Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-4000**
Office Instruction Title:	**Network Infrastructure Standard**
Revision Number:	**1.0**
Effective Date:	**June 30, 2014**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PCT**
Summary of Changes:	CSO-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.:	ML13295A407

Approvals				
Primary Office Owner	Policies, Compliance, and Training		**Signature**	**Date**
Enterprise Security Architecture Working Group Chair and Responsible SITSO	Kathy Lyons-Burke		**/RA/**	6/4/14
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	**/RA/**	6/4/14
	Director, OIS	Jim Flanagan	**/RA/**	6/5/14

Table of Contents

List of Figures

List of Tables

Computer Security Standard
CSO-STD-4000

Network Infrastructure Standard

---

1 PURPOSE

CSO-STD-4000, “Network Infrastructure Standard,” provides the minimum security requirements that must be applied to the Nuclear Regulatory Commission (NRC) network-computing environment processing information up to and including, the Safeguards Information (SGI) level. 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; network topology; Internet Protocol version 6 (IPv6); 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.”

CSO-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 Requirements Definitions

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 defintions 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*.

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 Exclusions from this Standard

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

- Classified networks

2.4 Security Categorizations and Impact Levels

The Federal Information Processing Standards (FIPS) Publication (PUB) 199 defines security categories for 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 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.

2.5 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.

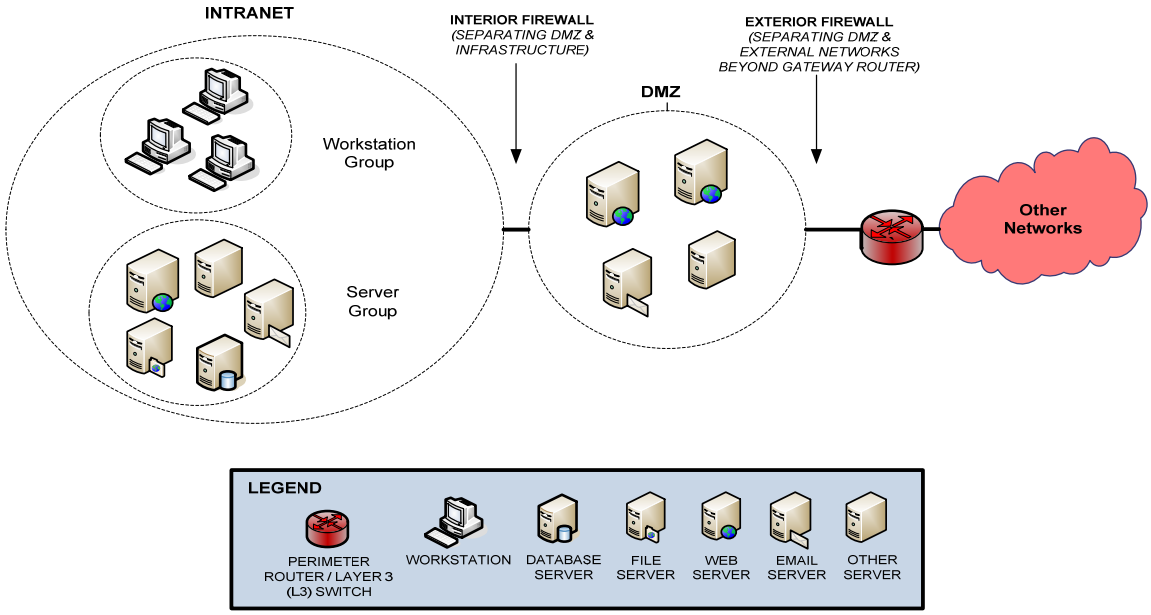


Figure 2.5-1: Basic Network

2.6 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.

2.6.1 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 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. • 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 stretched to accommodate 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.

Table 2.6-1: NRC Managed Networks

NRC Managed Networks	
Parent Network Type	**Child Network Type**
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.

2.6.2 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.

2.6.3 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.
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.

2.6.4 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.

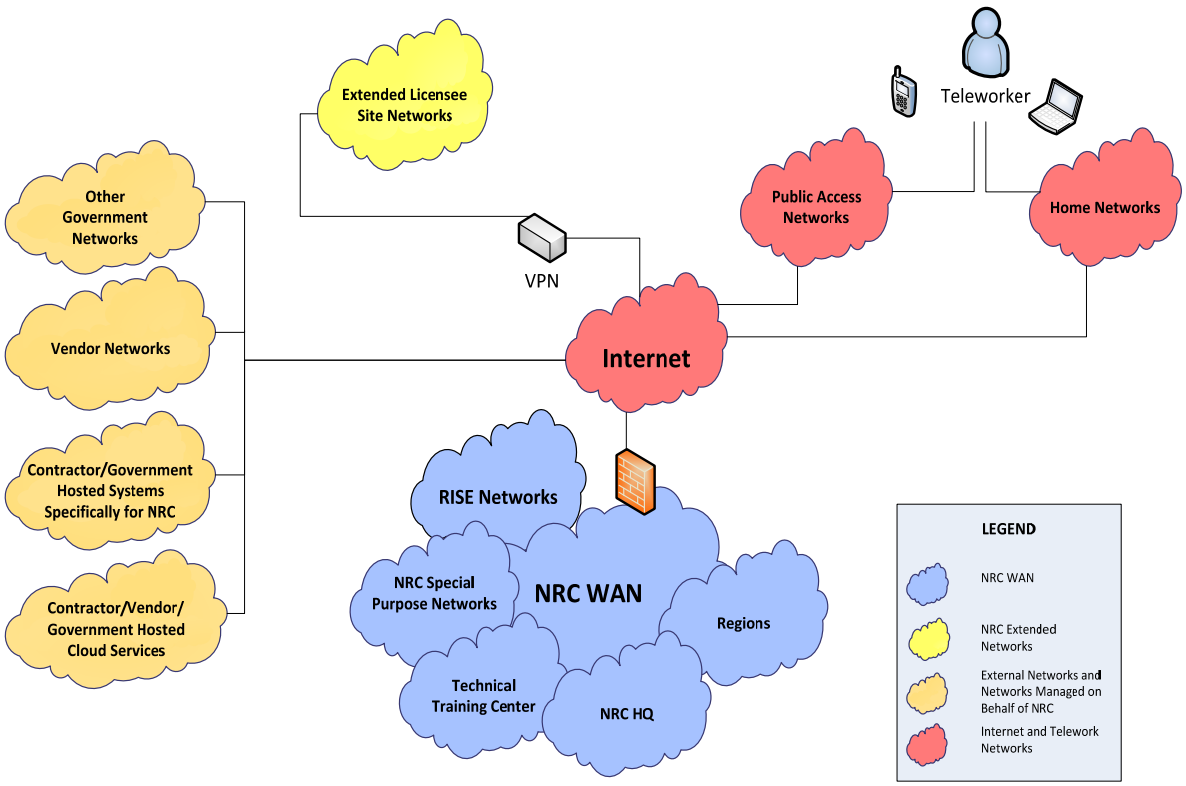


Figure 2.6-1: Conceptual NRC Network

2.6.5 NRC Network Types Summary

Table 2.6-4 NRC Network Type Summary, 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
	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

2.7 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.

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 less stringent security requirements because of the need to test 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.

2.8 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

2.8.1 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.

2.8.2 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.

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

2.8.3 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.

2.8.3.1 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:

[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.

- 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.

2.8.3.2 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.

2.9 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.

2.9.1 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.

2.9.2 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.

2.9.3 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.

2.9.4 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.

2.9.5 VLANs

The Institute of Electrical and Electronics Engineers (IEEE)'s 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.

2.9.6 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.

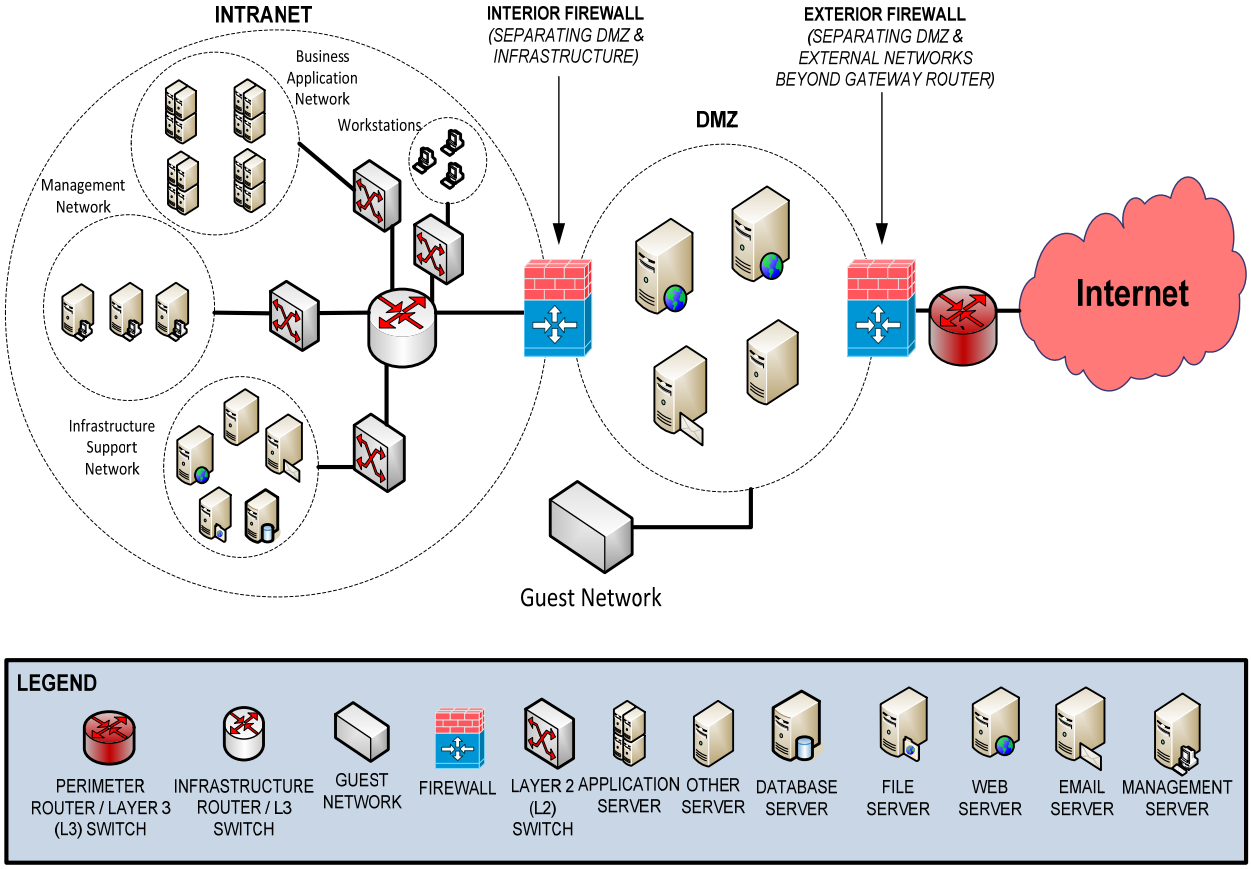


Figure 2.9-1: Conceptual View of Network Segmentation

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 Security 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 provides an example of how network segmentation can be achieved.

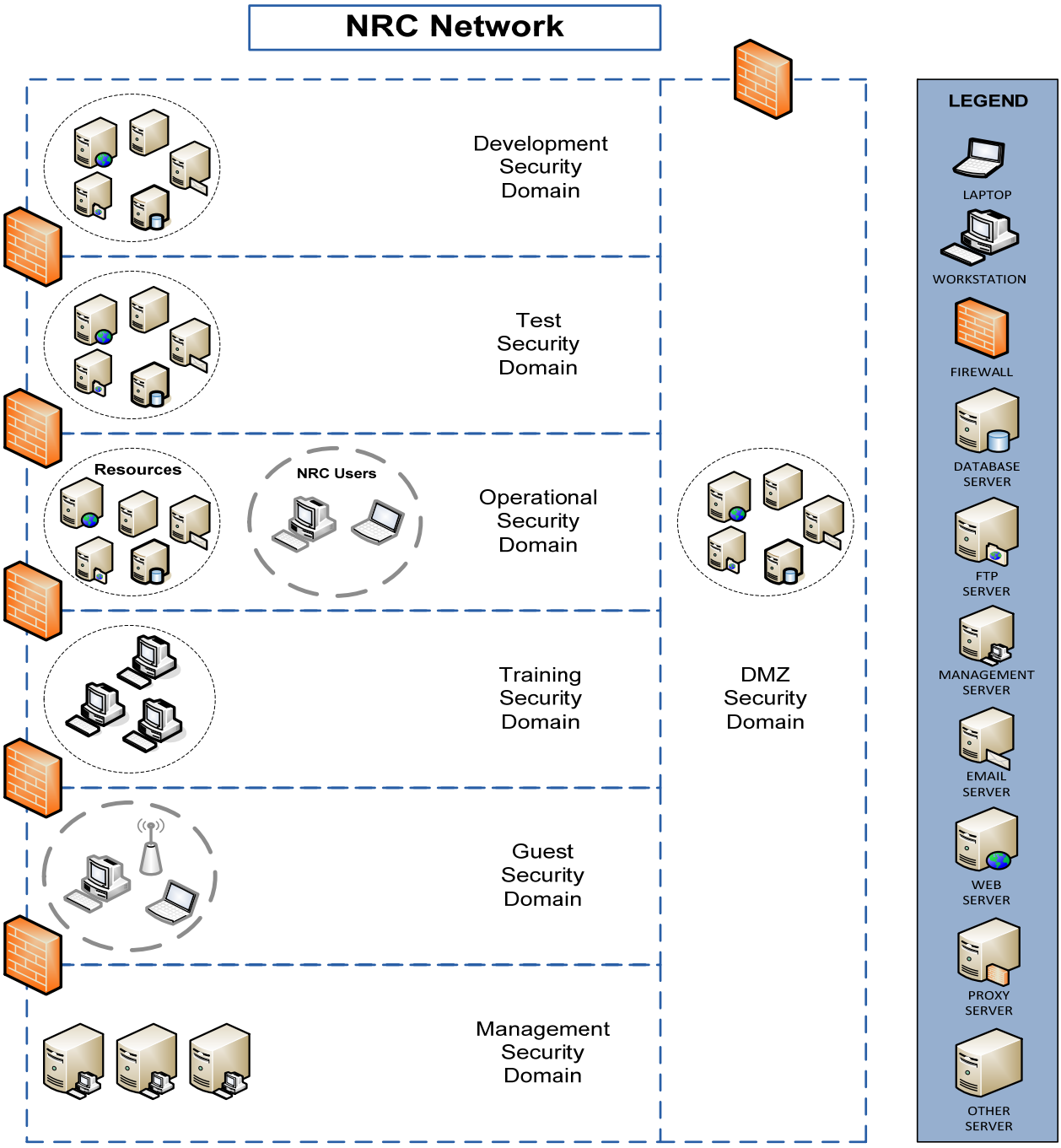


Figure 2.9-2: Network Segmentation

2.10 Network Structure

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

2.11 Network Devices and Technology

Network devices, technologies, and the capabilities they provide will be addressed in a future issuance of this document.

2.12 Wireless LAN Security

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

2.13 Transitioning to IPv6

Transitioning to IPv6 will be addressed in a future issuance of this document.

2.14 Network Resources

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

2.15 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 File Transfer Protocol [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.

2.15.1 Types of Interconnections

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

2.15.1.1 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.

2.15.1.2 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.

2.15.1.3 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.

2.15.1.4 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.

2.15.1.5 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.

2.15.1.6 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 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 approved for use under the NRC Bring Your Own Device (BYOD) program.
- 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.

2.15.1.7 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.

2.15.1.8 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.

2.15.2 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).
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).

2.15.3 Interconnection Security Agreement and Memorandum of Understanding/Agreement

The 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 Controls.” This standard defines the required NRC values for specific computer security controls identified in federal computer security control standards and guidance.
- Other Computer Security Office (CSO) standards (http://www.internal.nrc.gov/CSO/standards.html).

3.1 Cryptography

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

3.2 Information Sensitivity

Specific requirements are associated with specific information types.

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

  - Plaintext SGI must be processed by a physically separate network that has no connectivity with SUNSI networks.
  - Encrypted SGI is permitted to traverse SUNSI and public networks[2].

- Classified
  - Plaintext classified information is not permitted to traverse a public, SUNSI, SGI, or lower classification level network.
  - Plaintext classified information must be processed by a physically separate network that has no connectivity with lower level networks.
  - Encrypted classified information is permitted to traverse lower level networks using very specific requirements provided by the National Security Agency or in the case of sensitive compartmented information (SCI), by the Director of National Intelligence.

Full information sensitivity requirements will be addressed in a future issuance of this document.

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 Protocol Standard."

3.5 Network Access Control

Network access control (NAC) must comply with CSO-STD-2007, "Network Access Control Standard."

3.6 Network Types and Trust Levels

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

- All applicable network types must be identified for each network.
- Each network must be assigned a trust level based on the network's associated type(s) and specific attributes.

3.7 Interconnections

The following requirements must be addressed regarding network interconnections:

[2]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.

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

Appendix A, NRC Network Interconnection Diagrams, and Appendix B, 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.

3.8 Network Topology and Segmentation

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

- Each child network must be segmented from another child network regardless of child network type and trust level.
- Network domains must be segmented from each other (i.e., development, test, operational, training, guest, management, DMZ, and HPC).
- Communication between domains must be controlled. Details on the specific requirements and controls are provided in Section 4.1.1, Network Topology and Segmentation.
- The use of multiple layers of security must be used to provide defense-in-depth strategy for protecting networks, enclaves, and domains.
- 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 Topology and Segmentation.
- All network traffic from the NRC intranet destined for the Internet must be routed through a boundary protection device.

3.9 Network Security Protections

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

3.10 Wireless LAN Security

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

3.11 Transitioning to IPv6

All NRC networks 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).”

Details and requirements for specifically transitioning all NRC networks to IPv6 are provided in Section 4.2.3, Transitioning to IPv6.

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 Topology and Segmentation

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

4.1.2 Network Security Protections

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

4.1.3 Wireless LAN Security

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

4.1.4 Transitioning to IPv6

Transitioning to IPv6 will be addressed in a future issuance of this document.

4.1.5 Network Ports, Protocols, and Services

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

4.1.6 Network Monitoring

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

4.1.7 Physical Network Security

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

4.1.8 Interconnections

Specific requirements must be placed on an interconnection. 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 vary based on the actual interconnection itself and 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.

4.1.8.1 Interconnection Data Sensitivity and Information Exchange Security

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

- Interconnections that access non-public data must use authentication.
- Interconnections that process or exchange information that is SUNSI or more sensitive must use authentication and encryption in accordance with applicable CSO 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. 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, Requirements Definitions.

4.1.8.2 Interconnections Transiting over External Networks

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.

4.1.8.3 Interconnections Not Requiring a DAA Signed ISA

The following interconnections do not require an ISA:

- 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).

4.1.8.4 Interconnections Requiring a DAA Signed ISA

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 FTP or other general computational services).
- Interconnections between two networks, which are associated with separate systems, either internal or external to NRC.

4.1.8.4.1 Required Interconnection Information in an ISA

An ISA requires that the following be documented:

- Information sensitivity must be documented within the ISA and specific restrictions must be placed on the interconnection based on the overall information sensitivity.
- 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).
- 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).
- 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.
- 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 FTP server providing file sharing services).

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

- The specific requirements, restrictions, and security controls documented in the ISA must be reviewed and approved by the DAA.
- The ISA must be signed by the DAA before an interconnection is established.

4.1.9 Network Trust Levels

In order to be assigned a specific network trust level, the network must have the attributes specified in the sections below.

4.1.9.1 Trusted

Networks determined to be "trusted" by NRC must 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; and
- Be under NRC oversight, including NRC governing the facility, management, operational, and technical security controls.
- There is an expectation of strong security controls and hardening of the network.

4.1.9.2 Semi-Trusted

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

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

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

4.1.9.3 Restricted

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

4.1.9.3.1 Untrusted

Networks determined to be "Untrusted" 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.

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.

4.1.9.3.2 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 NRC Security Operations Center (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.

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).

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 Transitioning to IPv6

Transitioning to IPv6 will be addressed in a future issuance of this document.

4.2.4 Network Ports, Protocols, and Services

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

4.2.5 Network Monitoring

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

4.2.6 Physical Network Security

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

4.2.7 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, must be associated with a trust level. The network trust level is determined based on what considerations and security controls the network has in place. Table 4.3-1, Baseline for Network Type Trust Levels, identifies the 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

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
(NRC Special Purpose Networks Cont'd.)	*Guest Networks*	Untrusted	• Authorized to operate by the NRC DAA • Does not have an expectation of strong security controls and 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, “Home Wireless Networking Configuration Standard” or CSO-STD-1802, “Home Wired Network Configuration Standard” • 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-1801 or 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

Table 4.3-1: Baseline for Network Type Trust Levels

Network Type		Trust Level	Rationale
			security controls
(Telework Networks Cont'd.)	*State Government Telework Centers*	Untrusted	• Fall outside the purview of NRC oversight and have unknown security controls
	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

AP	Access Point
B2G	Non-Government/Private Organizations/Business-to-Government
BA	Business/Application
C2G	Citizen-to-Government
CM	Configuration Management
CSO	Computer Security Office
CSS	Cascading Style Sheets
D2T	Device-to-Telework
DAA	Designated Approving Authority
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
ESA	Enterprise Security Architecture
FTP	File Transfer Protocol
G2G	Government-to-Government
GHz	Gigahertz
HPC	High Performance Computing
I2G	International Entities/Organizations-to-Government
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
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
L2G	Licensee-to-Government
LAN	Local Area Network
LWAPP	Lightweight Access Point Protocol
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
NIST	National Institute of Standards and Technology
NMS	Network Management System
NPPS	Network Ports, Protocols, and Services
NRC	Nuclear Regulatory Commission
NRCEL	NRC Extended Licensee
OGC	Office of General Counsel
OMB	Office of Management and Budget
OSI	Open Systems Interconnection
PaaS	Platform as a Service
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
SCI	Sensitive Compartmented Information
SGI	Safeguards Information
SOC	Security Operations Center
SP	Special Publication
SSID	Service Set Identifier
STD	Standard
SUNSI	Sensitive Unclassified Non-safeguards Information
T2N	Telework-to-NRC Network
TCP	Transmission Control Protocol
TEMP	Template
TIC	Trusted Internet Connection
TTC	Technical Training Center
US-CERT	United States Computer Emergency Readiness Team
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

.

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 Service Set Identifier (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 Transmission Control Protocol (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

The NRC network interconnection diagrams 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 (hop-to-hop) 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.

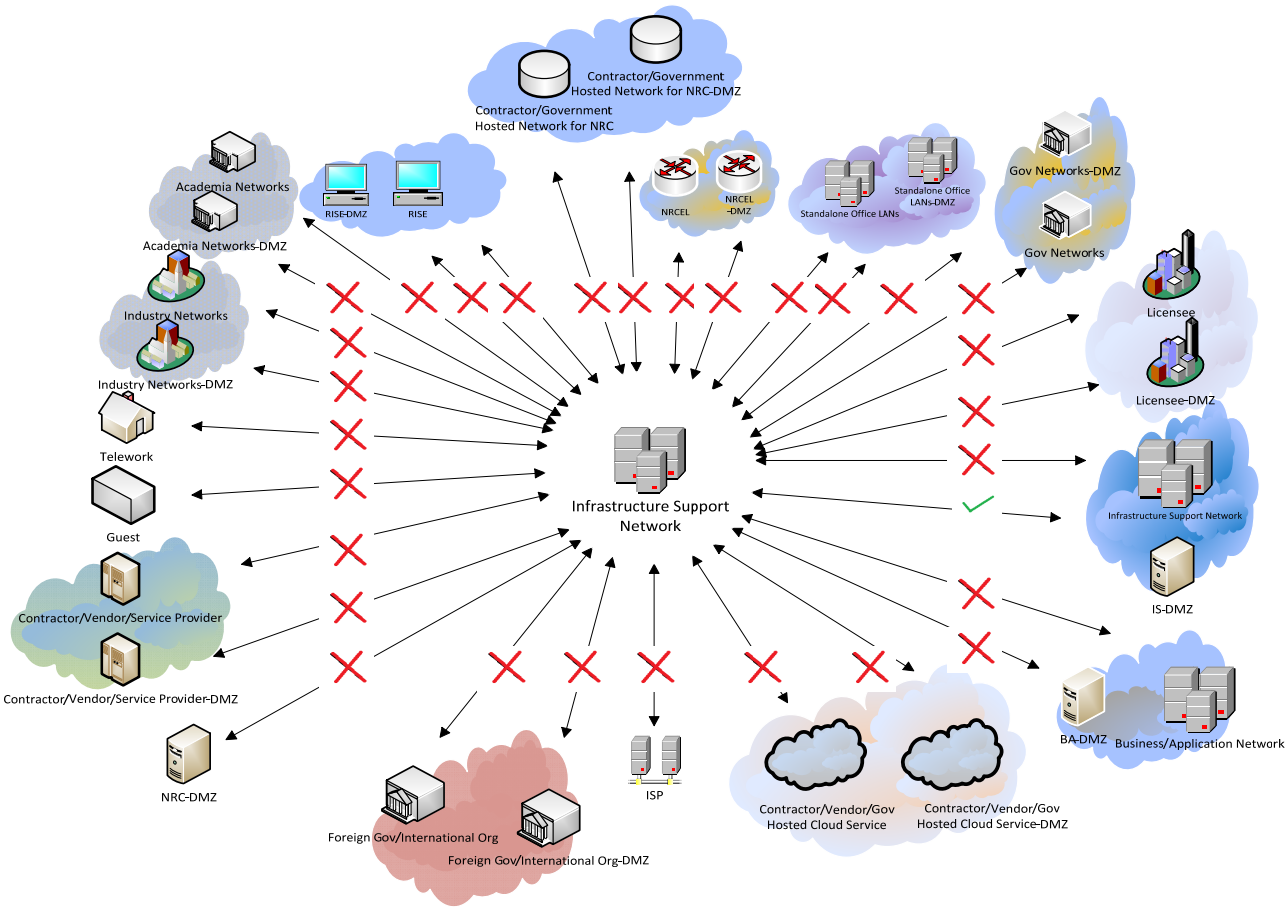


Figure A-5: Infrastructure Support Networks

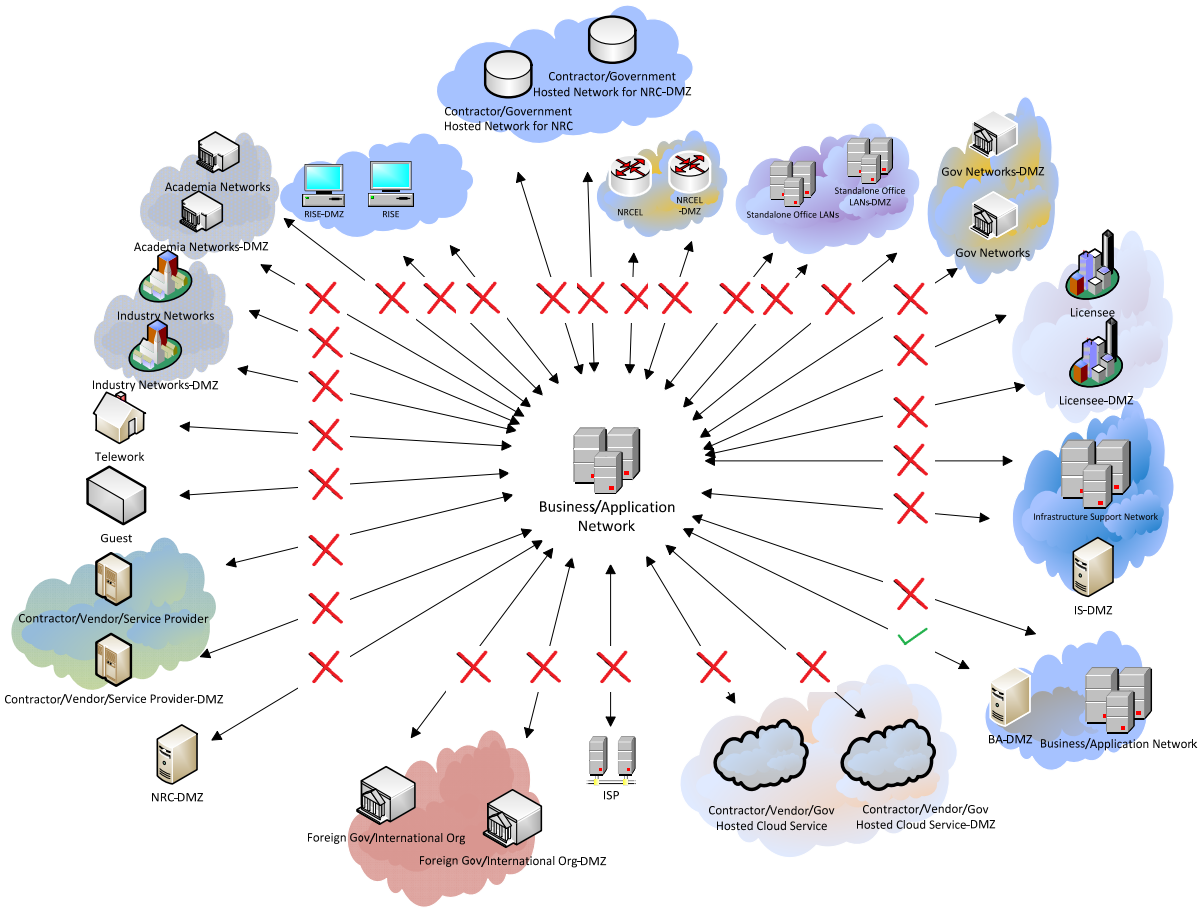


Figure A-6: Business/Application Networks

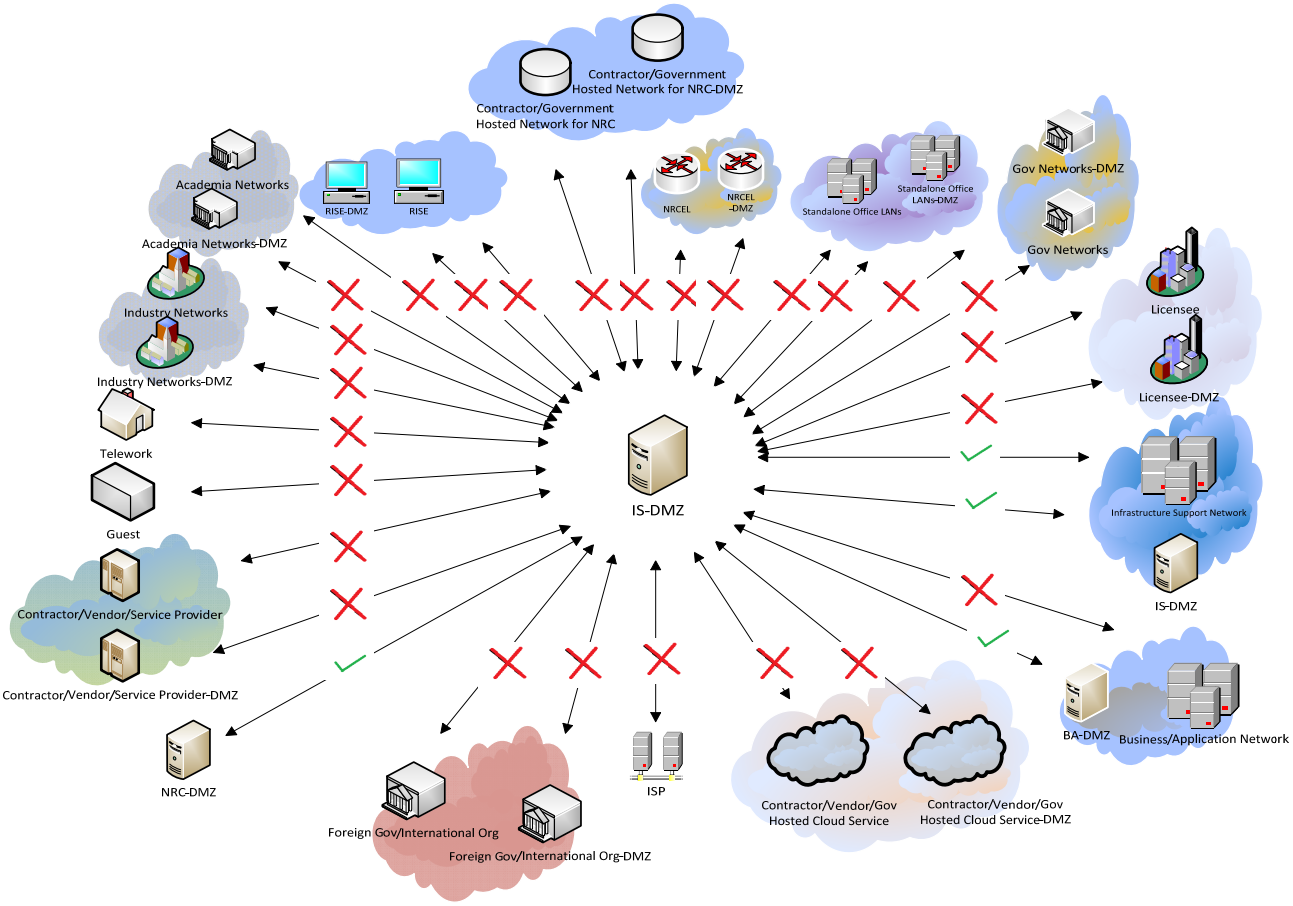


Figure A-7: IS-DMZ

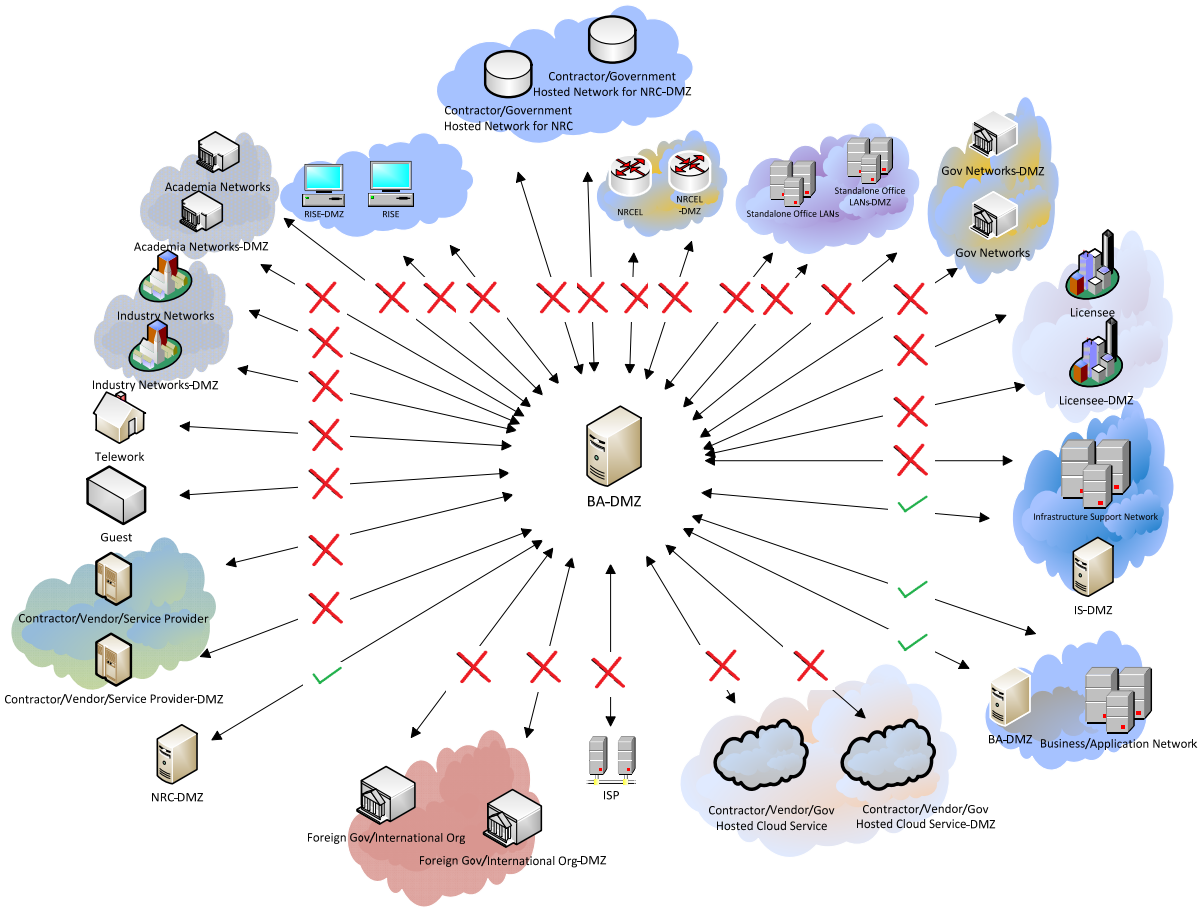


Figure A-8: BA-DMZ

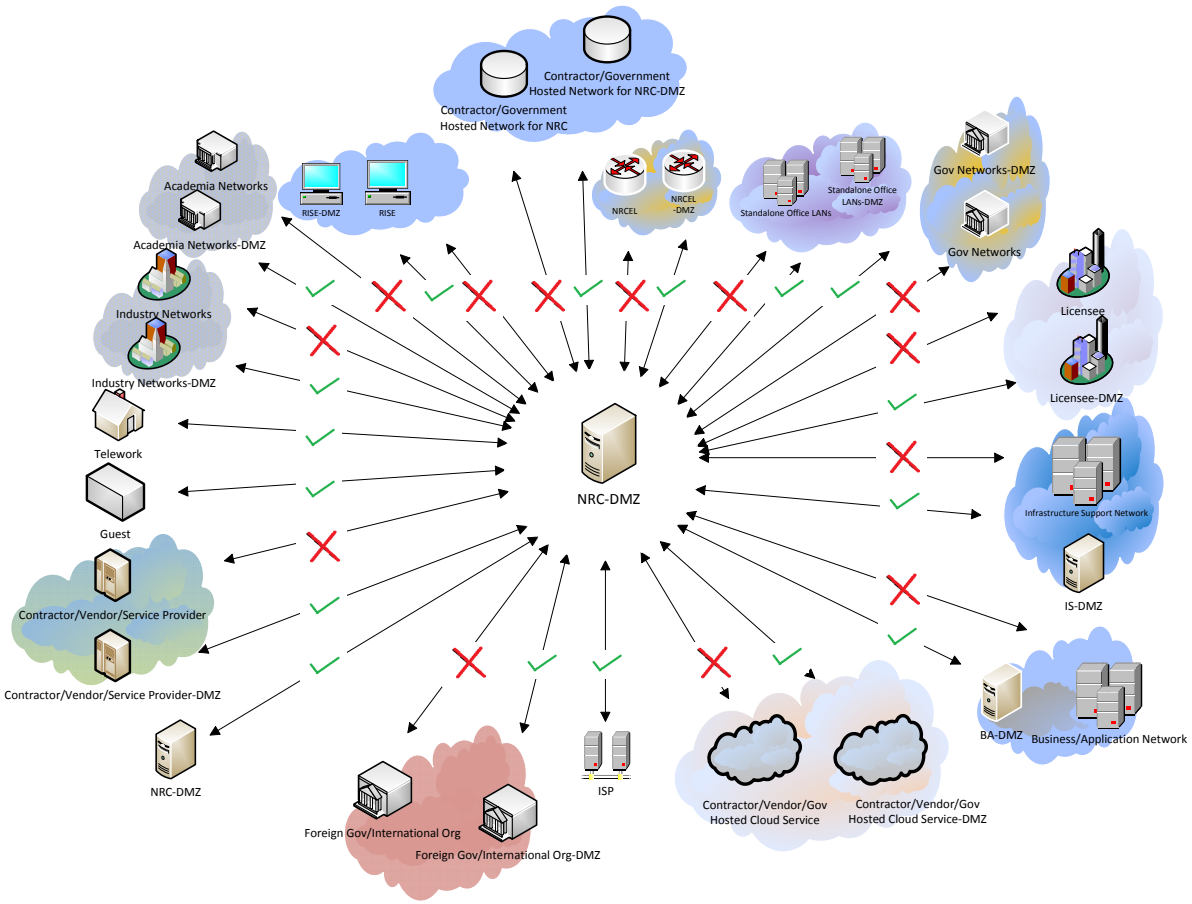


Figure A-9: NRC-DMZ

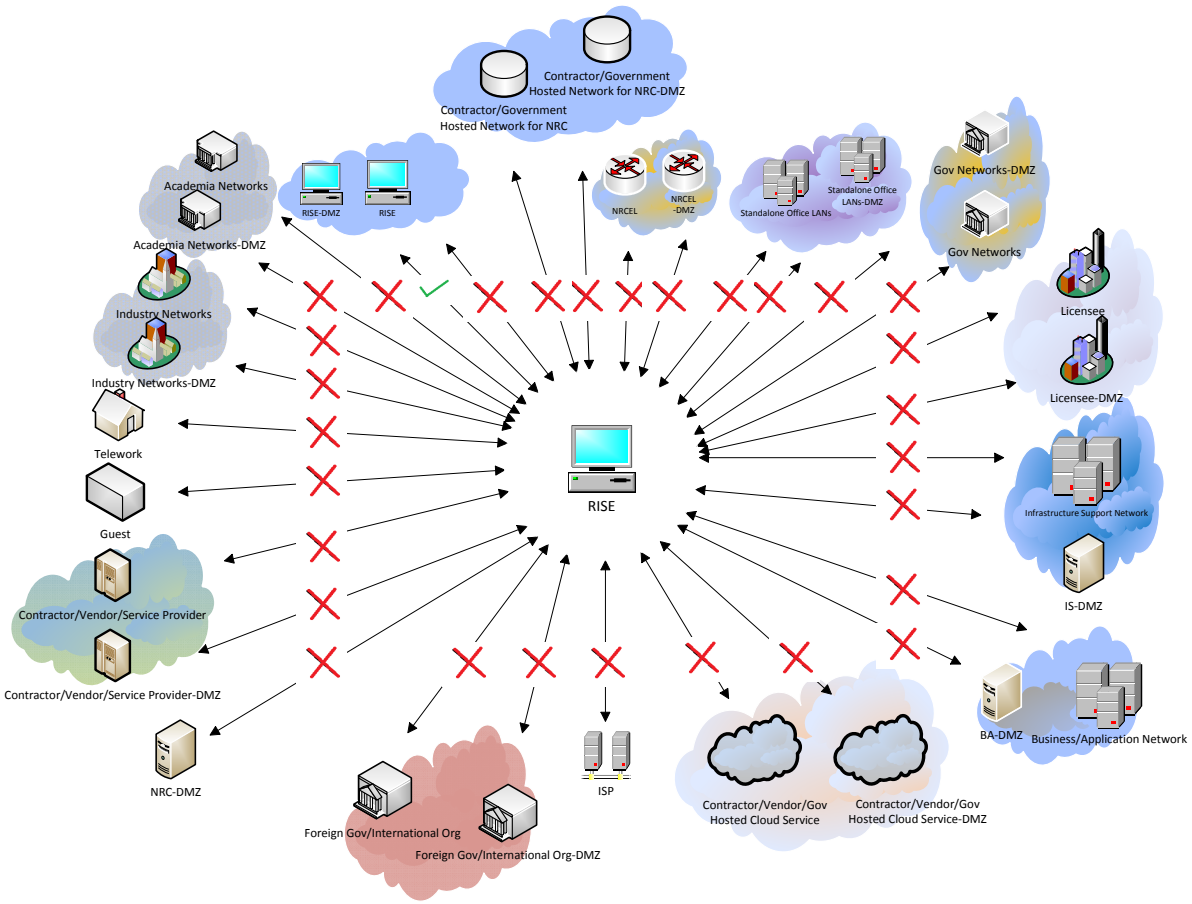


Figure A-10: RISE

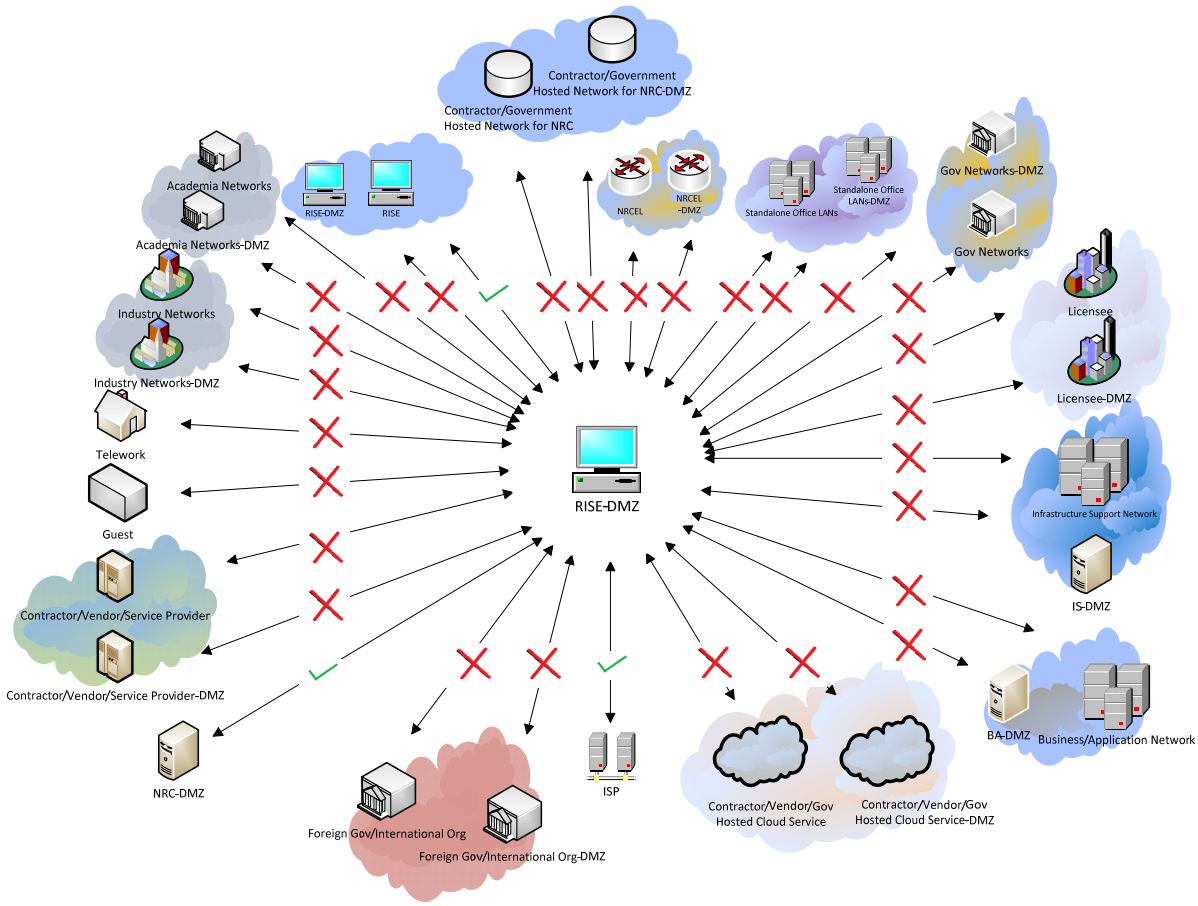


Figure A-11: RISE-DMZ

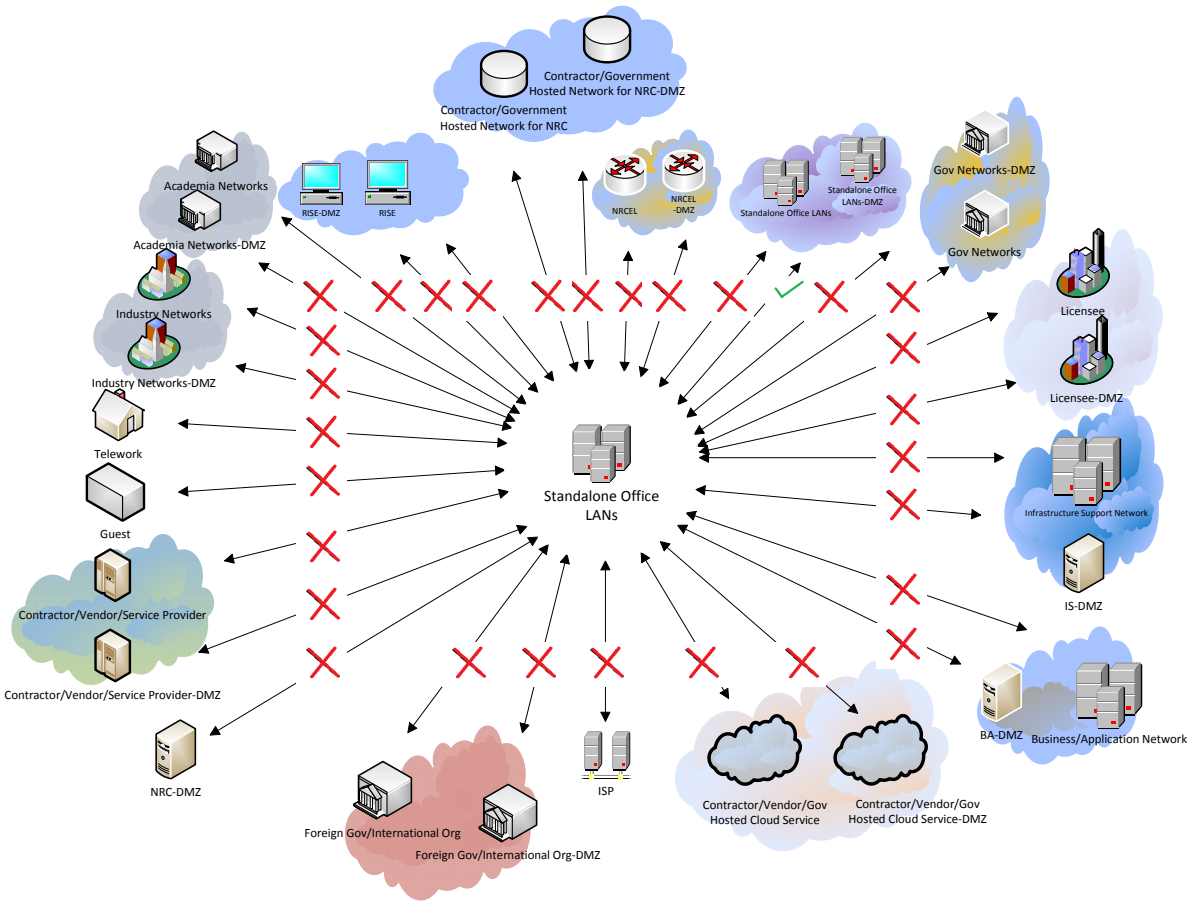


Figure A-12: Standalone Office LANs

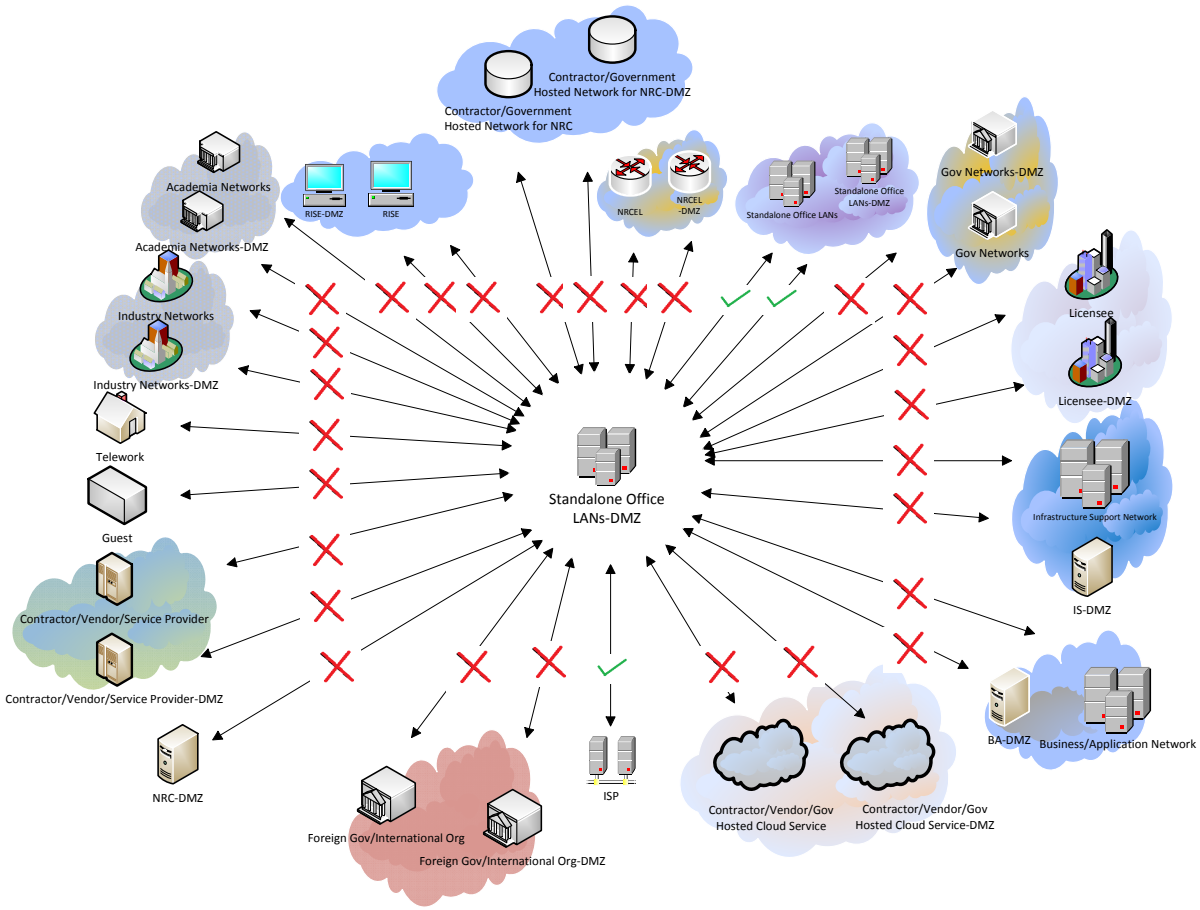


Figure A-13: Standalone Office LANs-DMZ

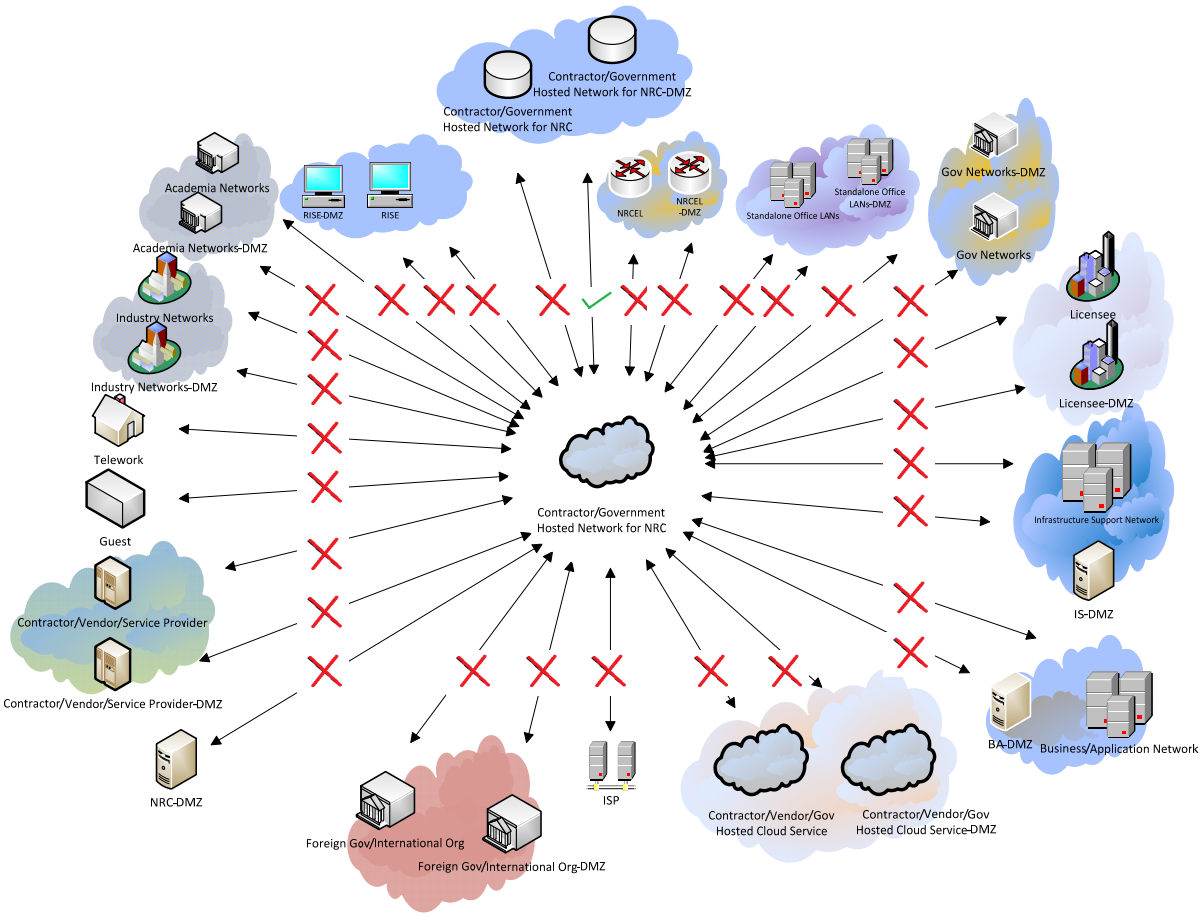


Figure A-14: Contractor/Government Hosted Network for NRC

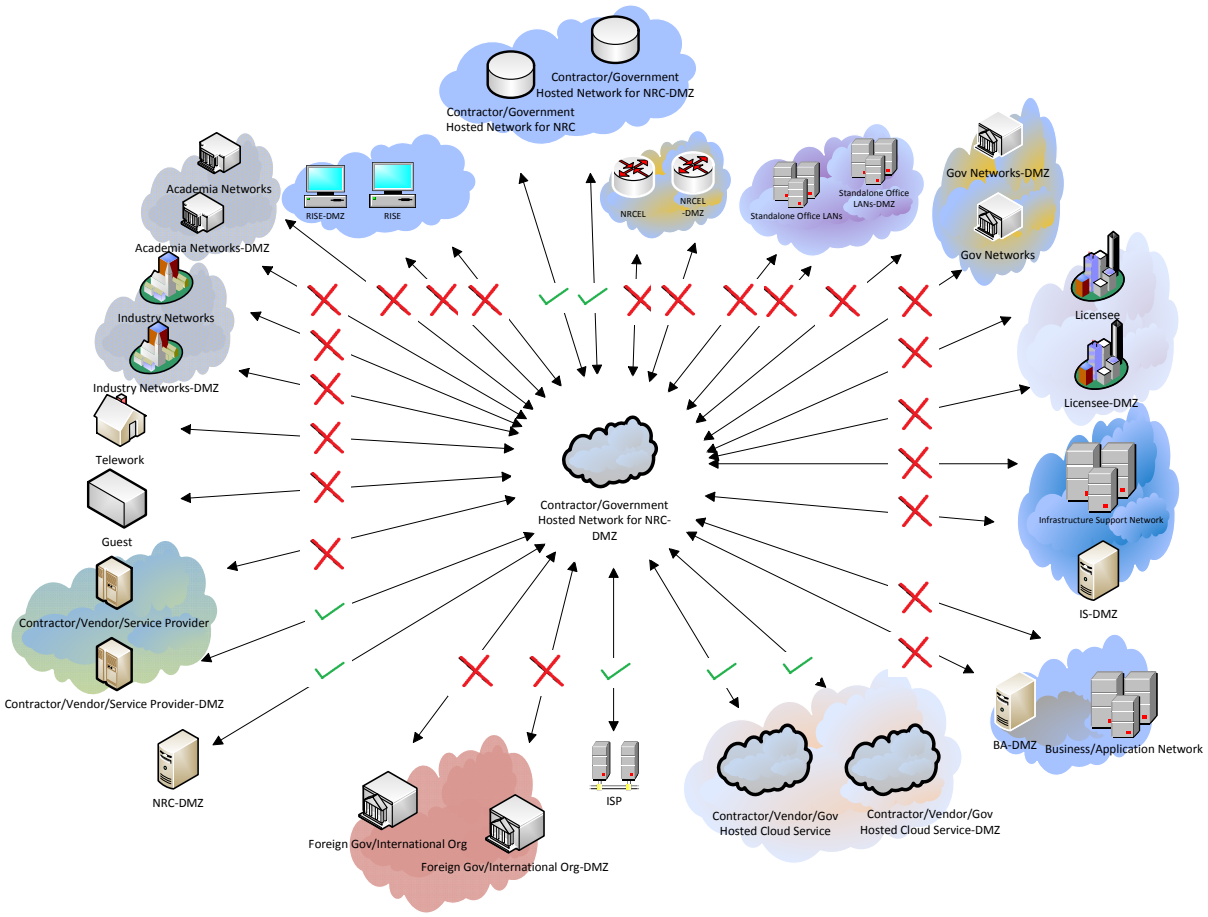


Figure A-15: Contractor/Government Hosted Network for NRC-DMZ

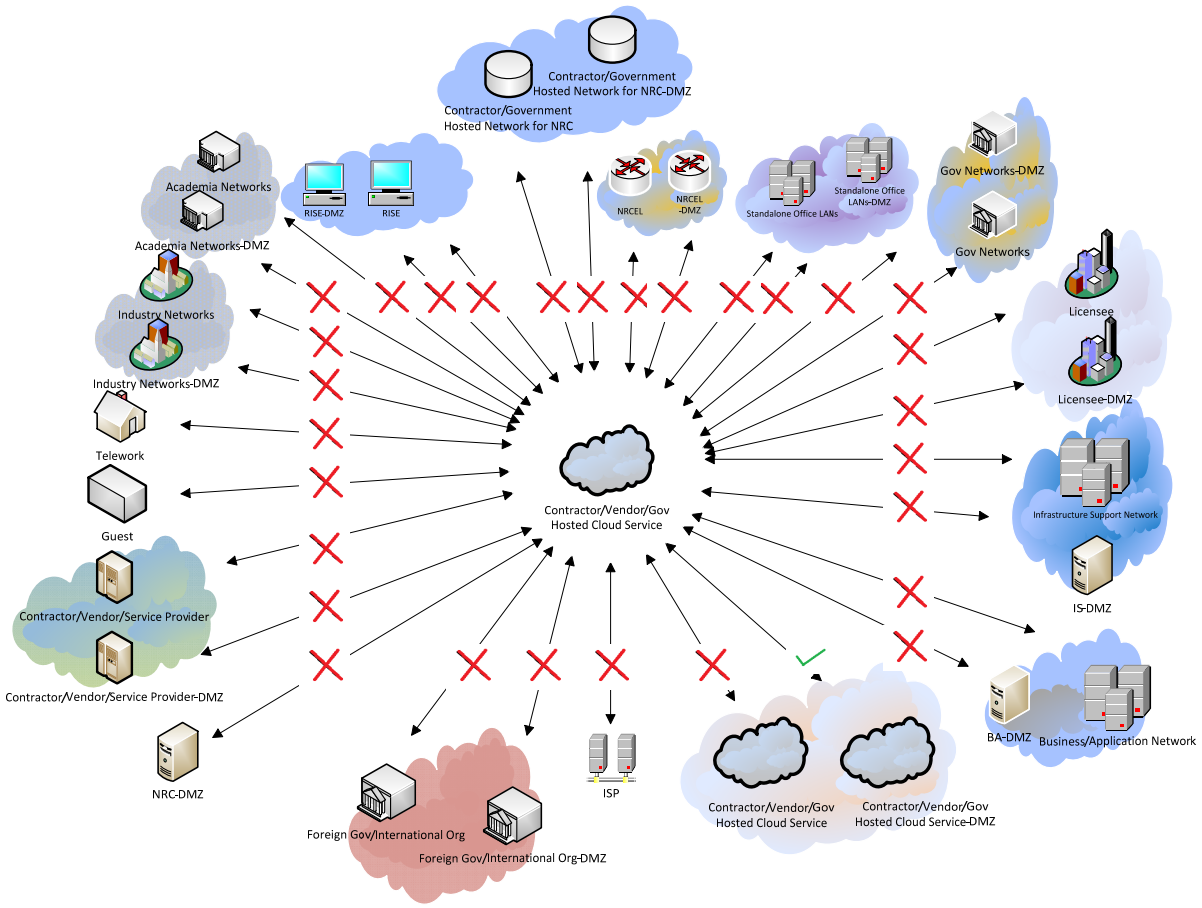


Figure A-16: Contractor/Vendor/Government Hosted Cloud Service

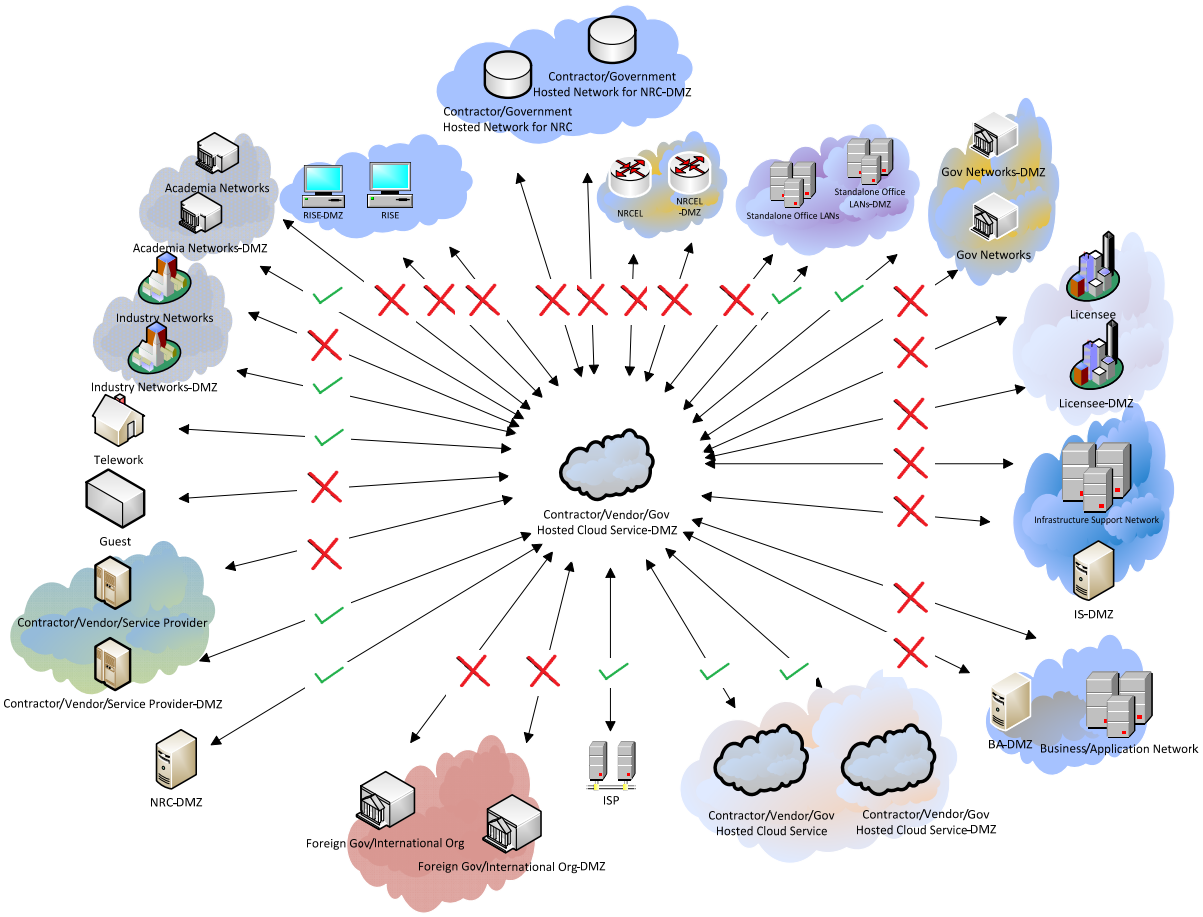


Figure A-17: Contractor/Vendor/Government Hosted Cloud Service-DMZ

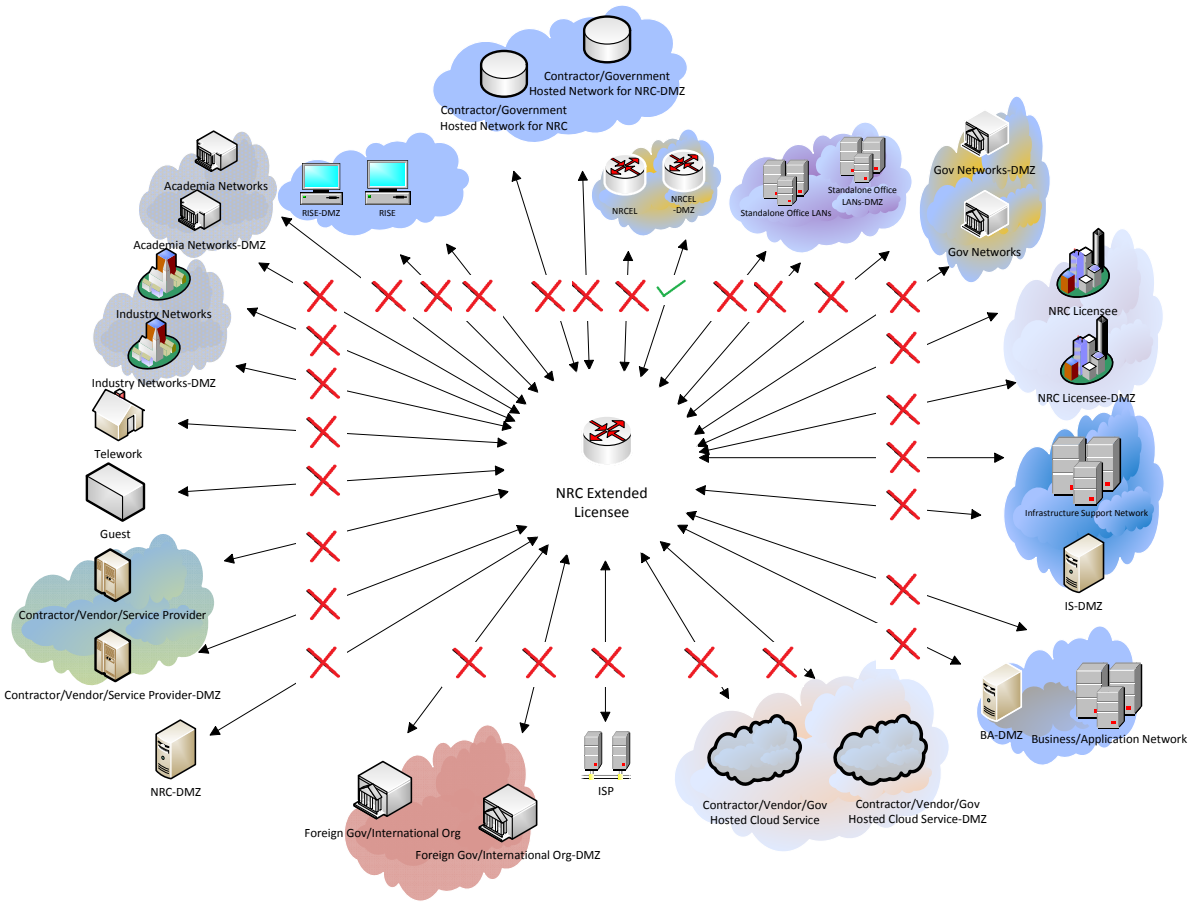


Figure A-18: NRC Extended Licensee

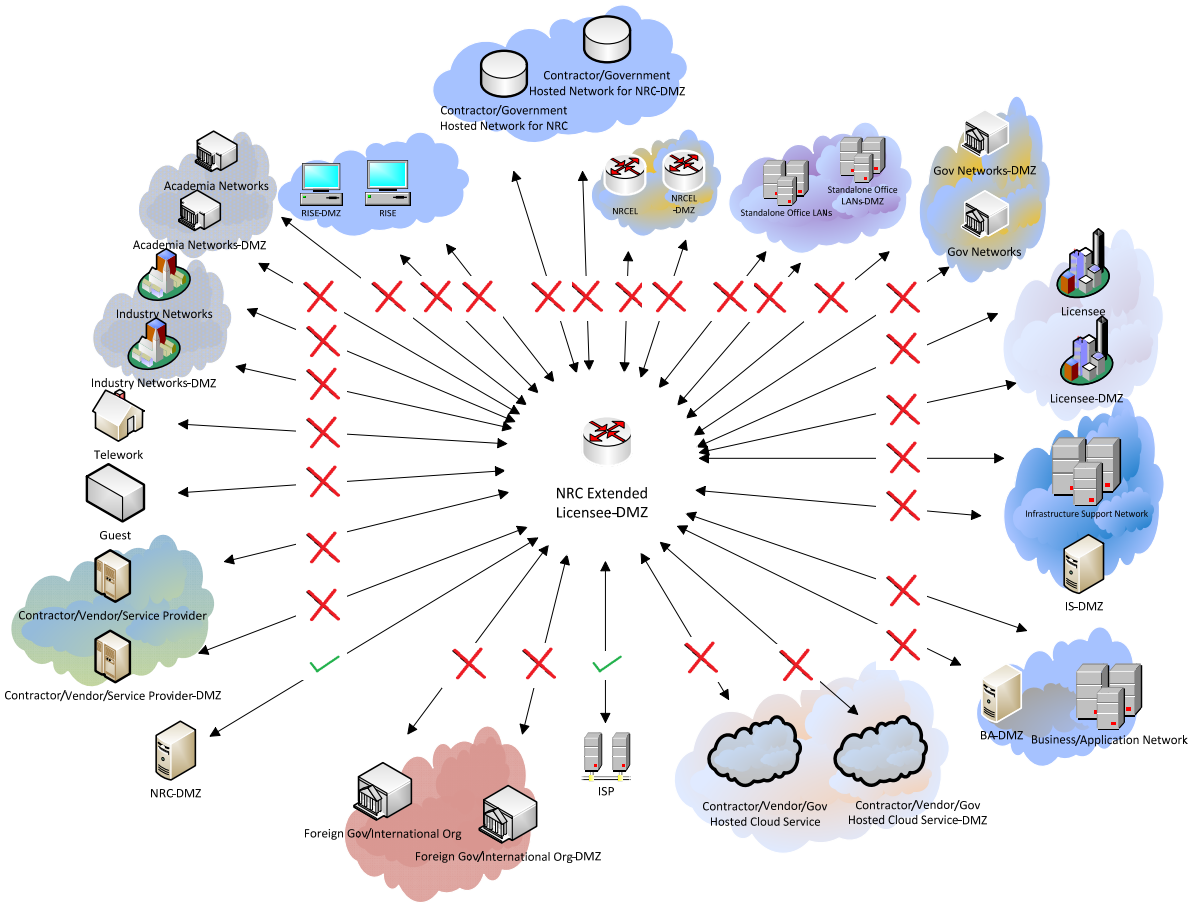
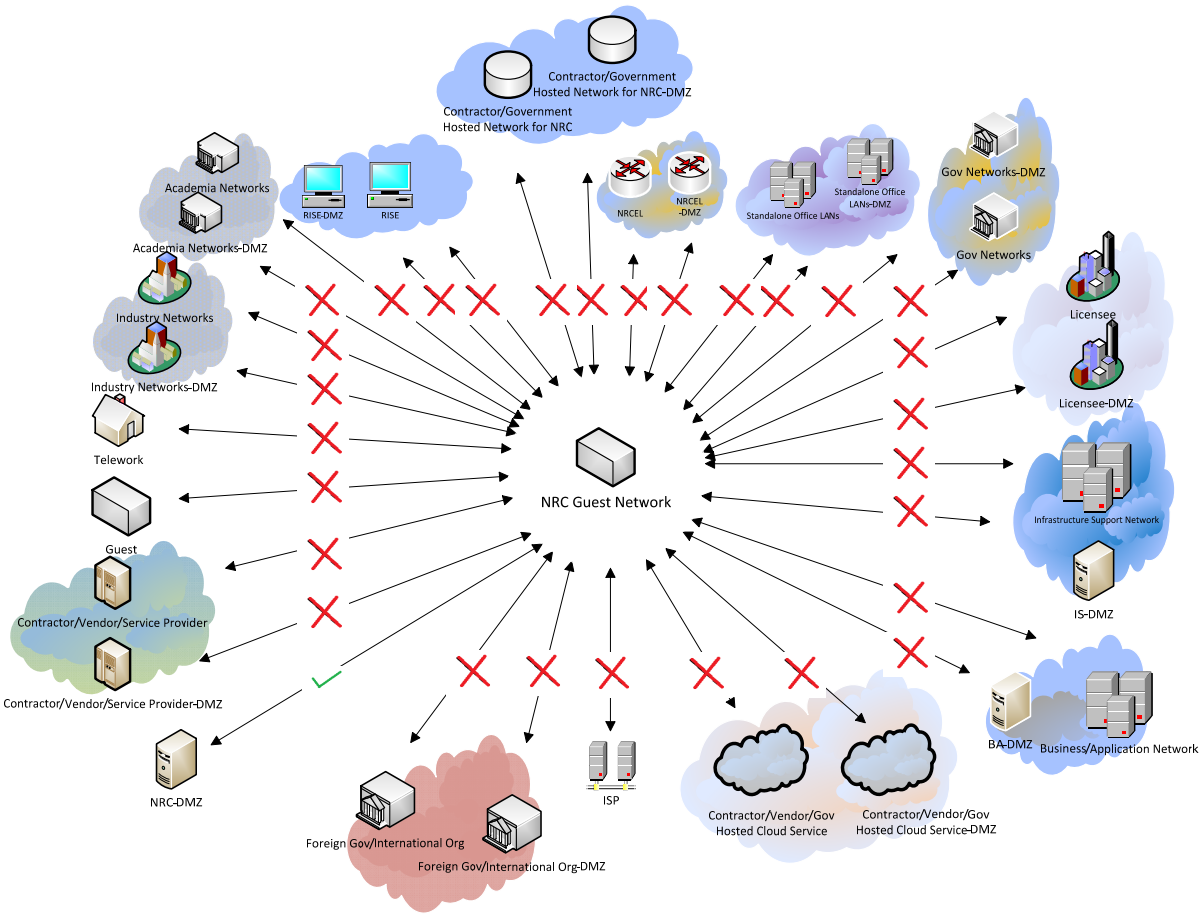


Figure A-19: NRC Extended Licensee-DMZ


Contractor/Government Hosted Network for NRC-DMZ
Contractor/Government Hosted Network for NRC
Academia Networks
Academia Networks-DMZ
RISE-DMZ
RISE
NRCEL
NRCEL -DMZ
Standalone Office LANs
Standalone Office LANs-DMZ
Gov Networks-DMZ
Gov Networks
Licensee
Licensee-DMZ
Industry Networks
Industry Networks-DMZ
Telework
Guest
NRC Guest Network
Infrastructure Support Network
IS-DMZ
Contractor/Vendor/Service Provider
Contractor/Vendor/Service Provider-DMZ
NRC-DMZ
Foreign Gov/International Org
Foreign Gov/International Org-DMZ
ISP
Contractor/Vendor/Gov Hosted Cloud Service
Contractor/Vendor/Gov Hosted Cloud Service-DMZ
BA-DMZ
Business/Application Network

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. Just because a connection is permitted does not mean that any connection can be made between the networks. The specific conditions associated with the interconnection must be met as well. 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 (hop-to-hop) 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, in which each specific network may potentially interconnect.
- 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
NRC WAN		
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
Industry Networks-DMZ	No	BA
Industry Networks -DMZ	No	IS-DMZ

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
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
ISP	No	BA
ISP	No	IS-DMZ

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
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
Academia	No	Guest
Academia-DMZ	No	Standalone Office LANs
Academia-DMZ	No	Standalone Office LANs -DMZ
Academia-DMZ	No	Guest

Table D-3: External Networks

Network Type	Interconnection Permitted (Yes/No)	Network Type
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

CSO-STD-4000 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
04-Jun-14	1.0	Initial Release	CSO web page	As needed