SECURE REMOTE COMPUTING (SRC)
SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 5

29 July 2011

Developed by DISA for the DoD

This page is intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

This page is intentionally left blank.

1. INTRODUCTION

This Secure Remote Computing (SRC) Security Technical Implementation Guide (STIG) provides guidance for secure configuration and usage of devices used for remotely accessing Department of Defense (DoD) networks. This document defines remote access as the ability of an organization's users to access its non-public computing resources from locations other than the organization's facilities or physically-controlled space. Policies have been removed from this main document and the text is now meant to provide an overview of remote access technologies.

Policies are applicable to network devices such as remote access gateways and appliances. Access environments include teleworking from home networks, government telework centers, hotel networks, airports, and mobile computing. Remote endpoint devices may include desktop computers with full operating systems (OSs), thin and ultra-thin clients with limited OSs, virtual computing applications, and a host of mobile devices. Guidance for remote access using mobile and wireless devices is located in the Wireless STIG. Depending on their access permissions, users may use these devices to read and send e-mail, access web applications and portals, review and edit documents stored on file servers, or perform a host of other tasks. The applications accessed via a secured remote access session are not within the scope of this document. This document provides an overview of remote access and mobile computing concepts, vocabulary, and general compliance requirements.

1.1 Purpose

The purpose of the SRC STIG is to provide additional guidance, specific to remote computing environments, above and beyond what is currently required by other DoD STIGs and applicable DoD policy. Remote access network and endpoint devices must provide secure, obtainable, and reliable services and data to all customers, DoD users. The purpose of this STIG is to assist sites in meeting the minimum requirements, standards, controls, and options for secure remote computing.

1.2 Authority

DoD Directive (DoDD) 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks Defense Information Systems Agency (DISA) to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA". This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in this STIG provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance Categories I through III, all DoD Instruction (DoDI) 8500.2 IA controls need to be applied to all systems and architectures.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Manager (IAM) will ensure compliance with the security

requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

The Joint Task Force-Global Network Operations (JTF-GNO) has also established requirements such as timelines for training, verification, installation, and progress reporting. These guidelines can be found on their web site: https://www.jtfgno.mil. Initially, these directives are discussed and released as Warning Orders (WARNORDs), and feedback to the JTF-GNO is encouraged. The JTF-GNO may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

NOTE: Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD customers.

1.3 Scope

This document applies to all DoD-administered or managed data center networks, assets, and security domains. The requirements set forth in this document are designed to assist IAMs, Information Assurance Officers (IAOs), and System Administrators (SAs) in support of protecting DoD network infrastructures and resources.

1.4 Vulnerability Severity Code Definitions

Table 1-1 provides the vulnerability severity codes and its definitions.

Table 1-1. Vulnerability Severity Code Definitions

Mission Assurance Code	Definitions
Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

1.5 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The Non-classified Internet Protocol Router Network (NIPRNet) Uniform Resource Locator (URL) for the IASE web site is at the following site: http://iase.disa.mil/.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

This page is intentionally left blank.

2. SECURITY CONSIDERATIONS FOR REMOTE ACCESS AND TELEWORK

Telework and mobile computing has become a necessity for most organizations. Telework policies are in place at the Federal and DoD levels which mandate that organizations facilitate remote workers to the maximum extent possible. However, opening the network to outside access presents many security risks which must be addressed through use of technological controls and user training. User training is particularly critical since not all risks can be mitigated using technological controls. The policies in the remote access STIG documents implement DoD policy and industry best practices in the following areas impacting remote network access.

- Remote access communication (e.g., wireless, broadband)
- Computing environment for the remote worker (e.g., home, hotel, apartment, or kiosk)
- Availability of products with features which are required to meet DoD security policy
- Network access control
- Logical policy enforcement
- Disaster recovery and continuity of operations
- Hosting of guest or visiting users from other authorized organizations
- Extranet access
- Scalability

To be used securely and implemented effectively, remote access solutions must integrate these general functions:

- Secure endpoint configuration using sound best practices for OS and application security;
- Network protection that detect the security of an endpoint prior to authentication;
- Network architecture that protects system and resources using access control policy based on the privileges allowed for the specified user and endpoint;
- Integration with network services such as Active Directory, Authentication, Authorization and Accounting (AAA), and proxy servers; and finally,
- Quality of service, ease of connection, and reliability/availability.

2.1 Purposes of Remote Access

Remote access security policy, like other information assurance policy, depends on the sensitivity, mission criticality, and risk presented by the type of connectivity and the purpose of the remote access. Remote access can be divided into three types of access based on the purpose of the access. Differentiation based on these access types or levels will help clarify the discussion of DoD remote access policies. The three types are as follows:

- **Administrative Access** – Remote users who will be connecting to a DoD core network to perform any system administration duties to include troubleshooting, configuration changes, and reviewing any system or configuration data, regardless of system type. This type of access will require the most stringent security controls and users must use government-owned or controlled devices. Administrative Access will employ encryption.

- **End-User Access** – Remote users who will be using network services or accessing, downloading, or uploading data. The End-User remote access level requires that users do not make any system configuration changes or view system configuration information. This type of access will require medium security controls on the remote system and users must use government-owned or controlled devices. End-User Access includes customers who access, change, or download Government data via Telnet and other clear-text terminal emulators. End-User Access will employ encryption.

- **Limited (General) Access** – Remote users who are viewing content or sending e-mail but are not altering or entering official Government data (e.g., accessing a DoD web site). This type of access will require minimum security controls and users may use non-government-owned devices with Designated Approval Authority (DAA) approval for this type of access. This type of access relies more heavily upon the network infrastructure and hosting server for security protections and authentication, because there is no assurance that the connection endpoint will be compliant with OS and other DoD configuration requirements.

In general, requirements in this checklist are required for Administrative Access. For End-User Access and Limited Access, checklist requirements must be implemented to the fullest extent possible for End-User and Limited Access. However, systems will be secured at the Administrative Access level. If the site allows Administrative or End-User access to a system, the remote device must be controlled or owned by a Government entity to allow for confiscation and review at any time. This requirement allows for the review of security vulnerabilities and checklist requirements, as well as determination of possible spillage or harm to the network infrastructure. These requirements pertain to any system within an enclave, excluding those resources specifically designed for public access (e.g., resources residing in a De-militarized Zone (DMZ) such as a web server).

2.2 Methods of Remote Access

Although remote access can mean different things depending on the technology (including the various forms of virtualization) and functionality used, there are two general methods of remote access – remote control and remote node.

Using the remote desktop control method, the remote user uses his endpoint to connect to a network-attached host computer located on the home organization's network. The user remotely controls this host computer to access network resources. For the remote control method, only keystrokes and mouse movement are sent from the remote machine, and only screen changes are sent back to the remote user's computer. All application processing takes place in the local computer. For example, Windows Remote Desktop is actually the Windows-based Terminal Server, which uses the Remote Desktop Protocol (RDP) to exchange only keystrokes and screen changes. If these applications are used, they must be configured in compliance with the applicable Windows STIG. Methods of remote access that allow users to bypass the network Intrusion Detection System (IDS) or network access controls to directly connect to their desktop personal computer (PC) are not authorized for use on the DoD enclave.

Using the remote node method, the remote endpoint connects to the network and becomes another node on the network. All requests and responses cross the communications connection, using encapsulated Transmission Control Protocol/ Internet Protocol (TCP/IP), to the home organization's network (typically, via an Internet or dial-up connection). All data flows to the remote machine as if it were a local PC. The goal is to give the same connectivity and access to enterprise resources as if the users were in the office.

With high-speed connections, remote node is the preferred method; however, if an enormous amount of data on the network must be processed by a remote user who has a slow connection or device, the remote control method should be used.

2.3 Remote Communications

Remote access, mobile access, and telework may use a number of different communications methods. These connections primarily use a virtual private network (VPN) client to create an encrypted "tunnel" into the DoD network or even use the older method of dial-up telephone to directly connect to a remote access server on the network. These methods include:

- Broadband networks (such as cable modem, digital subscriber line (DSL), satellite, and wireless broadband);
- Dial-up connection using a modem and telephone line;
- Guest access using a DoD host network;
- Guest access using a non-DoD network (such as an authorized telework center, home network, or contractor network); and
- Public wireless hotspots in hotels, restaurants, or airports (as addressed in the Wireless STIG).

Use of each connection method and environment has different security and technological implications. Vulnerabilities and mitigations for each method are discussed in subsequent sections and throughout this document.

In general, broadband refers to Internet access telecommunications signaling methods used for high-speed Internet connections. For the purpose of this document, the definition of broadband

communication is any form of transmission other than normal dial-in methods. Though there is no set bandwidth threshold for a communication method to be considered as broadband, generally, this term is used for methods capable of transmitting data at speeds exceeding one Megabit per second (Mbps).

In recent years, there has been an increasing use of wireless technologies for remote access. This access may take several forms. Use of public hotspots and home wireless networks for access to the public network must be addressed in each site's remote access policy. Some organizations are deploying or testing wireless broadband network connections. Additionally, wireless broadband can provide either endpoint access directly to the Internet or provide a backhaul for connecting wired or wireless Local Area Networks (LANs) across a campus or metropolitan area as an alternative to copper or fiber-based solutions.

The risk of exposure to vulnerabilities, malicious attackers, and opportunistic individuals has significantly increased with the use of "always–on" technologies such as broadband. Users are connected for much longer periods and these connections often use static IP addresses provided by Internet Service Providers (ISPs), providing a "fixed" target for the attacker. Furthermore, the additional speed and bandwidth of the connection makes it an attractive alternative over dial-up to not only the remote user, but the attacker as well. The threat of attack is the same for broadband communication as it is for any LAN. Because of its open architecture, connections to the Internet are inherently vulnerable and are subject to scans, probes, worms, Trojans, denial of service, spoofing, Zombies, etc. Therefore, it is imperative that any broadband connection be as secure as possible prior to connecting to a DoD network or resource.

Though rapidly diminishing in use, dial-up connections using modems are still widely used in the Government. The analog modem uses a standard telephone line to connect to an ISP, communications servers or terminal host adapters, and network access servers. Since long-term connections are not practical for dial-up access, this type of connection is normally not active for long periods. This provides an inherent security advantage over broadband connectivity due to this short-lived connection as well as dynamic IP addressing. When remote users dial into a device, they are usually provided a dynamic IP address as opposed to static IP addresses, making them a less attractive target for an attacker. In addition, they are not connected as long as a broadband remote user and are, therefore, not exposed to security threats for extended periods. However, these connections tend to be slow and users are likely to adopt a faster method of connectivity, if it is available.

Although the risks are greater with high-speed connections than with dial-up, those risks can be minimized with security measures such as personal firewalls, web browser security settings, OS secure configurations, anti-virus software with updated signature files, and encryption.

2.4 Securing Network Services

The sharp increase in telework, remote, and mobile computing has important implications for general Network Access Control (NAC) and security. High-speed broadband communications are now easily available using notebook PCs, desktop PCs used at home, handheld personal electronic devices (PEDs), telephones (such as, regular, cell, voice over IP (VoIP)), and desktop

videoconferencing. DoD end-users increasingly demand the same level of access available within the physical perimeters of the traditional office. This makes the old access control model of using simple scripts and profiles increasingly cumbersome for network administrators. The need for remote administration, contractor, inter-agency access, and an ever broadening wireless/mobile world also increases the need for more dynamic access control models. These diverse endpoints and multi-level access needs also demand an increase in security controls at the network perimeter and application levels.

Because the public network infrastructure is used to deliver remote access services to DoD users, these users and endpoints seeking access must be treated as untrusted. With the increasing use of these same endpoints for access over both secure and non-secure networks, both internal and external clients must be treated as untrusted. This method actually serves to simplify access control and endpoint management. As depicted in the Network Infrastructure STIG, access to restricted servers/databases is logically separated from wired endpoints and from publicly-accessed hosts. Both remote and hard-wired users must provide stringent access credentials prior to traversing this internal "resource perimeter". Using this paradigm, it is now possible to separate network access from resource access with two implications: Physical locations can become increasingly transparent and the Federally-mandated goal for DoD networks to provide emergency and guest access is also increasingly achievable.

The basic requirements for NAC are the identification and authentication of the endpoint device; identification and authentication of the end-user; and the inspection and remediation of the endpoint device to determine if it matches established entry criteria. Only after successful completion of this process should users be allowed access to authorized resources.

2.5 Remote Access Architecture

Regardless of the remote access method, connection method, or telework environment, enclave protection mechanisms must be in place to ensure security within specific security domains and across the DoD network backbone. The Enclave Security STIG and the Network Infrastructure STIG give details regarding the architectural components that must be in place to secure the infrastructure. These devices, their functions, security, and placement requirements are detailed in the aforementioned STIGs. This section provides a summary of these components and policy requirements specific to sites supporting remote access functionality.

The most critical part of a remote access solution is to create a centralized point of access and authentication close to the network edge. Both the accessing device and user must be verified prior to allowing access to network resources on the internal LAN. As shown in Figure 2-1, the remote access servers must be installed outside of the secured private network. A centralized access point, controlled by a compliant firewall is a sound best practice. Only services that are absolutely needed for end-users to conduct business should be allowed through the firewall from the central point of access. This architecture will prevent direct host-to-host communication between protected network resources and external entities. This type of direct connection could grant an attacker access to protected resource by creating a bridge to the internal LAN. This architecture also prevents direct remote access to the user's wired desktop from his mobile device, which also presents a potential back door into the network.

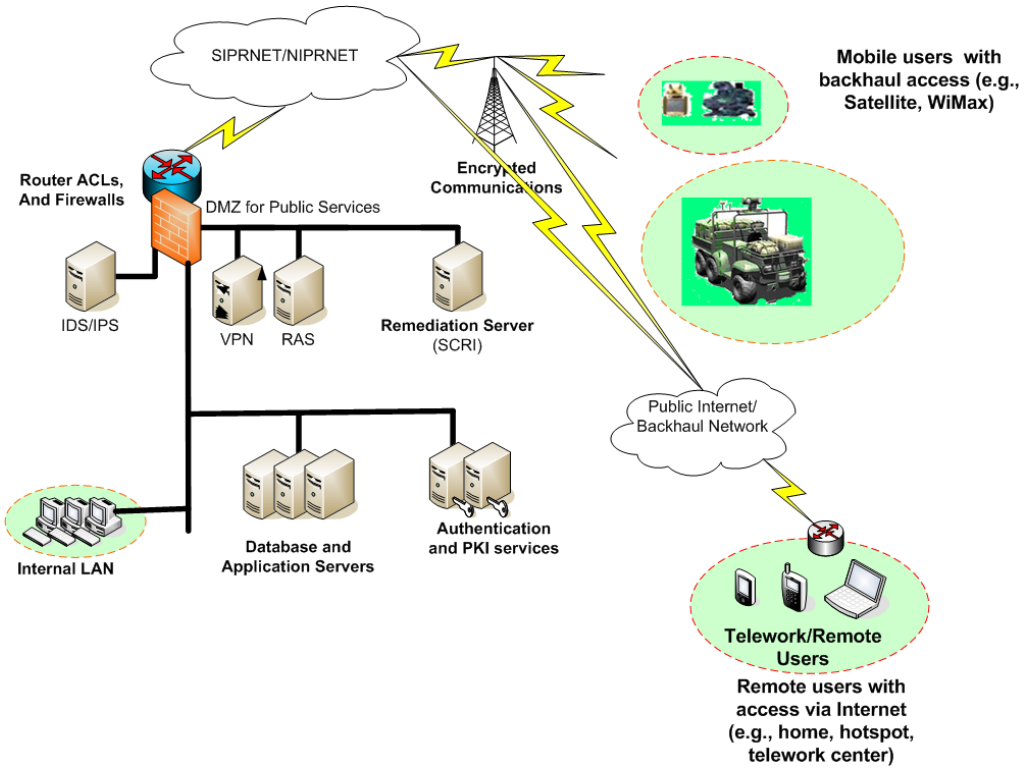

Figure 2-1. Sample Remote Access Architecture

The preferred solution for remote access control is to use a centralized policy manager to implement access control for all remote access connections (e.g., VPN or dial-up). This can be accomplished by placing the remote access server either in the DMZ or within a screened subnet along with the VPN gateway. The screened subnet architecture ensures that only authorized users are permitted access to the internal base network while providing protection for the remote access server. In addition, end-users should not have access to any management or configuration functions of the remote access server. This can be accomplished with the firewall or screening router by denying access to hosts within or outside the private network.

In accordance with the Network Infrastructure STIG, at a minimum, the enclave will include the following protections:

- An IDS at the enclave perimeter. To enable remote access, these technologies monitor content of network traffic for malicious code and unauthorized activities. Additionally, IDS technologies must block traffic performing unauthorized functions or carrying infected files or programs.

- Router Access Control Lists (ACLs) based on a policy of Deny by Default.

- An application-level firewall: Blocks unauthorized traffic from entering servers from the Internet.

- An internal network IDS.

- Vulnerability Management: Periodic assessment of security stance of the network.

Any access to the site from outside of the enclave must pass through this minimum architecture without circumventing the security controls in place. However, sites that allow remote access to the enclave must also have the following network architecture protections in place.

- Policy Management: Enforces security rules and regulations of information technology systems, including configuration of every remote endpoint device used by teleworkers.

- Remote Access Server (RAS: Provides dial-in capability for the remote access user. Can be integrated with the VPN gateway or router.

- VPN Gateway: A secure network for an organization that transmits data through the public network.

As shown in Figure 2-1, the Network Infrastructure STIG requires the RAS and VPN gateway devices to be installed in a DMZ or screened subnet. This architecture protects these servers from direct access to untrusted networks while making policy enforcement and authentication resources possible.

This page is intentionally left blank.

3. ASSESSMENT, ENFORCEMENT, AND REMEDIATION SERVICES

Logical access control to DoD networks must involve processes for device authentication and authorization as well as user authentication and authorization. Currently, user authentication and authorization is exercised at varying levels of assurance on DoD networks. However, although network security policy exists and some assessment tools are available, these policies and assessment tools are not yet integrated and leveraged for the purpose of automated access control decisions. An automated NAC solution takes security polices (such as those within this STIG) together with data collected by assessment tools and provides an automated policy decision point that controls network entry for both remote users and devices.

While authentication for both the remote endpoint and the remote user is required, a NAC appliance is not currently mandated within the DoD. However, many organizations are evaluating these appliances for use in their networks. Thus, the guidance in the SRC STIG and the Network Infrastructure STIG are not intended to mandate this solution but rather to provide guidance if these products are being considered. The Network Infrastructure STIG provides general guidance for use within the enclave, while this STIG provides guidance only for use of these products to control remote access from outside the enclave.

This section discusses architecture and policy for integrating DoD network security policy and assessment tools into the automated entry control technologies for the network. These devices allow for automated network policy assessment, enforcement, and remediation at the network edge prior to allowing access to the network. These services can enhance the level of assurance of the network entry determination and are critical to allowing granular access control assignments for users/devices with varying levels of trust or authorization. These services may facilitate compliance with Federal and DoD mandates to provide access for non-DoD assets, authorized DoD visitor access, and emergency guest access (e.g., during national emergencies).

3.1 Policy Assessment and NAC Services

NAC services are implemented using one or more network technologies to ensure that network devices and users are authenticated, authorized, and compliant with established network policy. Because there is currently no NAC server standard, each vendor's implementation can vary significantly. DoD requires physical port authentication on classified networks and logical port security on unclassified networks. Client devices are also required to be compliant with various operating STIGs and desktop application requirements. A policy assessment server can be placed in the network environment to implement the security required on the ports but also to assess and enforce the device's security posture. The results of the client posture assessment can then be leveraged to automate enforcement of access policy restrictions based on assessment status, community of interest, or group specific policy.

NAC systems integrate several different technologies to achieve security policy definition, authentication, authorization, and physical or logical network access enforcement. Depending on the network architecture and vendor, these services may be provided by different components of the NAC systems. In general, NAC systems include three major components: Network access point device (e.g., VPN, RAS, or Point-to-Point Protocol (PPP) gateway), NAC policy server,

and the endpoint. The network layer or network access point consists of wired ports on a switch, wireless access points, or remote access systems (such as VPN or RAS devices). NAC systems work in conjunction with these technologies to restrict and grant access to network resources. While there are a number of different access scenarios (discussed in later sections), the goal of NAC is for the endpoint to request access to the network; the NAC policy server to decide the level of access based on a number of attributes; and then for the NAC policy server to instruct the network access point device to handle the endpoint's network access appropriately.

NAC solutions can be configured to work in conjunction with pre-existing security technologies to provide post-connect NAC. Alerts from systems (such as IDS) and vulnerability scanners can trigger the NAC system to revoke access previously granted to an endpoint or a user. Other tools are available to DoD sites that give local SAs the ability to scan networks for vulnerabilities and to provide centralized reporting.

Finally, Host-Based Security System (HBSS) provides McAfee's ePolicy Orchestrator to all unclassified and classified networks in DoD through a console that centrally manages personal firewalls, IDS, Intrusion Prevention Systems (IPS), anti-viruses, and system. HBSS provides a robust white-list capability for executable programs. In other words, applications not given explicit permission to run on a desktop computer cannot be executed. NAC solutions must incorporate these services and be fully integrated with HBSS for baselining and enforcement of protection policies.

NAC systems require authentication and authorization for both the endpoint and the user. Successful authentication using multi-factor authentication is required before the network access point forwards traffic. Authorization of the OS security posture is also determined. Endpoints or users that fail authentication are blocked from any network access either by physically shutting down the port or by logically blocking the Media Access Code (MAC) or IP addresses. Endpoints failing security policy authorization are logically "quarantined" into a highly-restricted area using restricted Virtual Local Area Networks (VLANs) or ACLs. Endpoints that fail these pre-determined security checks are granted access to remediation services only.

3.2 NAC Appliances

NAC appliances can be deployed using either an in-band (inline) or out-of-band (offline) architecture. Careful assessment of each vendor's product is needed since not all modes or combination of modes may be supported. Also, implementation of each mode may vary with each vendor's solution.

An in-band NAC appliance acts as a gateway between the VPN gateway and the rest of the network. All traffic must flow through this appliance. This architecture is simple to deploy as it requires only that all traffic entering the VPN be decrypted and sent to the NAC appliance. However, this type of installation can become a network bottleneck and a single point of failure for remote users.

Installing the policy server out-of-band places the NAC so that the VPN or the RAS can direct the device seeking remote access, once authenticated, to the NAC appliance. However, after

passing the policy assessment, devices will be redirected to another VLAN and future authentication can bypass the NAC server.

Although this section focuses primarily on the remote access recommended architecture, NAC and policy assessment will most likely be centralized on the network to save cost and complexity. Thus, some considerations are included here for wired and wireless LAN implementation of the NAC policy server.

For remote access/VPN scenarios, an in-band NAC deployment is recommended. Authentication must occur at the VPN using an approved authentication technique. Authorization and network enforcement occurs logically via a bridging NAC device. The NAC policy server will block traffic from an endpoint until the endpoint has been assessed and has passed those tests. Once the device has passed, the device's traffic is allowed through to the network. With remote access scenarios, redundancy and bandwidth requirements are critical.

NAC solutions are generally involved in the endpoint and user access pathway and can render many users and endpoints without network access. Therefore, when used in support of mission critical remote access, they must be highly available with state-full redundancy and failover.

This page is intentionally left blank.

4. ENDPOINT SECURITY

This section gives requirements and best practices for securing PCs and consumer devices, securing the networks that telework devices use, and protecting information stored on and sent to and from telework devices. The following subsections also provide guidance on evaluating the security of third party-owned devices, so that teleworkers can decide whether the devices should be used for remote access.

4.1 General Security Controls

Remote access is now possible from a myriad of different endpoint technologies including notebook computers, desktop computers used at home, and PEDs. Thus, remote access devices can be divided into two general categories: PCs and PEDs. PCs include desktops and laptop computers running a standard OS (e.g., Windows Vista, Windows XP, or Linux/UNIX). PEDs are small, mobile consumer products with limited memory and other resources and are not able to run full versions of standard OSs. PEDs may include Personal Digital Assistants (PDAs), cell phones, and e-mail devices with direct or indirect (docking) networking capabilities. Security controls for mobile and telework devices includes the following:

- **Anti-virus Software**: Automatically checks new files entering a PC for infection.
- **Authentication Technology**: Includes technology such as multiple-factor authentication (including tokens and smart cards), digital certificates, and device authentication to verify identities of authorized users, web sites, and computers.
- **Encryption**: Is process of encoding data so that only the intended recipient can read it by using a pre-defined algorithm and a secret piece of information, whether data is in transit or at rest.
- **Firewall Blocks**: Prevents unauthorized traffic from entering PCs from the Internet.

4.2 Thin Client

Thin clients are lightweight machines primarily used for display and input requiring less maintenance and fewer upgrades. Organizations provide computing services to the thin clients from high-powered servers over a network connection. Server resources may be shared across many users, resulting in more effective utilization of computing hardware. Use of thin clients, depending on the implementation methodology, presents an opportunity for increased control of the security environment of the remote access devices connecting to the enclave.

Many thin client devices run only web browsers or remote desktop software, which means that all significant processing occurs on the server. In contrast, a thick or a fat client does as much processing as possible and passes only data for communications and storage to the server.

Thin client devices and appliances are specifically designed machines used primarily for accessing server-based computing environments, including web browsing, terminal emulation, and terminal server sessions. Thin client devices usually have no local hard drives or moving

parts and host primarily presentation logic. Thin client devices rely on the server for application and data logic processing. Also, thin client devices typically come with a keyboard, mouse, and monitor.

There are two types of thin client devices, stateful and stateless. Stateful thin clients have a small OS, or thin OS, and are most easily categorized by their local OS. Most of these devices run some form of chip-based Windows CE, XP embedded, Linux, or Java. Stateless thin clients, sometimes referred to as Ultra Thin Client technology, run the connection client software such as Citrix, Windows Terminal Services, etc., directly from the appliance's hardware. As a consequence, the term thin client has come to encompass any device marketed as a thin client in the original definition, even if its' actual capabilities are much greater.

NOTE: A thin client device is any computing device that enables users to perform computing tasks remotely on the server. A laptop, or a PC, that has no hard drive will be considered a thin client or a stateless thin client.

4.3 Thin Client Virtual Desktop Infrastructure

Virtual Desktop Infrastructure (VDI) is a new method for delivering desktops to users. Users have been using local desktops for years and have recently began accessing remote server-based computing (SBC) desktops running on Microsoft Terminal Servers or Citrix Presentation Servers. A virtual desktop allows users to run Windows or UNIX in the data center. Users would remotely connect to and control their own instance of the desktop in a one-to-one manner from the thin client device. The virtual desktop that is assigned to users is a virtual machine in the data center running the OS.

Virtualizing the desktop provides the benefits of thin clients without being concerned about current desktop and legacy applications in a typical server-based computing architecture. Users can continue to use their existing desktop operating environment of choice whether it is Windows or UNIX. Figure 4-1 illustrates virtual desktops.

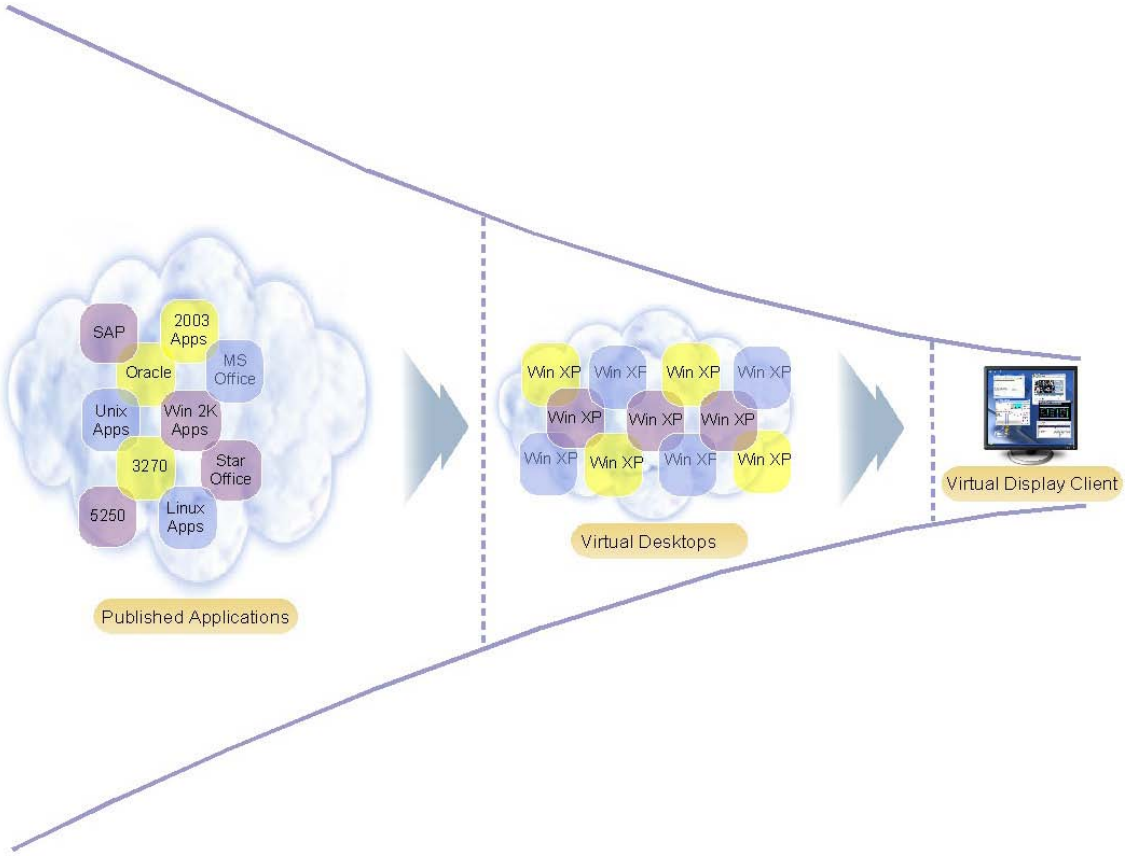

Figure 4-1. Virtual Desktops

The desktop virtualization solution is a multi-tiered architecture. Each tier comprises functional components that enable a thin client implementation. Figure 4-2 illustrates each tier. The four tiers (from top to bottom in Figure 4-2) are as follows:

- **Client Tier**: The client tier is the access points, or thin client devices, used by end users for accessing their desktop instance with the virtual desktop tier.
- **Access Tier**: The access tier is the infrastructure that enables and brokers thin client connections between the client tier and the virtual desktop tier.
- **Virtual Desktop Tier**: The virtual desktop tier is where users' desktop images are consolidated into a centralized farm of VDI servers.
- **Client Application Tier**: The client application tier is the application farms of applications traditionally delivered to the desktop via application publishing products or display protocols (such as Independent Computing Architecture (ICA), RDP, etc.).

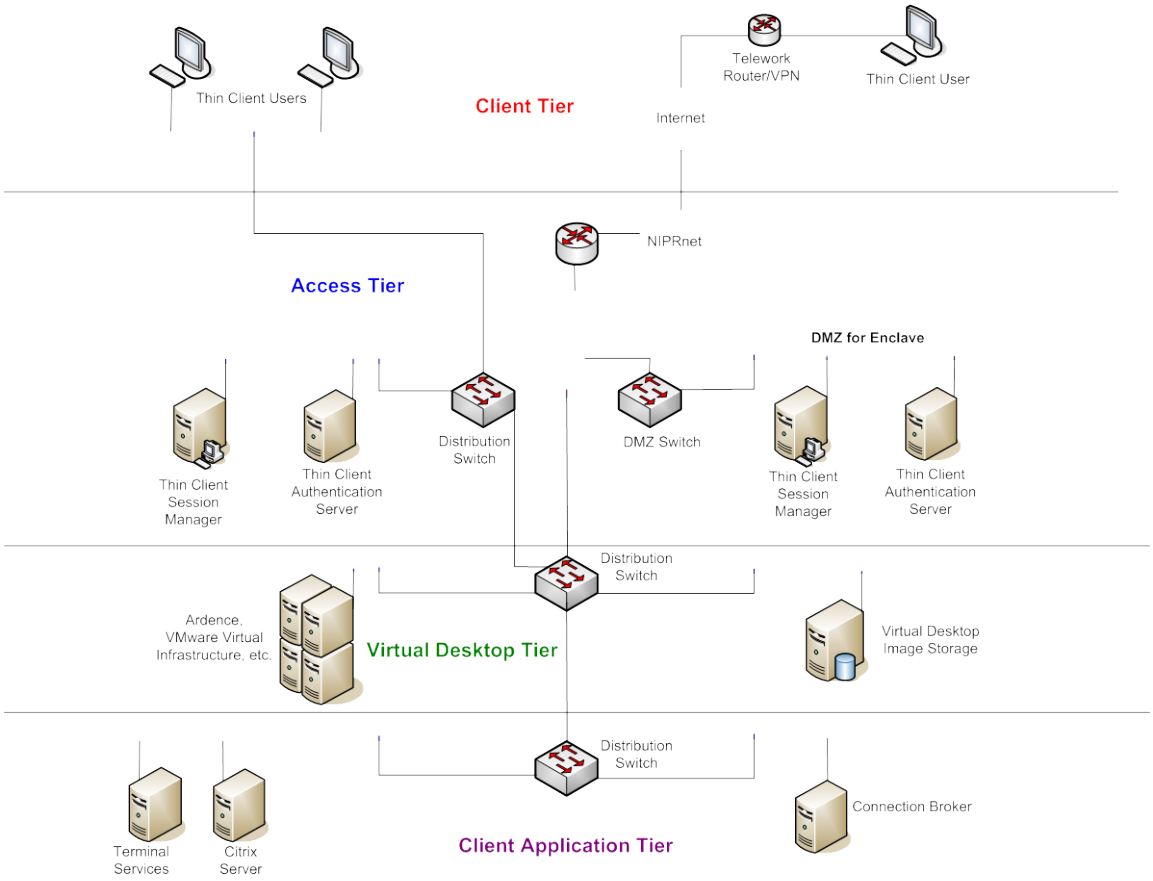

Figure 4-2. Multi-Tiered Architecture

The multi-tiered architecture is discussed in the following sections along with general security requirements that apply to all the tiers. These requirements include auditing, backup and recovery, patch management, and product-specific checklists.

5. SECURITY READINESS REVIEW REQUIREMENTS

This section presents the data collection and procedures for a Remote Access Security Readiness Review (SRR). The items reviewed as part of this SRR are based on the requirements published by DoDD 8500.1, paragraph 4.18. DoDD 8500.1 requires guidelines to be developed by DISA FSO in accordance with DoD-approved security configuration as specified in the DoDD O-8530.1

The requirements to perform a Remote Access SRR are as follows:

- **Remote Access Policy STIG** – Provides general checks which require a global administrative or network policy. Required for all sites which allow users to access remotely for telework or mobile computing access. Does not apply for site-to-site or out-of-band communications.

- **Remote_Access_Server (RAS) STIG** – Provides checks for RAS hosts and appliances.

- **Remote Access VPN STIG** – Provides checks which require global policy settings in the remote access VPN gateway. Applies only when the VPN Concentrator is used as the VPN gateway to allow remote access to the network for teleworking or mobile users.

- **Remote Endpoint STIG** – Provides checks applicable to all types of remote and mobile endpoints. Ensures browser and other applications installed on the remote endpoint are configured and used securely. Applies only when thin client hardware and servers are used for remote user access for telework or mobile computing. Implemented using the Desktop Applications – Remote Access posture.

- **Remote XenApp ICA Thin Client STIG** – Provides checks applicable to thin client endpoints which use the XenAPP Program Neighborhood for remote access. Use for checking the required policies using the remote client.

- The STIG document may be downloaded from IASE web site located at http://iase.disa.mil or the Defense Knowledge Online (DKO) web site located at https://www.us.army.mil/suite/portal/index.jsp.

- The review team will also need a Network and OS Reviewer or to verify a self-assessment using the Network Infrastructure and the applicable operating system STIGs to fully evaluate compliance with remote access requirements. If wireless networking devices or endpoints are used for remote access, then the Reviewer will verify that an SRR or self-assessment using the applicable Wireless STIG has been completed.

5.1 Data Collection and Assessment Procedures

Use the applicable checklist as described in the previous section to capture the initial data. The general steps involved in data collection and assessment are as follows:

1. Prior to arriving onsite, acquire the latest printed copy of a previously completed SRR or self-check security reviews to include the OS and Remote Access Policy SRR Checklists.
2. Ensure that you have a valid VMS account.
3. If possible, acquire a current copy of the site's network topology (network diagram) and, in particular, the remote access infrastructure, prior to arriving onsite or obtain a copy as soon as possible after arriving onsite.
4. During or soon after the in-brief at the site, obtain the name(s) and phone number(s) of the onsite points-of-contact for the remote access review.

The Reviewer is responsible for coordinating with site personnel in arranging the review of the site's network. The procedures for the collection of SRR data are as follows:

1. Interview the SAs/IAOs, either individually or as a group, to complete the Remote Access Policy (non-computing) checks.
2. The Team Lead will create a VMS Visits folder and provide the visit names to the Reviewer.
3. After all of the data for the checklist (s) are complete, enter the information into VMS.
4. Enter the SRR results into the proper VMS visit by cross-referencing the Vulnerability Identification (ID) with the STIG ID located on the checklist.
5. After the vulnerabilities have been entered into VMS, the Reviewer will verify that no vulnerabilities are in the Not Reviewed (NR) status. Any NR vulnerabilities will be reviewed again to ensure it has been entered correctly.
6. Open findings will be reviewed to ensure the "Finding Details" field has accurate text. If the "Finding Details" field is empty, the Reviewer will enter appropriate text explaining the cause of the Open finding.
7. The Reviewer will discuss with the site personnel the feasibility of closing all Category I findings before the team leaves the site. The Reviewer will keep the Team Lead informed of all Category I findings and provide additional emphasis and clarity when explaining why some Category I findings cannot be closed immediately.
8. Floppy disks, compact discs (CDs), Digital Versatile Discs (DVDs), Universal Serial Bus (USB) drives, data entry forms, and reports will be handled and protected in accordance with their level of classification.
9. The Reviewer will communicate to the Team Lead the status of VMS data entry through daily meetings and will send an e-mail to the Team Lead only if the VMS data entry cannot be completed on site.

5.2 VMS SRR Data Entry Procedures

Verify the asset is registered in VMS under the correct organization. Assets not registered will need to be created. When creating the asset, the asset ownership defaults to the person creating the asset. It is recommended that the SA create the asset. If the Reviewer creates the asset, the permissions will need to be reassigned to the SA.

1. Creating the Asset

a. Expand Asset Findings Maintenance.
b. Expand Assets/Findings.
c. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
d. Expand the sub-folder assigned. Each sub-folder represents individual visits in VMS assigned for review.
e. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing, and Computer Network Defense Service (CNDS).

1.1 Creating a Non-Computing Asset

a. Click the yellow folder icon located at the right of 'Non-Computing'.
b. Click the General tab.
c. Enter the Display name. The standard name for network non-computing asset will be: "SiteName_RemoteAccess_Policy".
d. Verify "Location".
e. Verify "Owner": Used to register asset to parent or child location.
f. Verify "Managed By": Used for remote locations being managed.
g. Verify Mac level, Confidentiality, and Classification are correct.
h. Click the 'Asset Posture' tab to add functions to the asset.
i. Expand Non-computing.
j. Expand 'Network Policy Requirements".
k. Click 'Remote Access Policy'.
l. Click '>>' to move it to the 'Selected' window.
m. Click the Systems / Enclaves tab.
n. For registered enclaves, choose the correct enclave.
o. If the enclave is not present, ensure that the IAM or the Team Lead works with the appropriate site personnel to request an enclave.
p. Click 'Save'.

1.2 Creating a Computing Asset

a. Click the Create Icon located next to computing. The asset form is displayed.
b. Click the General tab and enter the information into the required fields.
c. Click the asset identification tab and enter the IP address, MAC address, and click Add.

d. Click the Asset Posture tab and drill down to select an asset posture (as described in Table 5-1). Click Save when done.

Table 5-1. Asset Posture

Remote Access Technology	Asset Posture	Corresponding Manual Document
Add this posture to all remote access security assessments. Contains general training, documentation, and NAC appliance policies.	Non-Computing >> Network Policy Requirements >> Remote Access	Remote Access Policy STIG
Add this posture only if the site uses a RAS (dial-up) server or an integrated gateway which provides both VPN and dial-up access.	Computing >> Network >> Data Network >> Remote Access Server	Remote Access Server (RAS) STIG
Add this posture only if the site uses a VPN gateway (appliance or server) to provide remote access to endpoints (not other DoD hosts) from outside the enclave.	Computing >> Encryption/Tunneling >> VPN Concentrator	Network Infrastructure – Other Devices
	Computing >> Role >> Remote Access	Remote Access VPN STIG
Add this posture for manual review of remote access endpoints. Contains endpoint security checks that require inspection of client settings. For wireless remote access, also conduct a wireless review using the Wireless STIG.	Computing >> Application >> Desktop Application - Remote Access	Remote Endpoint STIG
Add this posture only if the site uses XenApp thin clients for remote access. Contains only client checks.	Computing >> Application >> XenApp Program Neighborhood Client	XenApp ICA Thin Client STIG

2. Reassign Permissions for Asset (If Required)

a. Expand Permissions.
b. Click Reviewer Asset Update.
c. Select Visit and submit.
d. Select Asset and submit.
e. Select User and submit.

3. Procedures for Review of the Asset

If all registration tasks have been accomplished, use the following procedures:

a. Expand Asset Findings Maintenance.
b. Expand Assets/Findings.
c. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
d. Expand the sub-folder assigned. Each sub-folder represents individual visits in VMS assigned for review.
e. Expand the visit and display the location summaries.
f. Expand 'Non-Computing' or 'Computing' depending on the asset type registration.
g. Expand 'Must Review'. *(Reviewer Only) SA will not see 'Must Review'.* If an asset was just created, it would reside in 'Not elected for Review' section. Have the Team Lead move the asset to 'Must Review'.
h. Expand Asset to review. Ready to review is colored in RED.
i. Expand each Asset, and then expand each Vulnerability Key.
j. Update the 'Status' of the vulnerability.
k. Identify details on all open vulnerabilities.
l. SAs will need to update the Plan of Action and Milestone (POA&M) prior to saving.
m. SAs should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level. Asset must be in the same status (such as 'Open').
n. Save the updates to the asset.

4. Verify that all Necessary Assets were Reviewed

a. Select Asset Findings Maintenance.
b. Expand Assets/Findings.
c. Expand visits to display the sub-folders.
d. Expand the sub-folder assigned.
e. Expand the visit and display the location summaries. Within the location, assets are divided into computing, non-computing, and CNDS.
f. Expand 'non-computing'.
g. Expand 'Computing'.
h. Expand 'Must Review'. (If checkmarks are gone, the asset has been reviewed.)

5. Add Comments

a. Select Visit Maintenance.
b. Expand Organization for the visit.
c. Expand Visit.
d. Locate the visit.
e. Click on Command Communications Service Designator (CCSD) or enclave name.
f. Add a comment on the Comments Tab.
g. Save Changes.

6. Compliance Monitoring

a. Select Reports from the VMS menu.
b. Select VC06 – Asset Compliance Report.
c. Select an asset or an org.
d. Select "open" status.
e. Sort on desired fields.
f. Display desired fields (e.g., Finding Comments, Finding Long Name, Finding Details, and Vulnerability Discussion).

The following additional report may be useful to the reviewer. Follow the on-screen directions if selecting these reports.

The AS01 report assists the Reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section "Looking at Network Assets" is a quick step by step instruction in creating the report. The site may want to do other reports if your site manages or owns assets which are not located at the site. Check Child Locations, if applicable. Navigate to the Reports menu, select the AS01 Report, and select the desired criteria for the report.

The VL03 report assists the Reviewer or SA by quickly identifying the IAVMs that will be identified to the asset by selecting the OS of the asset. Navigate to the Reports Menu, select the VL03 Report, and select the desired criteria for the report.

APPENDIX A. REFERENCES

Applicable Policies and Guidelines

Office of the Secretary of Defense Memorandum, Compliance and Review of Logical Access Control in the Department of Defense (DoD) Processes, 24 January 2007

Directive-Type Memorandum (DTM) 08-027 – Security of Unclassified DoD Information on Non-DoD Information Systems, 31 July 2009

Memorandum for Secretaries of the Military Departments, et al, “Department of Defense (DoD) Telework Policy and Guide,” 22 October 2001

NIST SP 800-77, Guide to IPSec VPNs, December 2005

NIST SP800-113, Guide to SSL VPNs, July 2008

NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access, November 2007

NIST SP 800-46 Rev, Guide to Enterprise Telework and Remote Access Security, 1 June 2009

DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003

DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices, April 18, 2006

DoD Instruction 1035.01, Telework Policy, April 3, 2007

DoD Policy Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, July 3, 2007

DoD Policy Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, July 3, 2007

Global Network Defense Warning Order (WARNORD) 06-16 Specified Tasks for Phase 1 of the Accelerated Public Key Infrastructure (PKI) Implementation, March 2006

Joint Task Force - Global Network Operations (JTF-GNO) Communications Tasking Order (CTO) 06-02, dated 17 January 2006

NSA Remote Access Secure Program Transition Guidelines, Version 1.0, March 31, 2005

Other References and General Information Sites

http://iase.disa.mil	DISA IASE site
http://csrc.nist.gov/cryptval/	FIPS 140-2 Products lists
http://www.telework.gov	Government telework information
http://www.telework.gov/	U.S. Interagency Telework Web Site Operated by General Services Administration and Office of Personnel Management
http://csrc.nist.gov/publications	NIST security publications and guidance

APPENDIX B. ACRONYM LIST

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CCSD	Command Communications Service Designator
CD	Compact Disc
CNDS	Computer Network Defense Service
CNDSP	Computer Network Defense Service Provider
CTO	Communication Tasking Order
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DKO	Defense Knowledge Online
DMZ	De-militarized Zone
DoD	Department of Defense
DoDD	DoD Directive
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
FSO	Field Security Operations
HBSS	Host Based Security System
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
ICA	Independent Computing Architecture
ID	Identification
IDS	Intrusion Detection System
IEEE	??
INFOCON	Information Operations Condition
IP	Internet Protocol
IPS	Intrusion Prevention Systems
ISP	Internet Service Provider
JTF-GNO	Joint Task Force-Global Network Operations
LAN	Local Area Network
MAC	Media Access Control
Mbps	Megabit per second

Acronym	Definition
NAC	Network Access Control
NAS	Network Access Server
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NR	Not Reviewed
NSA	National Security Agency
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestone
PPP	Point-to-Point Protocol
RAS	Remote Access Server
RDP	Remote Desktop Protocol
SA	System Administrator
SBC	server-based computing
SRC	Secure Remote Computing
SRR	Security Readiness Review
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
VoIP	Voice over IP
VPN	Virtual Private Network
WARNORD	Warning Order