SECURE REMOTE COMPUTING

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 2

10 August 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

TABLE OF FIGURES

SUMMARY OF CHANGES

GENERAL CHANGES

- The previous release was Version 1, Release 1, dated 14 February 2003.
- Minor editorial updates throughout.
- Change ISSM to IAM throughout.
- Changed ISSO to IAO throughout.
- Added PDI numbers and CAT codes throughout.

SECTION CHANGES

SECTION 1. INTRODUCTION

- Updated template information to include latest FSO approved verbiage, helpdesk contact information, and IASE website address.
- Deleted reference to SFUG.
- Added reference to new Secure Remote Computing Addendum.

SECTION 2. TYPES OF REMOTE ACCESS

- EN440 updated for clarification.
- NET1440 update for clarification. Added note for clarification.

SECTION 3. GENERAL STANDARDS FOR ALL REMOTE USERS

- Section 3, added not to clarification.
- NET0230 and NET0260 regarding password requirements. Separated into two policies and updated IAW latest FSO wording requirements.
- Section 3.2, deleted paragraph referring to the DISA Information System Contaminations Instruction 630-230 reference document, which does not exist at this time.

SECTION 4. END USER REMOTE ACCESS TECHNOLOGIES

- PDI numbers and CAT codes added.

SECTION 5. SECURING REMOTE ACCESS DEVICES

- SRC580 updated with note for clarification.
- NET1595 edited for clarification.
- EN390 removed section reference.
- EN400 updated for clarification with wording from Enclave STIG.
- NET1630 updated for clarification with wording from Network Infrastructure STIG.
- NET0340 updated for clarification with wording from Network Infrastructure STIG.
- NET1441 removed RASP and replaced with new solution program name, HARA.

APPENDICES

- Appendix A updated various publications to either show latest version and date or remote this information from the more fluid documents such as the STIGs.
- Appendix D Removed – CJCSM and Computing Services Handbook references

1. INTRODUCTION

1.1 Background

This *Secure Remote Computing Security Technical Implementation Guide (STIG)* provides the technical security policies and requirements for providing a secure remote access environment to users in Department of Defense (DOD) components. This document discusses both the remote user environment and the network site architecture that supports the remote user. Since information that the war fighter depends upon can be stored, processed, or transmitted from a number of locations, information systems management and Information Security (INFOSEC) must encompass the total environment. This guide is not a guide to telecommuting as a policy or practice; rather it is a guide to securing DOD assets within a remote access environment.

Further information on remote access is also provided in the *Secure Remote Access Service Addendum,* which is available on the IASE web site. This addendum provides a technical overview of a general DOD remote access architecture, guidance for secure remote computing, an evaluation of the risks that wireless connections present, and gives best practices to follow to ensure proper security for these connections. This addendum also discusses the functionality of the security components.

Unlike other STIGs, this STIG does not have a corresponding checklist. Most policies have been incorporated into the appropriate checklist, depending on the technology or area. For example, NET1441, is located in the Network Infrastructure Security Checklist while EN440 is in the Enclave Security Checklist. If the policy number is marked as N/A, this indicates that this check has not yet been incorporated into a specific checklist but will be in the future.

In its early days, remote access to network resources was limited to System Administrators (SAs) and consultants for emergency and diagnostic situations. Traditionally, dial-up connections with speeds up to 56K were used to access network resources and the Internet. However, the rapidly changing Information Technology arena has allowed for expansive growth in terms of remote access capabilities. Due to this expansion in technology, an important trend is the requirement for remote access to government networks and resources.

There are numerous advantages to remote access including the following:

- Allowing flexible work schedules
- Providing “road warriors” and teleworkers the advantage of accessing the network and resources when on official Government business
- System Administrator access to resolve problems remotely
- Increased productivity due to an improved work and home life balance
- Reduction of operational overhead (e.g., office space, infrastructure costs, less sick leave, flexibility)
- Environmental advantages such as the reduction in traffic and commuting times
- The ability to better provide for disadvantaged workers

As with any advantage, there is usually a security cost associated and remote access is no exception. With the advent of new high-speed, broadband technologies such as cable modems,

Digital Subscriber Line (DSL), satellite, and wireless, the need for increased security at the client and network levels becomes a preeminent factor as the threat of attack escalates significantly. These broadband technologies allow for increased transmission speed and bandwidth, which makes it easier for the remote user to access and transfer larger amounts of data and behavioral changes that allow the user to be on-line for greater amounts of time. However, this also makes the remote user an attractive target for attackers. Therefore, a greater potential exists for exposure of internal Government network resources and data from external sources.

The intent of this STIG is to include security considerations at the network and remote user level that are needed to provide an acceptable level of risk for information as it is transmitted to a network enclave and potentially to other sites. It also provides suggestions for redundancy, survivability, and some guidelines for best technical practices.

The DOD and all other Federal agencies are instructed by Public Law Public 106-346, Section 359, 10/23/2000 to do the following:

- Review telework barriers, act to remove them, and increase actual participation.
- Establish eligibility criteria.
- Subject to any applicable agency policies or bargaining obligations, employees who meet the criteria and want to participate must be allowed that opportunity if they are satisfactory performers.

Telecommuting, often referred to as "teleworking," is a flexible business solution in which an employee performs officially designated duties at an alternate work site. The DOD Telework Policy requires "each Executive Agency to establish a policy under which eligible employees of the agency may participate in teleworking to the maximum extent possible without diminished employee performance."

The DOD Telework policy was designed to actively promote telework to promote DOD as an employer of choice, improve recruitment and retention of high-quality employees, employ and accommodate persons with disabilities, reduce traffic congestion, reduce energy consumption and pollution emissions, and reduce office space, parking facilities, and transportation costs.

The number of attacks on computer systems and networks is doubling each year as Internet usage has increased along with the sophistication of hackers and their tools. With Federal policy now in effect, implementations of the Telework policy will be initiated by various agencies to include the DOD, therefore increasing the threat of serious attacks on DOD computer systems.

In preventing computer attacks, the DOD must protect a vast and complex information infrastructure. The DOD also depends critically on information technology (IT). It uses computers to help design weapons, to identify and track enemy targets, to pay soldiers, to mobilize reservists, and to manage supplies. It is imperative that this information and the media that it traverses be secure.

1.2 Authority

DOD Directive 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 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 DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

This document is a requirement for all DOD administered systems and all systems connected to DOD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and SAs with configuring and maintaining security controls.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity 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 has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1 Vulnerability Severity Code Definitions

1.6 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.

1.7 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.

2. TYPES OF REMOTE ACCESS

There are varying sensitivity levels when initiating remote access to a Department of Defense network and the resources it contains. The following levels are defined to differentiate the types of remote access users. These definitions are used to clarify differing requirements based on the type of access required by the user. If the site so chooses, Administrative and End-User access may be treated the same for configuration management purposes; 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 STIG 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 DMZ such as a web server).

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 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. It is strongly suggested that End-User access employs the use of 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., viewing e-mail via a webmail application such as Outlook for Web Access [OWA] or accessing a DOD web site). This type of access will require minimum-security controls and users may use personal computers or devices if approved by the local DAA.

2.1 Access Level Encryption Requirements

As System Administrators perform duties such as configuration changes, troubleshooting application and communications issues, and logging in to a system with privileges to perform maintenance functions, rigorous security measures must be in place to protect the data and communication to and from the system. Administrative access will require the use of encryption on all communication channels between the remote user and the system being accessed. If the system requires the use of a clear-text based terminal emulator such as TN3270 (which accesses 3270 and 5250 based applications over TCP/IP) or Telnet, the only acceptable methods of connectivity will be an encrypted session, the employment of VPNs, Secure Web Access (SWA) with Secure Socket Layer (SSL), IPSEC, or Secure Shell (SSH). Encryption should be used to protect the End-User access level. However, as of this writing, it is not required, but rather it is a suggested practice.

- (EN440: CAT I) The IAO will ensure all privileged user access to a DOD system or resource is secured using FIPS 140-2 validated encryption to secure the data traversing the network. This applies to unclassified data only. Classified data requires Type I encryption.

- (NET1440: CAT III) For End-User access, the NSO will limit the use of clear text Telnet, TN3270, and other terminal emulator TCP/IP sessions and must employ encryption to the fullest extent possible.

NOTE: Refer to the Enclave STIG for additional information on FTP and TELNET.

Limited access does not preclude the remote user from using their personal PCs to access services such as a webmail application (e.g., OWA) to send and receive e-mail. However, e-mail attachments, if downloaded, will be removed/deleted from the user's personal PC when they are no longer required. Limited Access users are not prohibited from accessing publicly accessible services that reside in a DMZ. While the intent at this time is to allow users to access a Government webmail application from a personal PC, the preferred method is to access e-mail from Government owned or controlled devices via dial-up or VPNs in order to limit the Government's exposure to malicious threats.

- *(N/A: CAT III) The IAO will configure webmail applications to limit the use of commercial addresses from entering the web site. Restricting to* ***.gov*** *and* ***.mil*** *address space, or restricting by source and destination address are acceptable methods.*

- *(EN480: CAT II) The IAO will ensure the webmail application server is located in a DMZ and the server is secured in accordance with the Web Services and appropriate OS STIGs.*

- *(N/A: CAT III) The IAO will ensure limited access users remove any downloaded e-mail attachments (from the webmail application) from their personal PC when no longer required.*

3. GENERAL STANDARDS FOR ALL REMOTE USERS

Information security vulnerabilities are inherent in all forms of computer systems, software, architectures, and devices. The goal of information security is to provide data integrity, confidentiality, and availability. In order to provide these services to the DOD community, general security standards for any form of remote access to a DOD network must be in place. These standards are set forth for ease of configuration management and to aid in developing a secure, standardized remote access environment.

The following sub-sections set security guidance applicable to remote access communication methods (e.g., Network Access Servers, dial-in connections, high-speed broadband connections, etc.). All requirements will be met for Administrative Access and to the fullest extent possible for End-User and Limited Access. This guidance will be followed, in addition to the requirements set forth in the individual sections, as well as all other applicable DISA Security STIGs.

- *(N/A: CAT II) The Network Security Officer (NSO) will ensure all network, remote access, device security, and architectural requirements contained in the Network Infrastructure and Enclave STIGs are followed.*

- *(N/A: CAT II) The remote user will follow all applicable site requirements pertaining to Local Area Network user responsibilities.*

NOTE: This check corresponds to EN120 in the Enclave STIG, which requires that all end users receive training.

- *(NET0230: CAT 1) The NSO will ensure all communications devices are password protected.*

- *(NET0260: CAT II) The NSO will ensure an accepted password generation scheme is used to create passwords. At a minimum, passwords will be created and maintained in accordance with the DODI 8500.2.*

- *(EN510: CAT II) The IAO will ensure all security requirements contained in the appropriate Operating System (OS) and Desktop Application STIGs are followed for any device that will access a DOD network remotely (i.e., the remote device will be STIG and IAVA compliant prior to connecting to a DOD network).*

- *(SM050: CAT II) The IAO will ensure personally owned computers are not used for remote access to a DOD network for administrative or end user access.*

- *(NET1446: CAT II) The IAO will ensure no Classified processing takes place at a remote user's site that is not explicitly approved for Classified processing. If Classified processing takes place in an alternative work site approved for such processing, all DOD policy will be strictly adhered to regarding facility clearances, protection, storage, distribution, etc.*

- *(NET1840: CAT II) The SA and the NSO will ensure if VPN technology is used to connect to a DOD network, the VPN client and concentrator will be configured to deny the use of split tunneling. The connection established will be an exclusive connection between the VPN client and the VPN network device; all other connectivity will be blocked after establishment of the VPN session, so there is no chance of IP packets being forwarded between the Internet and the DOD network.*

3.1 Remote Access Agreement

This STIG requires that prior to remotely accessing a DOD network or resource, a remote user must complete and sign a computer security checklist and a remote access agreement that are developed by the site.

There are numerous places from which a remote user can access a network, such as General Services Administration (GSA) Telework centers, hotel rooms, homes, airports, other DOD sites, etc. This STIG is intended to secure the remote user's PC or device as well as the site the user is accessing regardless of the location from which they are establishing a connection.

There are numerous requirements by various DOD agencies for performing work outside of the traditional work site in conjunction with connecting to a network or resource. To view the DOD Telework Policy and Memorandum, visit http://www.telework.gov. To obtain additional guidance or DISA Telework forms, visit https://mps-cmis.ncr.disa.mil/mps1.html.

- *(NET1446: CAT III) The IAM will develop a computer security checklist to be completed and signed by the remote user. This is to inform and remind the user of the potential security risks inherent with remote access methods. (See Appendix C, Checklist Example, for a security checklist example.)*

- *(NET1446: CAT III) The IAM will develop a policy for secure remote access to the site and an agreement between the site and remote user, to include, but not limited to, the following:*

  - *The agreement will contain the type of access required by the user.*

  - *The agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of their remote access device.*

  - *Incident handling and reporting procedures will be identified along with a designated point of contact.*

- *The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.*

- *The policy will contain general security requirements and practices and will be acknowledged and signed by the remote user.*

- *If Classified devices are used for remote access from an alternative work site, the remote user will adhere to DOD policy in regard to facility clearances, protection, storage, distributing, etc.*

- *Government owned hardware and software will be used for official duties only. The employee is the only individual authorized to use this equipment.*

3.2 Incident Handling and Response

In accordance with DOD policy, all components must establish Incident Handling and Response procedures. The steps taken when a computer or network incident occurs are paramount to the defense of the Global Information Grid (GIG). Once a suspected incident occurs on a DOD computer system or network, the DOD information infrastructure as a whole is in jeopardy. (See *Appendix G, CERT® /CC Intruder Detection Checklist*, for CERT guidance on what to look for in the event of a possible system compromise.)

Information System Contaminations, often referred to as spillage, result from the improper electronic processing, storage, or transmission of classified information using an unclassified network or stored in an information system. This type of contamination results in a compromise of the integrity of the Classified data and is therefore treated as a security incident and will be reported to the appropriate security officer.

- *(NET1446: CAT III) The IAO will ensure the site has an incident handling and response/reporting procedure outlined for the remote user. The remote user will in turn, follow the incident handling and reporting procedures as set forth by the site if there is a suspected or actual breach in security of the remote user's device.*

- *(SM050: CAT III) The IAO will ensure Incident Handling and Response procedures are followed in accordance with the Computing Services Security Handbook to include notifying the activity Director/Commander of all confirmed computer security incidents; submitting computer security incident reports as required; and coordinating any additional support with CONUS RCERT/DOD-CERT, if required.*

- *(N/A: CAT II) The SA will ensure all necessary security measures are in place to prevent computer security incidents (e.g., use of password protection, use of authorized software only, and use of virus detection software).*

- *(NET1441: CAT 1) The IAO will ensure a device (e.g., PC, workstation, laptop, etc.) that is used to remotely access the classified network will not be used to remotely access the unclassified network. The devices for accessing classified and unclassified networks will be mutually exclusive.*

3.3 Disaster Recovery

Theft, corruption, and the destruction of equipment or data all result in the loss of confidentiality and availability. If the computer is recovered, the integrity of the data itself is questionable. Due to the portability of laptops, notebooks, and PDAs, the risk of theft is significantly increased. Lost or stolen equipment has the potential to expose national security or sensitive data that, if divulged, could harm our national infrastructure. Remote users issued laptops or PDAs should be provided additional security awareness training to avoid potential loss of critical data. During travel, laptops and PDAs must be hand carried and never checked as baggage. If possible, carry diskettes or removable hard drives separate from the laptop. Laptops or PDAs may be stored in a locked car or hotel room but should be kept out of plain view. Laptops and other small computer devices are frequent targets of theft. The performance of regular system backups and attention to physical security are important factors in mitigating these risks. (Additional requirements for physical security are contained in the *Computing Services Security Handbook*)

- *(DTGW001: CAT II) The remote user will ensure Government data backups (not necessarily application or OS) are performed on a regular basis (i.e., once a week on some form of removable media).*

- *(SM050: CAT II) The remote user will ensure during travel, laptops and PDAs are hand carried and never checked as baggage. If possible, carry diskettes or removable hard drives separate from the laptop.*

- *(SM050: CAT II) The remote user will ensure when a laptops or PDA is stored in a locked car or hotel room; it will be kept out of plain view.*

- *(SM050: CAT II) The remote user will ensure all requirements as contained in the Computing Services Security Handbook are adhered to in regard to physical security of the remote device.*

4. END USER REMOTE ACCESS TECHNOLOGIES

4.1 Broadband Communications

"Broadband" is a general term that is used to refer to high-speed Internet connections that are capable of transmitting data at speeds in excess of one Megabit per second (Mbps), though there is no set bandwidth threshold. *Figure 4-1, Communications Connection Data Rates*, shows the various remote access connectivity options and the associated data rates. For the purpose of this document, the definition of broadband communication is any form of transmission other than normal dial-in methods. Digital Subscriber Line (DSL), cable modems, wireless, and satellite are examples of broadband technologies. Broadband connections supply the same services as dial-up, such as e-mail, web browsing, video access, and connections to Internet service providers (ISP) and other networks. According to Nielson/Netratings, the total number of broadband users set an all time record in excess of 21 million users in November 2001 and the number of telecommuters is expected to increase to 32 million in 2002.

REMOTE ACCESS CONNECTION	***DATA RATE***	***PHYSICAL MEDIUM***
Regular telephone service (POTS)	Up to 56 Kbps	Twisted pair
Integrated Services Digital Network (ISDN)	Basic Rate Interface: 64 Kbps to 128 Kbps; PRI: 23 (T-1) or 30 (E1) assignable 64-Kbps channels plus control channel; up to 1.544 Mbps (T-1) or 2.048 (E1)	BRI: Twisted-pair PRI: T-1 or E1 line
Wireless	IEEE 802.11a – 5GHz band = 6-54 Mbps IEEE 802.11b – 2.4GHz band = 1, 2, 5.5, & 11 Mbps	RF, IR, narrowband
Satellite	400 Kbps	RF in space (wireless)
DSL	256 Kbps to 8 Mbps	Twisted-pair (used as a digital, broadband medium)
Cable modem	512 Kbps to 52 Mbps (52 Mbps is to an ISP not individual user, the upper limit rate is subdivided between multiple users.)	Coaxial cable

Figure 4-1. Communications Connection Data Rates

4.1.1 DSL

DSL is a popular high speed, high bandwidth transmission technology that works over ordinary telephone lines. Traditional phone service (Plain Old Telephone Service – POTS) connects the end user to a telephone company central office (CO) over twisted pair copper wire. The signal is converted onto access paths for multimedia and high-speed data communications. DSL can transmit more than six Mbps downstream and 640 Kbps upstream, and as much as 1.1 Mbps in both directions. A DSL can carry both data and voice signals and the data stream is continuously connected. The digital modem accesses the local telephone companies' central office (CO) where a DSL Access Multiplexer (DSLAM) translates the DSL signal from copper onto a larger network backbone. Once the signal is transmitted to the backbone, it is directed to the ISP's

location, where the ISP verifies the access to the network and delivers users to the Internet through the ISP's relationship with a backbone network provider. See *Figure 4-2, DSL Connection Model*, for an example of remote access connectivity using DSL.

There are currently at least six different types of DSL. They are Asymmetric Digital Subscriber Line (ADSL), Symmetric Digital Subscriber Line (SDSL), ISDN Digital Subscriber Line (IDSL), High-bit-rate Digital Subscriber Line (HDSL), Very high-bit-rate Digital Subscriber Line (VDSL), and Rate-Adaptive Digital Subscriber Line (RADSL). Each type of DSL has different technical ranges, capabilities, and limitations. Not all types are available in all areas.

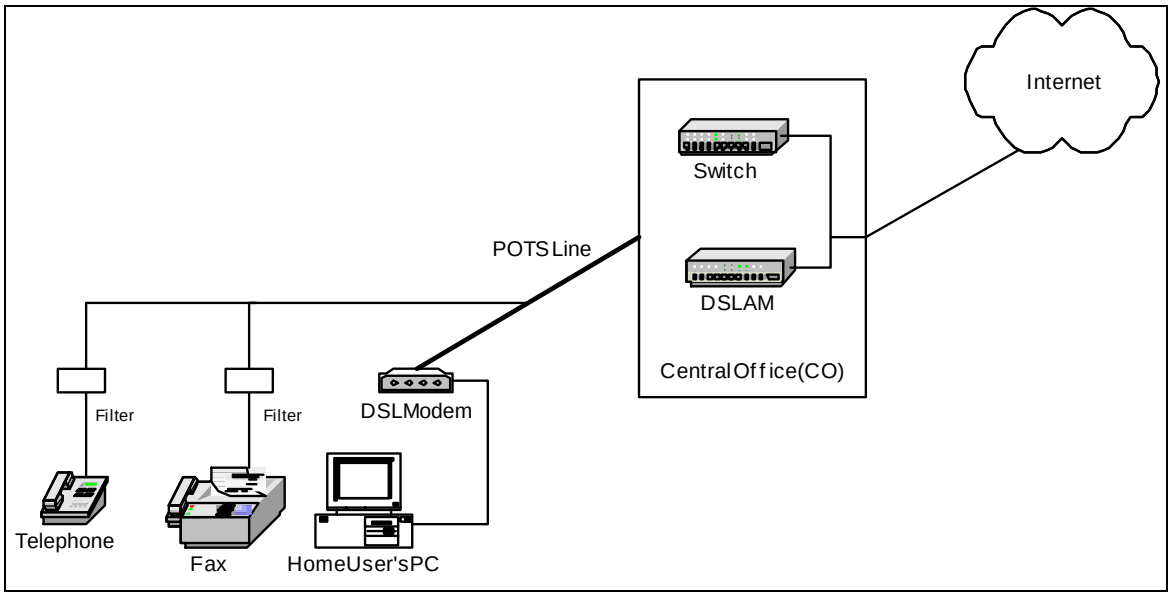

Figure 4-2. DSL Connection Model

4.1.2 ISDN

ISDN is a switched, end-to-end network that allows for simultaneous transmission of voice, data, and video information. ISDN uses a digital telephone line to provide guaranteed, two-way bandwidth that is switched by the telephone network. In most cases, the existing analog telephone line can be converted for ISDN service. Distance limitations from the Central Office are similar for ISDN and xDSL services while available bandwidth and data rates can differ substantially. See *Figure 4-3, ISDN Connection Model*, for an example of remote access connectivity using ISDN.

ISDN Basic Rate Interface (BRI) uses two 64 kbps B (Bearer) channels and one 16 kbps D (Signaling) channel. ISDN Primary Rate Interface (PRI) uses twenty-three B channels and one 64 kbps D channel. Other variations of ISDN are available as well. ISDN BRI is the service commonly used by telecommuters.

ISDN BRI is capable of providing simultaneous voice and data connections and provides its own bandwidth management with its D channel. Data transmission rates of 128 kbps are typical; 512 kbps can be realized with data compression. When there is a data call that is using the full 128

kbps (both 64 kbps B channels) of the BRI circuit, the Terminal Adapter (TA) has the ability to reduce the data connection to 64 kbps to allow voice or fax calls to be made or received on the other 64 kbps B channel. When the bandwidth is no longer needed for the voice call, the D channel allocates the bandwidth back to the data connection. This is often referred to as dynamic bandwidth allocation and is one of the main benefits of ISDN. A Terminal Adapter is required for the end user to interface with the ISDN circuit and is sometimes referred to as an ISDN modem.

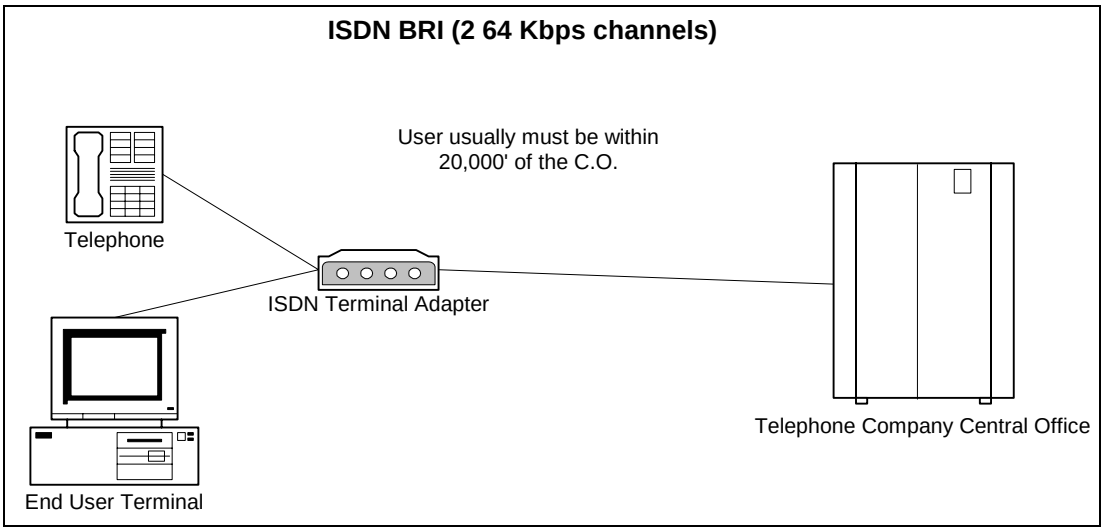

Figure 4-3. ISDN Connection Model

4.1.3 Cable Modem

A cable modem is designed to operate over cable TV lines (coaxial cable) to provide high-speed Internet access. This technology takes advantage of the unused capacity of cable television; one channel is used for downstream traffic and another is allocated for upstream. The signal sent to and from the user's PC communicates directly with a Cable Modem Termination System (CMTS) at the cable TV provider's facility. The traffic is then sent from the CMTS to an ISP network backbone. The cable modem architecture utilizes the bus topology in which several modems attached to the "network" share the available bandwidth provided by the cable company. The actual bandwidth for service over a cable TV line is up to 27 Mbps downstream and 10 Mbps upstream; however, due to limitations based on the cable company's line rate and the cable modem itself, 1.5 Mbps is a more realistic data rate.

There are three types of cable modems—external modem, internal modem, and interactive set-top cable box. A number of different cable modem configurations are possible. See *Figure 4-4, Cable Modem Connection Model,* for an example of remote access connectivity using a Cable Modem.

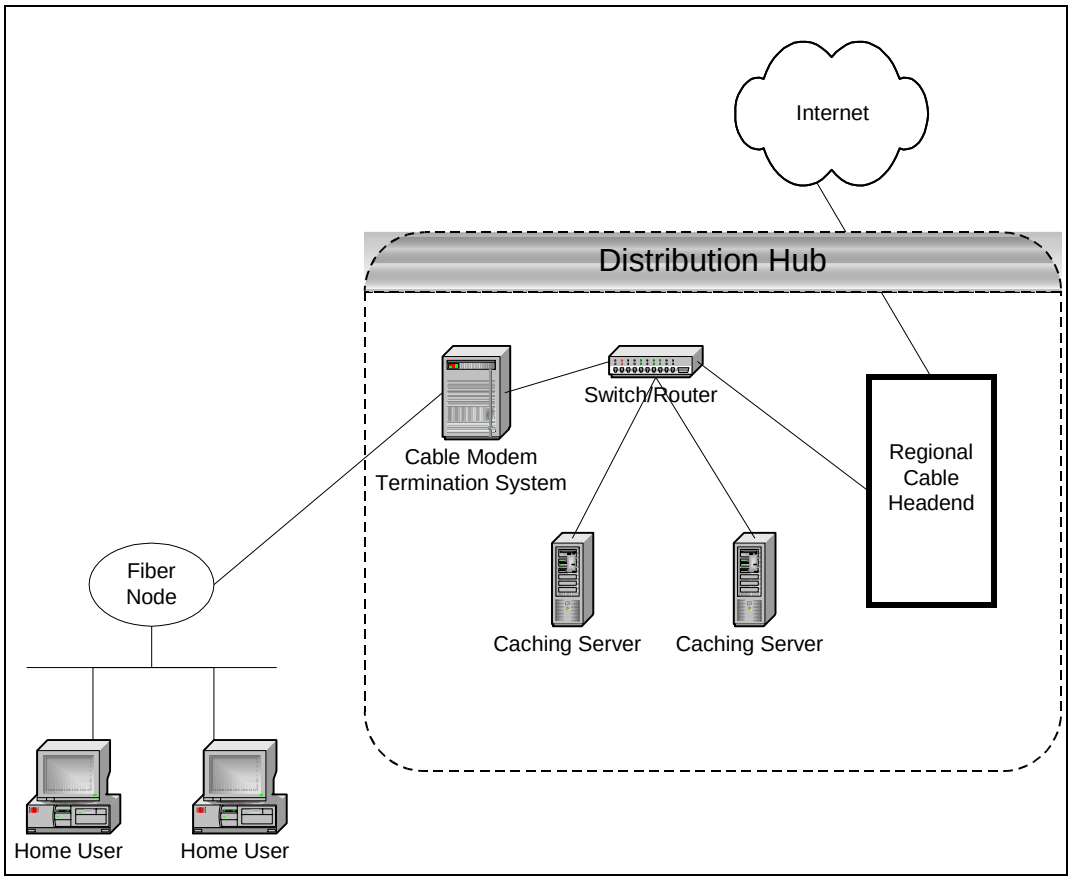

Figure 4-4. Cable Modem Connection Model

4.1.4 Satellite

A satellite Internet connection consists of an upstream (outgoing) and downstream (incoming) data connection to and from a computer through a satellite with the use of IP multicasting. The satellite in a fixed or geostationary (GEO) position maintains a connection to antennas on earth because the satellite orbits the earth at the exact speed of the earth's rotation. A geostationary transaction requires two round trips between the earth's surface and transponders orbiting over 22,000 miles above the equator. The terrestrial based data transfer between the earth station satellite system and the accessed Internet site occurs at uplink speeds of 50 to 150 Kbps and downstream speeds ranging from about 150 Kbps to more than 1200 Kbps. Internet traffic, server capacity, and download file size are all factors that determine the speed of the signal.

There are other types of broadband communication satellites and they are categorized according to their orbit. Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) satellites are much more costly and complex than GEO satellite systems. LEO/MEO systems require extensive tracking gateway earth systems, which must be capable of maintaining contact with multiple satellites.

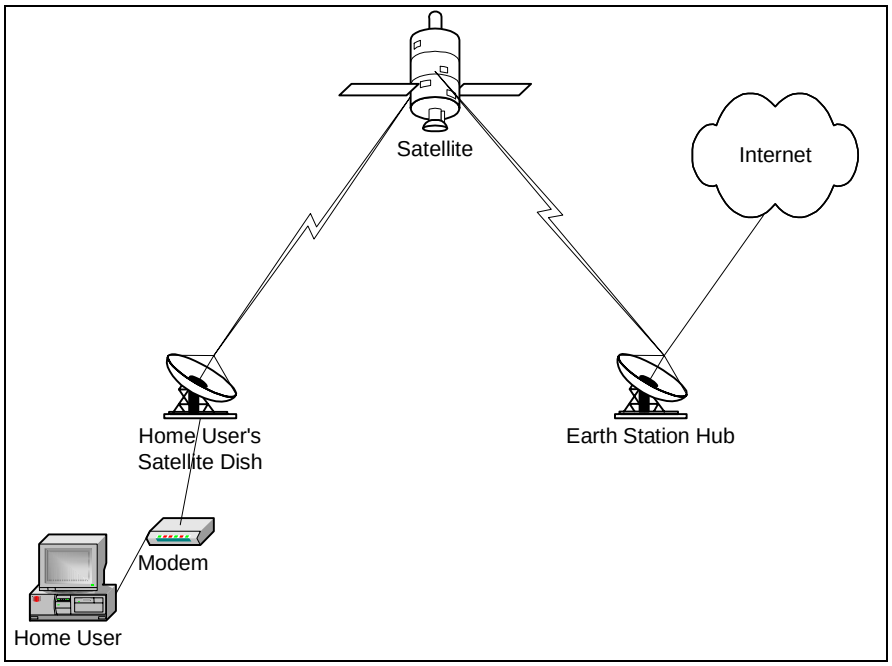

Figure 4-5. Broadband Satellite Connection Model

4.1.5 Wireless

Wireless technologies can provide significant productivity improvements for mobile DOD employees; however, they can also expose government information systems to severe security vulnerabilities. The security function of the wireless 802.11 standard is inadequate, leading to attacks such as "war driving" and "drive by hacking." Frequent warnings and advisories have demonstrated the inherent security flaws in the Wired Equivalent Privacy (WEP) standard, which is part of the 802.1x protocol suite. Wireless communication spans a wide range of different technologies including fixed microwave links, wireless LANs, data over cellular networks, wireless WANs, satellite links, digital dispatch networks, and more.

Wireless technologies can be divided into several categories to include fixed, mobile, portable, and infrared (IR). Fixed wireless systems are typically located in homes and offices where specialized modems provide connectivity to the Internet. IR wireless uses devices that send data using IR radiation. Portable and mobile wireless systems include devices such as cell phones and Personal Digital Assistants (PDAs) and operate using autonomous battery power.

- *(EN735: CATI I) The IAO will ensure both the site and remote user comply with applicable requirements in the Wireless STIG.*

- *(WIR0060: CAT II) The IAO will ensure wireless systems (WLAN, WPAN, and WWAN) are compliant with overall network security architecture, appropriate enclave security requirements, and DODD 8100.2 before the system is installed.*

- *(WIR0320: CAT II) The IAO will ensure SNMP is disabled on wireless remote access devices.*

- *(SRC190: CAT I) The IAO will ensure file and print sharing is disabled on wireless clients.*

- *(EN740: CAT II) The IAO will ensure additional encryption, beyond WEP, will be employed, such as encrypted VPN, SSL, or SSH.*

- *(EN750: CAT III) The IAO will ensure the NetBIOS protocol is disabled over TCP on wireless clients.*

- *(EN750: CAT III) The IAO will ensure all services not needed for operational use are disabled on wireless clients.*

- *(EN760: CAT III) The IAO will ensure the remote user does not install wireless hardware or software or otherwise alter the configuration on government-controlled devices for connecting to a wireless network at remote work sites without prior approval.*

- *(EN770: CAT III) The IAO will ensure personally owned wireless devices are not used for remote access to government systems.*

4.1.6 Security Implications of Broadband Connections

The risk of exposure to vulnerabilities, malicious attackers, and opportunistic individuals is 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 (ISP), 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 Local Area Network (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.

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, operating system secure configurations, anti-virus software with updated signature files, and encryption. Specific requirements for securing devices such as laptops and home PCs are contained in *Section 5, Securing Remote Access Devices*.

- *(SRC190: CAT I) The IAO/remote user will ensure file and print sharing is disabled on remote access devices, as there is an inherent risk associated with the technologies employed by broadband architectures. This will apply to all operating systems.*

4.2 Dial-up Connections

With the need for increased employee mobility, remote dial-in access security has become an issue of great concern. An installation security policy should not only examine network

protection from Internet or web-based access, but also against unauthorized dial-in access. While access to the private network can be restricted by physical security at the workplace (i.e., badges and PIN numbers), along with mandatory passwords to log into the network, accessing the same private network remotely presents additional challenges. Restricting remote access to authorized users and controlling what network services are provided to mobile users will require collaboration between various components within the network infrastructure.

The analog modem uses a standard telephone line to connect to an ISP, communications servers or terminal host adapters, and network access servers. Modems are still widely used in the Government and private sector to connect remote users to the network infrastructure. Modems can also provide an unchecked gateway to sensitive data within the DOD's computing boundaries; therefore, the need to secure them and the device they dial into still exists.

Long-term connections are not practical for dial-up access; therefore, 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 a remote user dials into a device, they are usually provided a dynamic IP address as opposed to static, 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.

This section will address the dial-in remote access model. The remote access infrastructure should determine that a dial-in user is indeed who they say they are, restrict access to authorized network resources and services, and log the entire event. These procedures will provide authentication, authorization, and auditing.

4.2.1 Remote and Network Access Server

A Network Access Server (NAS) is a device that provides for the initial entry point into a network. The NAS provides all the services that are normally available to a locally connected user (e.g., file and printer sharing, database and web server access, etc.) Permission to dial in to the local network is controlled by the NAS and can be granted to single users, groups, or all users. NAS servers such as Windows NT RAS, Shiva LanRover, and CISCO AS5200 have interfaces both to the network backbone and to the switched telephone service provider. These servers receive calls from remote clients or hosts that want to access the network using analog dial-up services that can support connections up to 56 Kbps. Access routers (e.g., Ascend Pipeline 4004 and Cisco AS5200) with an ISDN interface, as well as remote access servers with ISDN cards, support connections up to 128 Kpbs. NAS and RAS devices can also interface with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control Systems (TACACS).

Multi-modem adapter cards that plug into Windows NT servers can provide a low-cost analog alternative to a dedicated remote access server. These cards fit into any Intel-based server and support up to 24 communication ports bound to NT RAS services. Some multi-modem cards support RSA SecurID for user authentication, which can be used with a RADIUS server to

provide user management, session management, and accounting services. Because server cards can be installed on primary or backup domain controllers, a network administrator may inadvertently give all dial-in clients "log on locally" rights to the network. If a few permissions were to be configured improperly, a security breach could be created. Furthermore, some multi-modem cards rely solely on NT RAS for user authentication, and do not allow for the use of the approved authentication servers.

- *(NET1595: CAT II) The NSO will ensure remote access servers/cards will not be used to provide remote access services unless they have the ability to support authentication servers.*

- *(SRC290: CAT II) The NSO will ensure remote access server cards will not be installed and implemented on any Windows domain controller.*

4.2.2 Dial-in Connectivity

Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) are the two communication protocols that enable a remote computer to connect to a network over standard asynchronous serial lines. Both SLIP and PPP provide the ability to transport TCP/IP traffic over the serial lines; however, PPP can support additional protocols such as IPX and AppleTalk.

The most significant advantage PPP provides is authentication and configuration negotiation. With SLIP, the remote user must configure communication parameters such as maximum transmission unit (MTU) and maximum receive unit (MRU). In addition, SLIP does not support authentication; hence, chat scripts must be used to provide some form of authentication before SLIP is started. On the other hand, PPP negotiates the configuration parameters at the start of the connection to include which authentication method will be used, as well as all required transmission parameters. PPP provides authentication methods such as Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). These protocols are used for authentication at the Data Link Layer—that is, between the remote client and the remote access server. These methods provide the means for the remote client to send logon userid and password information to the remote access server.

Authentication takes place when the remote node attempts to establish a PPP session with a remote access server. The remote access server can be configured to use PAP, SPAP, or CHAP to authenticate the remote node. After the link is established, the remote node is required to send the username and password pair to the remote access server.

PAP transmits the username and password as plain text. NT RAS server supports SPAP to allow remote access to Shiva clients. Unlike PAP, SPAP does send encrypted passwords over the communication link as opposed to clear-text passwords. CHAP offers additional security by using encrypted keys during communication between the remote access server and the remote node. With CHAP, PPP sends a randomly generated challenge string to the client, along with its hostname. The client uses the hostname to look up an appropriate key, combines this with the challenge, and encrypts it with a one-way hashing algorithm. The resulting string is returned to the server, along with the client's hostname. The server performs the same computation as the

client on the challenge string. The server will only allow the client to connect if its computation result is identical to that received from the client. One of two encryption algorithms (DES or MD5) can be chosen when using CHAP. DES is the default option used by CHAP; however, MD5 is the recommended encryption algorithm. An additional security feature of CHAP is that client authentication is not only required at initial connect time but the server sends challenge strings to the client at regular intervals to detect if the client has not been replaced by an imposter. These two security features working together help to ensure data transfer security in the PPP network.

MS-CHAP is the most secure encryption algorithm that NT supports and is Microsoft's version of the RSA Data Security's MD4 standard. MS-CHAP uses a one-way hash function to produce a message-digest algorithm. A hash function takes a variable-sized input and returns a fixed-size 128-bit string. This type of algorithm produces a secure checksum for each message, making it almost impossible to change the message if the checksum is unknown. MS-CHAP V2 provides two-way authentication or mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.

- *(NET1610: CAT II) The NSO will ensure all remote clients and remote access servers are configured to use PPP instead of SLIP to provide the dial-up communication link.*

- *(NET1610: CAT II) The NSO will ensure CHAP with MD5 or MS-CHAP with MD4 encryption is used to authenticate the remote client.*

4.2.3 Centralized Access and Configuration Administration

Regardless of the dial-in configuration or devices used, the remote access servers should not reside within the secured private network. A centralized access point controlled by a firewall must be established to avoid setting up any direct dial-in lines to desktop machines or servers that could grant remote users—and trespassers—unlimited access to private network resources. Every exception to this requirement presents a potential back door into the network.

Configuring a central point of access is vital to the overall security of a remote access infrastructure. Only services that are absolutely needed for end users to conduct business should be allowed through the firewall from the central point of access. A sound approach would be to place dial-in users under the same access policy as those connecting via VPN. This can be accomplished by placing the remote access server either in the DMZ or within a screened subnet where the VPN gateway resides. The screened subnet architecture provides a layered defense ensuring only authorized users are permitted access to the internal base network while providing some 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 it from any hosts within or outside the private network.

In the case of an NT RAS server, a Windows NT, or 2000 platform with RAS card installed, any software that is not needed must be uninstalled. Furthermore, only those network services required to support the server and support remote access services should be enabled.

- *(N/A: CAT II) The IAO will ensure the architecture and dial-up connection method to a network access server or communications server is secured in accordance with the applicable sections in the Network Infrastructure STIG.*

- *(NET1595: CAT II) The NSO will ensure the RAS/NAS server is located in a dual homed screened subnet, thereby providing some protection while enforcing remote user access under the same remote access policy as those connecting by VPN.*

- *(N/A: CAT I) The NSO will ensure remote users do not have access to the management, control, and configuration functions of the remote access server.*

- *(NET1590: CAT II) The NSO will ensure a RAS/NAS server does not have any software or service installed on it or services enabled that are not required to support the server or remote access services.*

- *(NET1425: CAT III) The NSO will ensure auditing and accounting are enabled on the RAS or NAS server and will log user dial-in session statistics, at a minimum.*

- *(NET1420: CAT II) The NSO will ensure a dial-up solution requires two-factor authentication for the remote access user.*

5. SECURING REMOTE ACCESS DEVICES

Remote access from any location is considered untrusted. Whether the method consists of dialing into a Remote Access Server or using a form of broadband technology, the following general guidelines must be followed for securing remote devices, to include but not limited to laptops, workstations, and PDAs. The requirements in the following subsections will be met for Administrative Access and to the fullest extent possible for End-User and Limited Access.

- *(NET0140: CAT III) The SA will ensure when a modem is present, in-coming dial-up capability to the user's remote device (e.g., laptop, workstation, etc.) will be disabled.*

- *(SRC192: CAT III) The SA will ensure all remote access devices are configured so that the operation of the NIC and the modem is mutually exclusive (i.e., using hardware profiles, if the NIC is initialized, then the modem must be disabled).*

- *(SRC360: CAT III) The remote user will ensure no changes to the security configuration of software or hardware of a Government controlled remote access device will be made without prior approval of the IAO.*

- *(SRC361: CAT III) The IAO will ensure there is a mechanism in place to scan or review a remote access device for vulnerabilities, malicious code, or other security violations, immediately upon connection to a DOD network when the remote user returns to their official duty station.*

5.1 Minimum Operating System Requirements

Securing the remote access workstation, laptop, or other device is the first step to secure remote access to a DOD network. There are many DOD, DISA, and NSA policies detailing operating system security requirements. It is each DOD component's responsibility to adhere to the appropriate policy for their particular organizations. However, at a minimum, the following sections detailing additional requirements will apply for any remote access to a DOD network or resource.

- *(EN510: CAT II) The IAO will ensure the operating system of any remote access device complies with the appropriate Operating System STIG.*

- *(SRC360: CAT III) The IAO will ensure in addition to being STIG compliant, the operating system will have controls that will not allow a user to change the established security settings on the device without approval.*

5.2 Personal Firewalls

Attackers are constantly scanning and probing the Internet and associated IP addresses for known vulnerabilities. Although it is a requirement that some Government agencies install and configure firewalls to minimize the threat to internal systems, not all agencies have been able to implement firewall architectures. Therefore, in an effort to mitigate attacks on DOD systems and thwart the efforts of attackers, personal firewalls are required on remote access devices. Personal firewalls create an additional defense mechanism and help minimize Distributed Denial of Service (DDoS) attacks, where numerous compromised systems attack a single target, thereby creating a denial of service for legitimate users of that targeted system. Firewalls also help to prevent Trojans, hijacking of data, and the introduction of "backdoors" into a system.

- *(SRC1630: CAT II) The IAO will ensure any device that accesses a DOD network remotely will have a personal firewall installed (if technically capable). The firewall must be approved and distributed by DOD CERT. (Personal firewalls are available at the www.cert.mil web site.) This includes all devices that are capable of dialing in via modem.*

- *(SRC1631: CAT III) The IAO will ensure the site has developed a configuration baseline and policy regarding the use and configuration of personal firewalls for remote access clients.*

- *(SRC410: CAT I) The IAO will ensure all known DDoS ports and NetBIOS ports will be bi-directionally blocked by the personal firewall. Refer to the Network Infrastructure STIG, Appendix G, for additional port blocking guidance.*

  Following are the minimum DDoS ports required to be blocked by the firewall:

  TRINOO DDoS systems
  27665, 31335, 27444

  Back Orifice system
  31337

  Stacheldraht DDoS system
  16660, 65000

  TrinityV3 system
  33270, 39168

  T0rn rootkit system
  47017

  Subseven DDoS system and some variants
  6711, 6712, 6776, 6669, 2222, 7000

- *(SRC400: CAT I) The IAO will ensure all outgoing packets, except those necessary for operation (e.g., SMTP, SSL, HTTP, HTTPS, FTP, etc.) are blocked at the personal firewall. Refer to the Network Infrastructure STIG, Appendix G, for port blocking guidance.*

- *(SRC420: CAT II) The IAO will ensure a "deny by default" posture is enforced on personal firewalls. The IAO will ensure only ports or services required for operational use are open on the firewall and that all open ports are documented.*

- *(SRC430: CAT III) The NSO/IAO will ensure the personal firewall is configured to log all inbound connections.*

- *(SRC440: CAT III) The remote user will view the firewall logs on a daily basis and report any unusual events or suspicious activity to their security officer.*

- *(SRC450: CAT III) The IAO will ensure the personal firewall is configured at a minimum to a "Medium" level of security to include the following:*

  - *Blocking all Internet access until expressly permitted by the user*
  - *Silently block unused ports*
  - *Prompt for Java Applet and ActiveX controls*

- *(SRC451: CAT III) The IAO will ensure the personal firewall is configured to alarm the user for all suspicious events or intrusions.*

- *(SRC452: CAT III) The IAO will ensure if the capability exists within the firewall software to report errors back to the vendor, the messages will either be redirected to the DOD site for review by the NSO, or disabled.*

5.3 Web Browser Security

Web browsers, in and of themselves, create additional security risks to DOD networks and systems. Because web browsers are used extensively for Internet access, they are popular targets for attackers. Without proper security mechanisms and configuration, browsers can disclose DOD data, spawn an attack on DOD assets, or render the system inoperable. Mobile code, such as JavaScript and ActiveX, is particularly vulnerable to malicious attacks. Mobile code is a powerful tool used by developers to run mini-applications or scripts, and they are somewhat easily altered.

- *(N/A: CAT III) The IAO will ensure web browsers are secured in accordance with the Desktop Application STIG, Version 1, Release 1.*

- *(EN710: CAT III) The IAO will ensure the Memorandum for Secretaries of the Military Departments, Policy Guidance for use of Mobile Code Technologies in DOD Information Systems is adhered to. (See Appendix F, Mobile Code Policy, for additional details on Mobile Code.)*

- *(DTBG001: CAT II) The IAO will ensure the web browser software used on all remote access devices is the most current supported release with all current, applicable security-related patches installed.*

- *(DTBG007: CAT II) The IAO will ensure the web browser will be capable of supporting 128-bit encryption.*

- *(N/A: CAT III) The IAO will ensure cookies are either disabled or accepted from the originating web site only.*

5.4 Anti-Virus Software

Virtually all computer systems are susceptible to viruses, malicious mobile code, Trojans, worms, etc. Therefore, it is necessary to take the appropriate steps in an attempt to mitigate the risk of "infection" or possible compromise to the system itself, or becoming an intermediary to an attack on a DOD network or other DOD systems.

The DOD CERT makes several anti-virus tools and software available for download from their web site at http://www.cert.mil/antivirus/antivirus_index.htm. These tools include anti-virus packages that can be used for laptops and wireless devices running Windows NT, 2000, XP, PALM OS, Windows CE, or EPOC. The CERT also makes documentation available for installation and configuration.

- *(DTAG004: CAT II) The IAO will ensure vendor supported, DOD approved, anti-virus software with the most recent virus signature definitions is installed on all remote devices.*

- *(N/A: CAT II) The IAO will ensure anti-virus software is configured in accordance with the Desktop Application STIG, V1R1.*

- *(DTAG009: CAT II) The IAO will ensure the anti-virus software is configured to scan automatically upon startup (once daily).*

- *(DTAG005: CAT II) The IAO will ensure the remote device is configured to update virus signatures every fourteen days or less, or when the CERT provides an updated virus definition list.*

- *(DTAG011: CAT II) The IAO will ensure the anti-virus software is configured to scan e-mail attachments, web site downloads, and all other files prior to placing them on any Government system. The configuration of the anti-virus software will be in auto-detect, auto-protect, or real time protection mode.*

- *(DTAG011: CAT II) The IAO will ensure the web browser download protection is enabled (e.g., Norton Anti-Virus has the ability to scan all downloaded files, if checked in the Options tab, under Auto-Protect).*

5.5 Passwords on Remote Access Devices

Password cracking software packages, such as John the Ripper, are widely available on the Internet. The first line of defense against attack of any computer system is a strong, unique, hard to crack password. All remote access devices, regardless of technology, must be password protected.

- *(SRC1562: CAT II) The remote user will ensure all devices used to remotely access the network are protected with hard to guess, unique passwords (i.e., the passwords used on remote access devices will not be the same as any other password).*

- *(SRC1561: CAT II) The IAO will ensure accepted password generation schemes to create passwords will be used. At a minimum, passwords will be created and maintained (i.e., they must be changed) in accordance with the requirements identified in the DODI 8500.2 IA Control IAIA-1.*

- *(SRC1562: CAT II) The IAO will ensure a schedule is in place to periodically check passwords using password-cracking software.*

5.6 Encryption

Encryption, although not a secure solution alone, is a powerful tool used to secure the privacy and integrity of data. There are two primary forms of encryption—asymmetric and symmetric. Public key encryption is a cryptographic asymmetric system that uses two keys—public to encrypt the data, and private to decrypt the data. Private Key or symmetric encryption, utilizes only one secret key to perform the encryption and decryption process. If a device, PC, or laptop is lost or stolen, it is important that the Government data contained on the device be as secure as possible to avoid compromise. The best means to protect the data is by encrypting the files on the device itself.

- *(SRC570: CAT II) The remote user will employ a FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) to encrypt Government data on the remote device. Windows 2000/XP Encrypting File System (EFS) is also an acceptable solution to protect the storage of data on a remote access device. If EFS is not a practical solution due to profile and certificate conflicts, a third-party encryption application is acceptable.*

NOTE: In order to use EFS for both a domain account and a local user account you must export the certificate and private key into the other profile.

- *(SRC580: CAT II) Remote users will encrypt all temporary folders (e.g., C:\temp, C:\windows\temp, Temporary Internet Files, etc.) so that any temporary files created by programs are automatically encrypted.*

- *(SRC580: CAT II) Remote users will encrypt folders instead of individual files so that if a program creates temporary files during editing, these will be encrypted as well.*

- *(SRC590: CAT II) The remote user will back up and store the private encryption key in a secure location (e.g., floppy disk, CD, etc.).*

- *(SRC600: CAT II) The IAO will ensure there is a mechanism in place for key recovery or data recovery to prevent loss of data if the user losses the encryption key.*

5.7 VPN Client

For a remote access VPN to be as secure as possible, the traffic should be both encrypted and integrity protected. That is to say, without encryption, an unauthorized person could access the data, and without integrity protection, encrypted traffic is susceptible to attacks and modification of data. The VPN client software communicates with a VPN device within the network infrastructure and establishes a secure connection over the Internet. It is strongly recommended that with any implemented VPN solution the VPN client should be from the same vendor.

- *(SRC1800: CAT II) The remote user will ensure Split Tunneling is disabled on the VPN Client (i.e., upon the establishment of a VPN connection to a DOD network, no other connections of any kind will be established [e.g., if home networks are used, no connection between the device and other home network devices will be established during a VPN session]).*

- *(SRC610: CAT II) The remote access user will not configure or change security settings of the VPN client without prior approval from the system or network administrator.*

- *(SRC620: CAT III) The IAO will ensure the remote user has complete instructions on the use of a VPN client used to access a DOD network or resource.*

- *(SRC630: CAT II) The IAO will ensure a VPN client supports and is configured for IPSec attributes such as 3DES, Tunnel encapsulation mode, and a FIPS 140-2 approved authentication algorithm.*

6. REMOTE ACCESS TO A DOD NETWORK

Regardless of the media the data traverses, or the method used to access a network, Enclave protection mechanisms must be in place to ensure security within specific security domains and across the DOD network backbone. The *STIG on Enclave Security* and the *Network Infrastructure STIG* outline in detail 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. At a minimum, the Enclave will include the following:

- A network intrusion detection system (IDS) at the Enclave perimeter
- Router Access Control Lists (ACLs) based on a policy of Deny by Default
- An application level firewall
- An internal network IDS

Any access to the site from outside of the Enclave must pass through the architecture without circumventing the security controls in place.

- *(NET1595: CAT II) The NSO will ensure placement of remote access communications devices complies with the architecture outlined in the Network Infrastructure and Enclave Security STIGs.*

NOTE: This PDI is regarding architectural configuration and placement (logical) rather than physical location.

- *(N/A: CAT II) The NSO will ensure all components and devices of the remote access infrastructure adhere to the Network Infrastructure STIG guidelines in relation to password management, in and out-of-band network management, ACLs, and general administration requirements.*

NOTE: This policy corresponds to the appropriate sections and policies in the Network Infrastructure STIG.

- *(EN450: CAT II) The NSO will ensure remote access device traffic/data will not bypass the security architecture as outlined in the Network Infrastructure STIG (i.e., all ingress traffic will pass through the firewall and Network IDS).*

- *(NET270: CAT II) The IAO will record all administrator passwords used on remote access and other communications devices (e.g., Communications Servers, NAS, RAS, routers, VPN devices, etc.) and store them in a secure or controlled manner.*

6.1 Virtual Private Networks (VPNs)

VPNs provide a variety of methods to protect network data integrity, confidentiality, and availability using techniques such as connectionless integrity, data origin authentication, traffic analysis, and access protection. A VPN is a private data network that maintains confidentiality by using encryption and security procedures across a shared public telecommunications

infrastructure. The data is transported or tunneled across a public or private network employing encryption technologies such as L2TP, PPTP, and IPSec. Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions.

Point-to-Point Tunneling Protocol (PPTP), an extension of the Internet's Point-to-Point Protocol (PPP), allows a host with PPP client support to use an ISP to connect securely to a server elsewhere in the local area network. Layer 2 Tunneling Protocol (L2TP) is an extension of PPTP, which enables VPN implementation by merging PPTP and Layer 2 Forwarding (L2F) protocols. L2TP does not include mechanisms for encryption or authentication and must obtain these services through use in conjunction with other devices or protocols.

Internet Protocol Security (IPSec) is the most widely used secure network protocol. IPSec provides VPN capabilities at Layer 3 of the Open System Interconnection (OSI) model, whereas PPTP and L2TP operate at Layer 2. IPSec consists of two packet encapsulation protocols—the Authentication Header (AH) that allows authentication of the sender; and the Encapsulating Security Payload (ESP) that supports both authentication of the sender and encryption of data. In addition, IPSec supports two encryption modes—transport and tunnel. Transport mode encrypts the data portion (payload) of each packet, but does not encrypt the header. Tunnel mode encrypts both the header and the payload, making this mode more secure. In either mode, the receiving side of an IPSec compliant device decrypts each packet.

VPNs can be divided into three categories—remote access, site-to-site, and extranet. The type of VPN technology employed is based on bandwidth requirements, resources, and differing security needs, all of which is determined by the function it will perform and impacts the placement of the device in the network infrastructure. Placement of the VPN should not adversely impact the Enclave security and all VPN traffic must pass through the Enclave Security Architecture. Although encrypted data (e.g., SSL, SSH, TSL) that enters the VPN tunnel does not need to be unencrypted prior to leaving the tunnel, the data must pass through the respective application proxy on the firewall. Host-to-gateway VPNs are preferred; however, if a host-to-host VPN is required to meet mission needs, it will be established between trusted, known hosts. (Refer to the *Network Infrastructure STIG*)

- *(EN390: CAT II) The NSO will ensure all VPN implementations adhere to the VPN section of the Network Infrastructure STIG.*

- *(NA: CAT II) The NSO will ensure all broadband remote user access (with the exception of dial-in) will be encrypted via VPN.*

- *(EN400: CAT II) The NSO will ensure VPNs are established as tunnel type VPNs that terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router). Location is not as paramount as being in compliance with DODI 8500.2 EBVC-1 "VPN traffic is visible to network IDS."*

- *(EN410: CAT II) The NSO will ensure all communications to/from the network will employ at a minimum a FIPS 140-2 approved data encryption algorithm (i.e., AES or 3DES). (See http://csrc.nist.gov/cryptval.)*

- *(NET1630: CAT II) The IAO/NSO will ensure remote access via VPN uses IPSec ESP in tunnel mode. For legacy support, L2TP may be used if IPSec provides encryption (DAA approval required), or another technology that secures using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(N/A: CAT II) The NSO will ensure data integrity is achieved with the use of 128-bit MD5 or 160-bit SHA.*

6.2 Access Controls

In order to gain access to a DOD network or resource, all users and system support personnel must have the required security clearances, authorization, and need to know, and must be instructed on organization security practices before being granted access to any information system.

- *(EN160: CAT II) The IAO will ensure a list of authorized users, with the required security clearance for remote access, will be developed and checked on a regular basis, and any unused/expired accounts will be removed from any network device. In addition, the IAO will use the DD Form 2875, or similar access authorization form, to validate users on systems for which there is no current access request documentation in place (e.g., VPN access, RAS).*

- *(NET0240: CAT I) The IAO will ensure all default manufacturer passwords are changed on any device used for remote access to include, but not limited to routers, switches, VPN devices, Network Access Servers, and Communications Servers.*

- *(NET0170: CAT II) The IAO will ensure all known backdoor userids and passwords will be removed from any communications device used for remote access. If the default accounts cannot be removed, then one of the following mitigating actions will be performed:*

  - *Disable and/or rename default accounts*
  - *Install new hardware*
  - *Disable all administrative accounts*

- *(NET1453: CAT III) The IAO will ensure periods of inactivity in excess of 30 minutes will time out and disconnect the remote access user from any device, server, network, or resource they are accessing.*

- *(NET0340: CAT II) The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.*

6.2.1 Authentication, Authorization, and Accounting (AAA)

An AAA server manages user requests for access to computers or network resources. Authentication is the mechanism for identifying users before allowing access to a network component. Authorization is the method used to describe what users have the right to do once they have been authenticated. Accounting or auditing is the component that keeps track of the services and resources accessed by the users. This information can be used later for resource tracking or troubleshooting.

AAA servers provide services by interacting and managing account databases and directories containing user information with network access points and gateway servers. AAA services allow for the enforcement of policy, auditing of user activity, and access to network resources. The general methods by which devices or applications communicate with an AAA server are the Remote Authentication Dial-In User Service (RADIUS) specification or Terminal Access Controller Access Control System (TACACS+) protocol.

RADIUS is an IETF proposed standard (RFC2865) for securing network components against unauthorized access. RADIUS can be used to provide authentication, authorization, and accounting services. RADIUS is a distributed client/server based architecture used to pass security information between access points and a centralized server. Most vendors support RADIUS specification in their remote access servers as well as their VPN network gateways for user authentication. A single RADIUS server with a single authentication database can be used to authenticate all users dialing into multiple remote access servers, thus simplifying management of users and associated rights.

All communications between a RADIUS client and server are authenticated by a shared secret key that is never sent over the network. In addition, user passwords contained in RADIUS messages are encrypted. The remote access server takes authentication information, such as a username and password, and passes this information to the RADIUS server. The username and password information exchanged between the remote access server (now the RADIUS client) and the Radius server is encrypted before it traverses the local area network. Thus, the remote access authentication information is protected against sniffers that may have breached the network. The RADIUS server then validates the password against either its database, a NetWare Bindery, a NetWare Directory Service, or against an NT Primary Domain Controller (PDC) user database. If the user has access privileges to the network, the RADIUS server notifies the remote access server to allow the connection. In addition, the RADIUS server sends back the user's profile to the remote access server. The profile can include information such as the user's IP address, the maximum amount of time the user can remain connected to the network, and the phone number the user is allowed to dial to access the network.

Another protocol that provides authentication services is the Terminal Access Controller Access Control Systems (TACACS) protocol. Originally, described in RFC 1492, it has been reengineered over the years by Cisco and is supported on many routers and network access servers found in enterprise networks today. The current version is called TACACS+, which includes many enhancements made to the original TACACS and Extended TACACS or XTACACS. TACACS+ improves on TACACS and XTACACS by separating the functions of authentication, authorization, and accounting by encrypting all traffic between the TACACS

client and the TACACS server. Both TACACS and XTACACS lack many features that TACACS+ and RADIUS offer. Furthermore, both TACACS and XTACACS have reached end-of-maintenance support; hence, they should no longer be used as an authentication protocol.

TACACS+ separates authentication, authorization, and accounting, whereas RADIUS provides a user profile along with the authentication. Consequently, a TACACS+ implementation does not require a configuration of all three. Other differences are TACACS+ uses TCP as a transport whereas RADIUS uses UDP, and TACACS+ will encrypt the entire packet payload whereas RADIUS encrypts only the user password.

The CiscoSecure access control server (ACS) can be used to authenticate users by centrally controlling dial-in access to a Cisco network access server such as the 2509, 2511, 3620, 3640, and AS5200. CiscoSecure can authenticate users against the operating system user database, the CiscoSecure User Database, a token-card server's database, or a Novell Directory Services (NDS) Database. Using either the RADIUS or TACACS+ protocol, the NAS sends all dial-in user access requests to the CiscoSecure ACS for authentication and authorization of privileges by verifying the username and password. The CiscoSecure server then returns a success or failure response to the network access server that permits or denies user access.

Kerberos, an IETF standard (RFC1510) as a network authentication system, provides strong authentication for client/server applications by using secret-key cryptography. This mechanism can verify the identities of two users or network components. This authentication is performed using a trusted third-party service using conventional shared-secret-key cryptography. In this system, a client would request the credentials of the party they wish to contact from the trusted authentication service. The communications between all parties are encrypted using known secret keys or session keys issued from the authentication service. After two users or network components have been authenticated, Kerberos can be used to provide confidentiality and data integrity services.

User authentication using RSA's SecurID is accomplished through an RSA ACE/Server that functions as an authentication server. When a user attempts to access the network via dial-in, the RSA ACE/Agent that is integrated in the remote access server, initiates an RSA ACE/Server authentication session. Most leading remote access server, firewall, VPN, and router products have built-in RSA ACE/Agents for compatibility with RSA SecurID two-factor authentication. For example, Cisco IOS includes RSA ACE/Agent software code, so that each Cisco router or network access server can authenticate directly against an RSA ACE/Server to provide RSA SecurID authentication. RSA ACE/Server can also be used in conjunction with a primary user authentication and authorization services such as a LanRover internal user list, a Shiva User List server, a TACACS+ server, or a RADIUS server.

RSA's strong two-factor authentication is based on something known. The first factor is a Personnel Identification Number (something you have); the second factor is the SecurID token. The numeric token code is displayed on the card and changes every 60 seconds in conjunction with the ACE/Server database. The combination of the PIN + Tokencode = the Passcode. Because the token code changes every 60 seconds, the passcode is unique to each access session requested.

NetWare Bindery is a security protocol that runs on a NetWare server in the network and communicates with a RAS device over IPX. NetWare Bindery has been largely succeeded by Novell Directory Services (NDS). NetWare Bindery was riddled with Year-2000 bugs; hence, the NetWare 4 operating system replaced the bindery name services with NDS.

Single-factor authentication is based on a simple premise (what you know, i.e., a password). Single-factor authentication is analogous to no security at all, as passwords can be very easily compromised. In contrast, two-factor authentication is not limited to what you know. Two-factor authentication requires the use of two separate pieces of information unique to the user, to include two of the following:

- Something you are (Biometrics)
- Something you know (PIN, passphrase)
- Something you have (token)
- Something you can do (sign your name)

- *(NET1451: CAT II) The NSO will ensure one of the following methods will be used to authenticate all remote access users—RADIUS, TACACS+, CiscoSecure ACS, or SecurID. Other secure authorization, authentication, and accounting packages will have to be approved and documented on a case-by-case basis by the IAM.*

- *(NET1451: CAT II) The NSO will ensure NetWare Bindery is not used by a RADIUS server to authenticate remote users accessing a Novell network.*

- *(NET1451: CAT II) The IAO will ensure all remote connections will be identified and authenticated. Cryptographic-based authentication performed at the enclave boundary will be employed to ensure only authorized users have the ability to gain access to the network. The authentication mechanism will provide mutual authentication of the remote user and the enclave's boundary protection mechanism (CJCSM_6510).*

- *(NET1452: CAT III) The IAO will ensure any remote access solution will uniquely identify all users and the device, port, and resource they are accessing.*

- *(NET1451: CAT II) The IAO will ensure all remote users are required to use a form of two-factor authentication to access any network resource to include dial-in devices, VPNs, etc.*

- *(NET1452: CAT III) The IAO will ensure each communications device that a remote user accesses (e.g., RADIUS, TACACS+, VPN device) will have the ability to log date, time, userid, event, MAC address or DHCP assigned IP address, success or failure of the event, etc.*

- *(NET1452: CAT III) The IAO will ensure all authentication failures or violations are logged. The audit logs will contain, at a minimum, all user identification information, date, time, origin of the event, and type of event.*

- *(NET1455: CAT III) The IAO will ensure audit logs for any remote access server authentication mechanism are maintained for no less than a period of 30 days on-line, and one year off-line.*

- *(NET1456: CAT III) The IAO will ensure audit logs are viewed on a daily basis and set to alarm/notify the administrator of moderate to severe security events that may be detected.*

6.3 Classified Remote Access

To ensure security within a classified environment, strict controls must be in place prior to any outside, remote access to the classified network or resource. NSA, DISA, and the DOD have stringent policy on the access, storage, location, and containment of all classified data and processing. Prior to any form of remote access to a classified network, all policy must be followed.

- *(NET1441: CAT I) The IAO will ensure an NSA Certified remote access security solution (e.g., HARA) is in place for remote access to a classified network and will only be used from an approved location.*

  - *The solution will be used in accordance with all NSA and DOD policy and guidelines.*

  - *The solution will use a High Assurance (Type 1) Link Encryptor to provide high assurance link protection (confidentiality, integrity, authentication), using NSA-certified cryptographic components, between the remote user and DOD enclaves or other computing environments. A High Assurance (Type 1) Media Encryptor to provide high assurance protection (confidentiality and integrity), using NSA-certified cryptographic components, to a remote user's hard-drive and removable media.*

  - *The NSA Type 1 link encryption device will be kept in the user's possession at all times or stored in accordance with policy applicable to classified storage.*

  - *The NSA Type 1 link encryption device will be stored separately from the computer when not in use.*

- *(SM050: CAT III) The IAO will ensure the device accessing the classified network is Government Owned/Leased equipment and protected to the classification level of the data that the device is able to access.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense 5200-28-STD, "DOD Trusted Computer System Evaluation Criteria," December 1985.

Public Law 100-235, 100th Congress, An Act cited as the "Computer Security Act of 1987," 8 January 1988.

Department of Defense Directive (DODD) 5200.28, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency Instruction (DISAI) 630-225-7, "Internet, Intranet, and World Wide Web," 6 September 1996.

Department of Defense Directive (DODD) 5200.40, "DOD Information Technology Security and Accreditation Process (DITSCAP)," 30 December 1997.

Memorandum for Secretaries of Military Departments, et al, "DOD Public Key Infrastructure," 12 August 2000.

Public Law 106-346, Section 359, Attachment 1, Memorandum to Executive Departments and Agencies, Congressional Federal Telework Mandate 2001, 23 October 2000.

Memorandum for Secretaries of Military Departments, et al, "Policy Guidance for the Use of Mobile Code Technologies in Department of Defense (DOD) Information Systems," 7 November 2000.

NSA Remote access secure program transition GUIDELINES, Version 1.0, March 31, 2005

DISA Computing Services Security Handbook
Enclave Security STIG

Network Infrastructure STIG

NIPRNet STIG

Desktop Application STIG

UNIX STIG

Web Application STIG

DNS STIG

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

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND),” 15 March 2002.

National Institute for Standards and Technology (NIST), Special Publication 800-46, “Security for Telecommuting and Broadband Communications,” D. Richard Kuhn, Miles C. Tracy, Sheila E. Frankel, August 2002.

Defense Information Systems Agency (DISA) Naming Convention Standards, October 2002.

DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), 14 April 2004.

DOD Directive 8500.1, Information Assurance, 24 October 2002

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

Secretary of the Navy Instruction (SECNAVINST) 5239.2, “Department of the Navy Automated Information Systems (AIS) Security Program,” 15 November 1989.

Army Regulation (AR) 380-19, “Information Systems Security,” 1 August 1990.

Air Force Systems Security Memorandum (AFSSM) 5007, “A Methodology for Addressing DOD-Mandated ‘C2 by 92’ for Operational Air Force Systems,” 25 March 1991.

Defense Logistics Agency Regulation (DLAR) 5200.17, “Security Requirements for Automated Information and Telecommunications Systems,” 9 October 1991.

Navy Staff Office Publication (NAVSO Pub) 5239-15, “Controlled Access Protection Guidebook,” August 1992.

General Information Sites

http://www.gsa.gov	General Services Administration – DOD Telework Policy and Guide
http://iase.disa.mil	Defense Information Systems Agency Information Assurance
http://www.disa.mil/handbook/toc.html	DISA/NCS World Wide Web Handbook, Version 2
http://www.datahouse.disa.mil	DISA Instructions and Publications to include Telework Forms
http://www.cert.mil	Department of Defense Computer Emergency Response Team (CERT)
http://www.cert.org	Focal point for the computer security concerns of Internet users
http://csrc.nist.gov/publications	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.informationweek.com	Technology Information Site
http://www.cerias.purdue.edu	Center for Education and Research in Information Assurance and Security (formerly COAST)
http://www.microsoft.com/technet/security/current.asp	Microsoft Security Bulletin and Patch Listings
http://www.nipc.gov	National Infrastructure Protection Center (an FBI program)
http://nielsen-netratings.com	Internet Rating reports provided by Nielsen/Netratings, Internet audience measurement service.
http://disadtc.den.disa.mil	DISA Computing Services Standard Operating Environment Naming Standards

This page is intentionally left blank.

APPENDIX B. DEPARTMENT OF DEFENSE TELEWORK POLICY

The following are excerpts from the DOD Telework Policy as directed by Section 359 Public Law No.106-346. The complete policy is located at the following URL: http://www.telework.gov/.

Any implementing telework regulations or other guidance developed by DOD Components must comply with this policy, as well as the law from which it is derived.

D. POLICY STATEMENT

It is DOD policy that:

i. No classified documents (hard copy or electronic) may be taken by teleworkers to alternative work sites;

ii. Government-furnished computer equipment, software, and communications, with appropriate security measures, are required for any regular and recurring telework arrangement that involves sensitive unclassified data, including Privacy Act data, or For Official Use Only (FOUO) data;

iii. Where employees telework on an adhoc basis, personal computers can be used to work on limited amounts of sensitive unclassified material, on the basis that the teleworker must delete the files as soon as they are no longer required, and verify in writing that he or she has deleted all files containing Department information from personally owned computer hard drives.

iv. Employees who telework may be approved by the Component Designated Approving Authority (DAA) to use their personal computers and equipment for work on non-sensitive, unclassified data consistent with DOD policy. Personal computers may not access DOD systems or networks remotely. The employee is responsible for the installation, repair, and maintenance of all personal equipment;

v. Providing and/or installing Government-furnished equipment at alternative work sites is a matter for determination by the DAA in each Component. The Component will be responsible for the service and maintenance of Government-owned equipment. DOD remote access software may be installed onto Government-furnished computers to enable access to DOD systems and networks;

vi. Government-furnished equipment must only be used for official duties, and family members and friends of teleworkers are not authorized to use any Government-furnished equipment. The employee must return all Government-furnished equipment and materials to the agency at the conclusion of teleworking arrangements or at the Component's request;

vii. Teleworkers are responsible for the security of all official information, protection of any Government-furnished equipment and property, and carrying out the mission of DOD at the alternative work site;

a. Where it is determined by the DAA that Government equipment will be provided to the teleworker, excess property should be the first source of supply before considering the purchase of new equipment;

b. An employee who is approved for work-at-home telework must sign a safety checklist prior to commencement of teleworking.

APPENDIX C. CHECKLIST EXAMPLE

Remote Access Security Checklist	YES	NO
Anti-virus Software		
Is anti-virus software installed?		
Are the latest virus definitions installed and updated on a regular basis (weekly)?		
Is the anti-virus software performing a system scan at each boot?		
Personal Firewalls		
Is a personal Firewall installed (e.g., McAfee Desktop Firewall, Norton Personal Firewall)?		
Is the firewall configured to lock out network access during periods of inactivity (when the screensaver activates or the computer is not in use)?		
Are all DDoS and NetBios ports blocked as directed by the Network Infrastructure STIG, Appendix G? (e.g., 31337,6669,6776, 137-139, etc) (For a complete list, see your network/system administrator.)		
Is the firewall configured to log suspicious activity and alert the user, to include outbound connection attempts?		
Is the firewall set to at least a medium level of security?		
Operating System		
Is the Operating System STIG compliant?		
Are all security-related patches installed for the OS and any additional fixes as required by IAVAs?		
Are all security-related patches installed for additional software (e.g., Word, IE, etc.) and fixes performed as required by IAVAs?		
Is file/data encryption being employed?		
Internet Browser		
Is the Internet browser software (i.e., Netscape) configured according to the Desktop STIG?		
Is Mobile Code limited as directed in the DOD Mobile Code policy and as directed in the Desktop Application STIG? (ActiveX, JavaScript, etc.)		
Disaster Recovery		
Is all Government data being backed up on a regular basis?		
Is the device in a secure location or protected from non-Government usage?		
Are access controls in place to limit use by those who are not authorized to use Government equipment?		

This page was intentionally left blank.

APPENDIX D. MOBILE CODE POLICY

Mobile Code is the term given to software modules obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. An example is a workstation or laptop, where the web browser is executed without explicit installation or initiation of execution by the recipient.

Category 1 (Active X, Windows Scripting Host and Shell Scripts). Technologies in Category 1 exhibit a broad functionality allowing unmediated access to host and remote system services. Category 1 technologies have known security exploits with few or no countermeasures once access is gained (e.g., all or nothing decision [run with full power or do not run at all]). All end systems in DISA will be configured to disallow the execution of unsigned Category 1 mobile code obtained from outside the enclave boundary. Category 1 mobile code may be used in DOD information systems when it is signed with a DOD-approved PKI code signing certificate and the mobile code is obtained from a trusted source.

Category 2 (Java, MS Office VBA, Lotus Script, PerfectScript, and Postscript). Category 2 Mobile Code technologies have full functionality allowing mediated access and environment-controlled access to host system services. Category 2 technologies may have known security exploits, but also have known fine-grained, periodic, or continuous countermeasures/safeguards. Category 2 technologies may be used if they are obtained over a trusted channel (e.g., PKI server certificate, SSL, or SIPRNet) from sources specifically known to be trustworthy. All trusted channels will use some form of encryption. Where feasible, protections against malicious forms of Category 2 mobile code will be employed at the end-user workstation and at the enclave boundary.

Category 3 (JavaScript, JScript, VBScript, PDF, and Shockwave/Flash). Technologies in Category 3 support limited functionality, with no capability for unmediated access to workstation, host, or remote system services and resources. Category 3 technologies may have a history of known exploits, but also support fine-grained, periodic, or continuous security safeguards. Category 3 technologies may be used in DISA Information Systems.

Un-Categorized Mobile Code Technologies. Owing to the uncertain risk, Un-Categorized Mobile Code Technologies are prohibited unless explicitly authorized by the DOD CIO Control Board. This technology category will be blocked by all means available at the enclave boundary, workstation, and application layer.

For additional policy guidance and usage restrictions see *Assistant Secretary of Defense (C3I) Memorandum, Subject: "Policy Guidance for use of Mobile Code Technologies in Department of Defense (DOD) Information Systems," 7 November 2000.*

This page is intentionally left blank.

APPENDIX E. CERT® /CC INTRUDER DETECTION CHECKLIST

(www.cert.org)

Look For Signs that Your System May Have Been Compromised

- Examine log files for connections from unusual locations or for other unusual activity. You can use the Event Viewer to check for odd logon entries, failures of services, or odd system restarts. If your firewall, web server, or router writes logs to a different location than the compromised system, remember to check these logs as well. However, remember that this is not foolproof unless you log on to append-only media; many intruders edit log files in an attempt to hide their activity.

- Check for odd user accounts and groups. You can use the User Manager tool or the "net user," "net group," and "net localgroup" commands at the command line. Ensure that the built-in GUEST account is disabled if the system does not require guest access.

- Check all groups for invalid user membership. Some of the default NT groups give special privileges to the members of those groups. Members of the Administrators group can do anything to the local system. Backup operators can read any file on the system. PowerUsers can create shares.

- Look for invalid user rights. To examine user rights, use the User Manager tool under Policies, User Rights. There are 27 different rights that can be assigned to users or groups. Generally, the default configuration for these rights is secure.

- Check to see if unauthorized applications are starting. There are a number of different methods an intruder could use to start a back door program, so be sure to do the following:

  Check the Startup folders. Check all items in c:\winnt\profiles*\start menu\programs\startup folders. You can also examine all the shortcuts by selecting Start, Programs, Startup. Note that there are two startup folders—one for the local user and one for all users. When a user logs on, all of the applications in both the "All Users" and in the user's startup folder are started. Because of this, it is important to check all of the startup folders for suspicious applications.

Check the registry. The most common locations for applications to start through the registry are:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs
HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\KnownDLLs
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" line)
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" value)

Check for invalid services. Some backdoor programs will install themselves as a service that is started when the system boots up. Services can then run as any user with the "Logon as Service" user right. Check services that are started automatically and be sure that they are necessary. Also check that the services executable file is not a Trojan horse or backdoor program. A batch file to help gather information about NT services running on a system is available at **www.cert.org**.

- Check your system binaries for alterations. Compare the versions on your systems with copies you know that have not been altered, such as those from your initial installation media. Be cautious of trusting backups; they could also contain Trojan horses.

  Trojan horse programs may produce the same file size and timestamp as the legitimate version. Because of this, just checking file properties and timestamps associated with the programs is not sufficient for determining whether or not the programs have been replaced. Instead, use MD5, Tripwire, and other cryptographic checksum tools to detect these Trojan horse programs (provided that the checksum tools themselves are kept secure and are not available for modification by the intruder). You may want to consider using a tool (PGP, for example) to "sign" the output generated by MD5 or Tripwire, for future reference.

  Using anti-virus software will also help you check for computer viruses, backdoors, and Trojan horse programs. However, remember that malicious programs are continuously created, so it is important to keep your anti-virus software up to date constantly.

- Check your system and network configurations for unauthorized entries. Look for invalid entries for settings like WINS, DNS, IP forwarding, etc. These settings can be checked using the Network Properties tool or using the "ipconfig /all" command at the command prompt.

  Make sure that only the Network Services you want to have running on your system are listed in the Network Services configuration.

  Check for odd ports listening for connections from other hosts by using the "netstat –an" command. The following batch file parses out ports that are in a listen state and then tries to show what service may be running on that port. This batch file uses the well-known port numbers file, which can be retrieved from the following location: http://www.isi.edu/in-notes/iana/assignments/port-numbers.

- Check for unauthorized shares. You can use the "net share" command at the command prompt or use the Server Manager tool to list all the shares on a system. NT provides a way to show hidden shares by adding a "$" to the end of a share name. There are a few default share names that NT uses (such as PRINT$), but if you are not sharing a printer with other users, check to see why that share was created. If you notice an odd share name, the tools will show you the actual location on the system that is being shared. A drive or directory can have multiple share names. Each of these shares can have different permissions associated with them.

- Check for any jobs scheduled to run. Intruders can leave back doors in files that are scheduled to run at a future time. This technique can let an intruder back on the system (even after you believe you had addressed the original compromise). Also, verify that all files/programs referenced (directly or indirectly) by the scheduler and the job files themselves are not world-writable. To check for jobs currently pending, use the "**at**" command or the WINAT tool from the NT resource kit.

- Check for odd processes. You can use the Task Manager tool or the pulist.exe and tlist.exe commands from the NT resource kit at the command prompt to gather information about the processes running on your system. The utilities, pulist.exe and tlist.exe, are included in the NT resource kit. A number of shareware/freeware applications also exist to show what files are in use.

  With the **pulist** command, you can see who started each process. Services are usually associated with the SYSTEM account. The **tlist** command with the -t flag will show you what processes started child processes.

- Look throughout the system for unusual or hidden files. These can be used to hide tools and information (password cracking programs, password files from other systems, etc.). Hidden files can be seen with the NT Explorer. Select View, Options, Show all Files. To view hidden files at the command prompt type "**dir /ah**."

- Check for altered permissions on files or registry keys. Part of properly securing an NT system is to set the proper permissions on files and registry keys so that unauthorized users cannot start unauthorized programs (e.g., backdoors or keyloggers) or change system files. In order to check many files throughout your directory tree, you can use the XCACLS.EXE program that is part of the NT Resource Kit. The NT Security Configuration Manager can also be used to analyze your system against a configuration you have defined previously. This would help to determine what might have been modified.

- Check for changes in user or computer policies. Policies are used on NT systems to define a wide variety of configurations and can be used to control what users can and cannot do. Since a number of items are configured in the policy editor (poledit.exe), it is recommended to keep a current copy of the policies you create in case they are altered and you need to determine what was changed.

- Make sure the system has not been redefined to a different Domain. An intruder may attempt to gain Domain Administrator access to a workstation by changing the current domain to a domain that the intruder has control over.

- When searching for signs of intrusion, examine all machines on the local network. Most of the time, if one host has been compromised, others on the network have also been compromised.

APPENDIX F. GLOSSARY OF TERMS

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADP1	Automatic Data Processing Level 1
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
AIS	Automated Information System
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BOOTP	Boot Protocol
BSD	Berkeley Software Distribution
CAP	Connection Approval Process
CCSD	Commercial Circuit System Designator
CDP	Cisco Discovery Protocol
CERT	Computer Emergency Response Team
CIDR	Classless Inter-Domain Routing
CIP	Channel Interface Processor (Cisco product)
CJCS	Chairman Joint Chiefs of Staff
CMIP	Common Management Information Protocol
CMTS	Cable Modem Termination System
CNA	Computer Network Attack
CNO	Computer Network Operations
COI	Community of Interest
COMPUSEC	Computer Security
CONUS	Continental United States
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
CPPP	Compressed Point to Point Protocol
CS	Communication Server
CSLIP	Compressed Serial Line Interface Protocol
DAA	Designated Approving Authority
DDoS	Distributed Denial of Service
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Digital Encryption Standard
3DES	Triple Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DID	Defense-in-Depth
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DISN	Defense Information System Network

DLSw	Data Link Switching
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOD	Department of Defense
DOD-CERT	Department of Defense-Computer Emergency Response Team
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
EAL	Evaluated Assurance Level
EGP	Exterior Gateway Protocol
EIA/TIA	Electronic Industry Association/Telecommunications Industry Association
EIGRP	Enhanced Interior Gateway Routing Protocol
ELAN	Emulated LAN
ESP	Encapsulating Security Payload
FA	Firewall Administrator
FDDI	Fiber Distributed Data Interface
FEP	Front End Processor
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FTP	File Transfer Protocol
FSO	Field Security Office
FSO	Field Security Operations
GAO	General Accounting Office
GD	General Deployment
GEO	Geostationary
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
HDSL	High bit rate Digital Subscriber Line
HLC	Host LAN Controller
HP	Hewlett Packard
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
IANA	Internet Assigned Number Authority
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ICMP	Internet Control Message Protocol
IDNX	Integrated Digital Network Exchange
IDS	Intrusion Detection System
IECA	Interim External Certification Authorities
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
INFOCON	Information Operations Condition
INFOSEC	Information Security
INFOWAR	Information Warfare

IOS	Internetworking Operating System
IP	Internet Protocol
IPSEC	IP Security
IS	Information System
ISC	Internet Software Consortium
ISP	Internet Service Provider
IS-IS	Intermediate System to Intermediate System
IAM	Information Systems Security Manager
IAO	Information Systems Security Officer
ITSDN	Integrated Tactical Strategic Data Networking
JIS	Joint Interoperability System
JTF	Joint Task Force
JTFCNO	Joint Task Force Computer Network Operations
LAN	Local Area Network
LEO	Low Earth Orbit
L2F	Layer Two (2) Forwarding
L2TP	Layer Two (2) Tunneling Protocol
LRA	Local Registration Authority
MAC	Mission Assurance Category
MD5	Message-Digest Five Algorithm
MEO	Medium Earth Orbit
MIB	Management Information Base
NA	Network Administrator
NAS	Network Access Server
NAT	Network Address Translator
NetBIOS	Network Basic Input/Output System
NHRP	Next Hop Resolution Protocol
NIC	Network Information Center
NID/JID	Network Intrusion Detector/Joint Intrusion Detector
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIST	National Institute for Standards and Technology
NMS	Network Management System
NOC	Network Operations Center
NOSC	Network Operations Security Center
NSA	National Security Agency
NSO	Network Security Officer
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PDA	Personal Digital Assistant
PDI	Potential Discrepancy Item
PKI	Public Key Infrastructure
POC	Point of Contact
POP	Point of Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PR	Perimeter Router or Premise Router
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Service
RADSL	Rate-Adaptive Digital Subscriber Line
RCERT	Regional Computer Emergency Response Team
RFC	Request for Comments
RIP	Routing Information Protocol
RMON	Remote Monitoring
RNOSC	Regional Network Operations and Security Center (formerly ROSC)
RPC	Remote Procedure Call
SA	System Administrator
SDID	Short Description Identifier
SDSL	Symmetric Digital Subscriber Line
SHA	Shared Hash Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLIP	Serial Line Interface Protocol
SMs	Security Managers
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedure
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
STEP	Standardized Tactical Entry Point
SYN	Synchronization
SYSLOG	System Log
TACACS	Terminal Access Controller Access System
TCP	Transmission Control Protocol
TDY	Temporary Duty
TFTP	Trivial File Transfer Protocol
TSIG	Transaction Signatures
TSL	Transport Security Layer
TTY	Teletype
UDP	User Datagram Protocol

VCTS	Vulnerability Compliance Tracking System
VDSL	Very High Bit Rate Digital Subscriber Line
VLAN	Virtual LAN
VMS	Vulnerability Management System
VPN	Virtual Private Network
VTY	Virtual Teletype/Terminal
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WESTHEM	Western Hemisphere
WWW	World Wide Web
XML	Extensible Markup Language

This page is intentionally left blank.