BA-DMZ
ISP	Yes	NRC-DMZ
ISP	No	IS

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
ISP	No	BA
ISP	No	IS-DMZ
ISP	No	BA-DMZ
Contractor, Vendor, and Service Provider Networks	Yes	NRC-DMZ
Contractor, Vendor, and Service Provider Networks	No	IS
Contractor, Vendor, and Service Provider Networks	No	BA
Contractor, Vendor, and Service Provider Networks	No	IS-DMZ
Contractor, Vendor, and Service Provider Networks	No	BA-DMZ
Contractor, Vendor, and Service Provider Networks	No	Standalone Office LANs
Contractor, Vendor, and Service Provider Networks	No	Standalone Office LANs -DMZ
Contractor, Vendor, and Service Provider Networks	No	Guest
Contractor, Vendor, and Service Provider Networks-DMZ	No	Standalone Office LANs
Contractor, Vendor, and Service Provider Networks-DMZ	Yes	Standalone Office LANs -DMZ
Contractor, Vendor, and Service Provider Networks-DMZ	No	Guest
Other Government Networks	No	Standalone Office LANs
Other Government Networks	No	Standalone Office LANs -DMZ
Other Government Networks	No	Guest
Other Government Networks-DMZ	No	Standalone Office LANs
Other Government Networks-DMZ	No	Standalone Office LANs -DMZ
Other Government Networks-DMZ	No	Guest
Telework Networks	No	Standalone Office LANs
Telework Networks	No	Standalone Office LANs -DMZ
Telework Networks	No	Guest
Academia	No	Standalone Office LANs
Academia	No	Standalone Office LANs -DMZ

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
Academia	No	Guest
Academia-DMZ	No	Standalone Office LANs
Academia-DMZ	No	Standalone Office LANs -DMZ
Academia-DMZ	No	Guest
Industry Networks	No	Standalone Office LANs
Industry Networks	No	Standalone Office LANs-DMZ
Industry Networks	No	Guest
Industry Networks-DMZ	No	Standalone Office LANs (SOL)
Industry Networks-DMZ	No	Standalone Office LANs-DMZ
Industry Networks -DMZ	No	Guest
Licensee and Licensee Contractor Networks	No	Standalone Office LANs
Licensee and Licensee Contractor Networks	No	Standalone Office LANs-DMZ
Licensee and Licensee Contractor Networks	No	Guest
Licensee and Licensee Contractor Networks-DMZ	No	Standalone Office LANs
Licensee and Licensee Contractor Networks-DMZ	No	Standalone Office LANs-DMZ
Licensee and Licensee Contractor Networks-DMZ	No	Guest
Foreign Government and International Organizations' Networks	No	Standalone Office LANs
Foreign Government and International Organizations' Networks	No	Standalone Office LANs-DMZ
Foreign Government and International Organizations' Networks	No	Guest
Foreign Government and International Organizations' Networks-DMZ	No	Standalone Office LANs
Foreign Government and International Organizations' Networks-DMZ	No	Standalone Office LANs-DMZ
Foreign Government and International Organizations' Networks-DMZ	No	Guest

OCIO-CS-STD-4000 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
04-Jun-14	1.0	Initial Release	ISD web page	As needed
08-Jul-14	1.1	Editorial change to clarify connectivity to licensee networks based upon OGC NLO	ISD web page	As needed
10-Jan-17	1.2	Revision to incorporate requirements for wireless LAN security, network security protections, and network segmentation.	Computer Security web page	As needed