NETWORK INFRASTRUCTURE

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 5, Release 2

29 September 2003

DISA
FIELD SECURITY OPERATIONS

This page is intentionally left blank.

TABLE OF CONTENTS

Page

APPENDICES

FIGURES

TABLES

This page is intentionally left blank.

SUMMARY OF CHANGES

General Changes:

- The previous release was Version 4, Release 2, dated 15 October 2002.

Section Changes:

- **Section 1.4 Authority**

  Update the DOD Directive from 5200.28 to New 8500.1 Directive Policies.

- **Section 1.6 DISA Information Assurance Vulnerability Management (IAVM Program /Vulnerability Compliance Tracking System Process**.

  Updated this paragraph to reflect correct VMS information.

- **Section 1.8 Waivers and Exemptions**

  Change this section name to **Extensions**.

- **Section 1.12 Physical/Personnel Security**

  Updated paragraph deleted DISA Westhem and updated document to read Computing Services.

- **Section 1.14 Information Operations condition (INFOCON)**

  Deleted section 1.14 and renumbered Section 1.16 to 1.15.

- **Section 1.16 Security Vigilance**

  Added requirement that all network devices must have a vulnerability assessment performed prior to deployment into the network infrastructure.

SECTION 2 – ENCLAVE ARCHITECTURE OVERVIEW

- **Section 2.1 Enclave Protection Mechanism**

  Replaced MVS entry with OS/390.

  Included reference to the DNS STIG.

  Changed JID and NID to External Network Intrusion Detection System and Internal Network Intrusion Detection System respectively.

SECTION 3 – NETWORK INFRASTRUCTURE

Moved the NIPRNet Connection Approval Process (CAP) requirement for connections to Section 3.2.

- **Section 3.1 Joint Intrusion Detector (JID) renamed to External NetworkIntrusion Detection System.**

  Changed section to read “near real time”.

  Moved requirement of access only via SSH from section 3.1.2 to 3.1.1.

- **Section 3.2 Leased/Dedicated Lines**

  Renamed 3.2 to External Connections

  Added Section 3.2.1 Leased/Dedicated lines

  Added Section 3.2.2 ISP Connections

  Added that an ISP connection requires approval by the GIG Panel.

  Added Section 3.2.3 Backdoor Connections

- **Section 3.3 Backdoor Circuits**

  Renamed to Backdoor Connections and moved to Section 3.2.3

  Moved 3.5.1 Network Layer Addressing to 3.3.

- **Section 3.5.1 Network Layer Addressing**

  Renamed this section to 3.3.

  Added the requirement for IPv4 only across operational DoD networks.

- **Section 3.3.1 IANA Reserved Addresses was added**

  Added the IANA reserved address blocks that need to be blocked by the ingress ACL.

  Moved the requirement for using RFC 1918 addresses to this section. Qualified this requirement for NIPRNet only networks.

- **Section 3.3.2 Network Address Translation was added**

  Moved requirement for NAT from firewall section to this section to collaborate with the requirement for using private addresses from RFC 1918.

- **Section 3.3.3 DHCP was added.**

  Provided explanation of requirement for assigning static IP addresses to communication devices.

  Added SIPRNet requirement for a minimum lease duration of 30 or more days.

- **Section 3.4.2.2 In-band Management.**

  Added requirement for encryption of remote administrative access sessions to network devices.

- **Section 3.5.2 Router Tables**

  Delete portion of this section, which lists definitions. This portion was a duplicate of the TABLE 1, BGP, EIGRP, IS-IS, RIP, and OSPF in the same section.

  Moved requirements for route table integrity and neighbor router authentication to section 3.5.3.

- **Section 3.5.3 Common Routing Hazards**

  Renamed this section to Route Table Integrity

  Moved requirements from section 3.5.2 to this section.

  Added clarification for neighbor router authentication.

- **Section 3.5.4 Router Accounts**

  Removed the reference to using SSH as this is irrelevant to router accounts and is being addressed in the in-band management section.

  Added the requirement that only one “emergency account” can be defined.

- **Section 3.5.5 Router Passwords**

  Removed the requirement that only privilege level 1 can be defined locally since the emergency account will need full privileges.

Removed the statement that encryption mechanisms are only used if there is no TACAS+ server.

- **Section 3.5.8 Router Global Configuration Commands**

  Updated the minimum required IOS release level to 12.1(13).

  Included note to see Appendix I for Juniper router configuration requirements.

- **Section 3.6 Access control Lists (ACLs)**

  Added clarification for those ports and services that are permitted conditionally IAW Appendix G.

  Noted provisioning for placing the egress filter on the outside interface but noted that best practice was to place it on the internal interface going outbound.

- **Section 3.6.1 Filtering Traffic to Router**

  Removed the requirement for SNMP V3 and community string integrity since this will be addressed in the Network Management section to cover the entire network infrastructure.

- **Section 3.6.2.2 Exploit Protection**

  Made it clear that SYN Flood protection for servers must be done on either the firewall or the router—but not both.

.

  Added guidance for implementing the TCP intercept command.

- **Section 3.7.5 Configuration**

  Moved NAT requirement to section 3.3 Network Layering to be in conjunction with RFC 1918 addressing requirements.

  Added the caveat that SYN flood protection for the network is not required to be provided by the firewall if the protection has been implemented on the premise router.

- **Section 3.7.7 Implementation and Waivers**

  Change to Implementation and Description Report

- **Section 3.10.2 Virtual Local Area Networks (VLANs)**

  Removed requirement for MAC-based VLAN implementation using port security.

  Added new requirements to insure trunk link and tagged traffic integrity.

SECTION 4 –REMOTE ACCESS

- **Section 4.1 Dial-up Communications Servers**

  Moved this section to 4.4 and renamed Dial-up Communications

- **Section 4.1.1 Communications Server Management**

  Moved ANI option and device management compliance requirements to section 4.4.2 Remote Access Server/Network Access Server.

  Removed this section since remainder of the requirements are already covered in section 3.4.2 Device Management.

- **Section 4.1.2 Infrastructure Modems**

  Integrated this section with 4.4.1 Modems.

- **Section 4.1.3 Callback Procedures**

  Moved to section 4.4.2 Remote Access Server/Network Access Server.

- **Section 4.1.4 Workstation Modems**

  Removed this section.

- **Section 4.2 General Standards for Remote Access Methods**

  Reorganized to create the following new sections:

  4.2 Remote Access Agreement
  4.4.2 Remote Access Server/Network Access Server
  4.4.3 Dial-in Connectivity
  4.5 Remote Client to VPN Gateway.

- **Section 4.1 Levels of Remote Access**

  Created from the Secure Remote Computing STIG.

- **Section 4.2 Remote Access Agreement**

  Updated to include requirements from the SRC STIG.

  Remote User Responsibilities is now referencing the Secure Remote Computing STIG.

- **Section 4.3** Authentication, Authorization, and Accounting (AAA)

  Created from the Secure Remote Computing STIG.

- **Section 4.3 Remote Client to VPN Gateway**

. VPN requirements from the Secure Remote Computing STIG were added.

SECTION 5 – NETWORK MANAGEMENT AND SUPPORT SERVICES

- **Section 5.3 Domain Name System**

  Removed this section.

- **Section 5.1.2 Network Management Security Implications**

  Clarified the requirement to implement the SNMP Version 3 Security Model across the entire network infrastructure.

  Moved community string integrity requirements from section 3.6.1 to this section to cover the entire network infrastructure.

APPENDIX A – RELATED PUBLICATIONS

- Added ASD (NII) Memo, “Internet Protocol Version 6” (IPv6), June 9, 2003.

APPENDIX B – GLOSSARY OF TERMS

- Made changes and additions as appropriate.

APPENDIX C – CJCSM AND DISA COMPUTING SERVICES HANDBOOK REFERENCES

- Updated title to reflect Computing Services Handbook instead of Westhem Security Handbook.

APPENDIX D – DOD-CERT INFOARMTION ASSURANCE VULNERABLITY MANAGEMENT (IAVM)

- No changes.

APPENDIX E – REMOTE DIAGNOSTICS

- No changes.

APPENDIX F – JID GUIDANCE

- No changes.

APPENDIX G – REQUIRED FILTERING RULES

- Added clarification for those ports and services that are permitted conditionally IAW Appendix G.

APPENDIX H - DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT

- New Appendices

APPENDIX I – JUNIPER ROUTER SPECIFIC REQUIREMENTS

- New Appendices

APPENDIX J - NSA GUIDE TO E-MAIL SECURITY was added.

- New Appendices

This page is left intentionally blank.

1. INTRODUCTION

A core mission requirement for the Defense Information Systems Agency (DISA) Field Security Operations (FSO) is to secure DISA Networks. The processes and procedures outlined is this STIG when applied will decrease the vulnerability of security information as well as allay fears of system breach/sabotage. Network Security is clearly still one of the biggest concerns for our Department of Defense (DOD) customers (i.e. the warfighter).

Increasingly, the warfighter is relying on critical real time information, which must be provided with minimal delay. In addition to having the information provided, concerns center around the storage and transport process that assures the integrity of the information, and that the information be available only to authorized users. Since information the warfighter depends upon can be stored, processed, or transmitted from a number of locations, information systems management and Information Security (INFOSEC) must contend with the total environment

Technology can provide so much information that efficient management, sorting, manipulating, processing, storing, and transmission have become major elements in providing the proper information to users of the entire Global Information Grid (GIG). Relevant information can be so disbursed that reliance on a single information source may be inadequate. As the DOD systems and networks become more interrelated and sophisticated, ensuring the security of this information has become even more complex.

Security in this interactive operating environment must focus on the entire GIG and not simply on individual systems and networks. In addition to securing information while in transit across the GIG, a major effort must be placed on ensuring that networks attached to the GIG do not present a security problem to other users within the GIG. This concern is heightened by the fact that network vulnerabilities become magnified when external access is permitted. The GIG is only as secure as its weakest component and threats can be global as well as local. However, a secure backbone network is necessary to minimize the risks for the attached connections while ensuring the required interconnectivity.

The intent of this *Network Infrastructure Security Technical Implementation Guide (STIG)* is to include security considerations at the network level needed to provide an acceptable level of risk for information as it is transmitted throughout an enclave and potentially to other sites using the GIG. It also provides suggestions for redundancy, survivability, and some guidelines for best network technical practices.

1.1 Background

Department of Defense Directive (DODD) 8500.1 establishes policy and assigns responsibilities to the Defense Information Systems Agency (DISA) to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency. Paragraph 4.18 of the 8500.1 states, " All IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines." DISA Field Security Operations (FSO) develops the guidelines, which are called Security Technical Implementation Guides. It should be noted

that FSO Support and Technical Support for the STIGs, Checklist and Tools is only available to DOD Customers.

1.2 Purpose

Each site's network/communications infrastructure must provide secure, available, and reliable data for all customers, especially the warfighter. This document will assist the sites in meeting the minimum requirements; standards, controls, and options that must be in place for secure network operations. The Information Assurance Officer (IAO) and the Network Security Officer (NSO), in cooperation with customers, must weigh security with operational necessities. Each site may implement additional security measures as necessary to optimize the system's overall operation. Changes in security measures—although intended as improvements—may impact existing measures and possibly weaken overall security. Deviations from security measures contained within this document may be implemented only after obtaining approval from DISA FSO. Change requests are to be submitted in writing. They will be reviewed and returned with comments.

Note: If the guidelines contained in this document must be modified for the proper, secure operation of an operating environment, the IAO will first ensure the overall secure operation of the infrastructure, and then notify OP7 of the circumstance for the change and the proposed solution.

1.3 Scope

The requirements set forth in this document will assist Information Assurance Managers (IAMs), Information Assurance Officers, System Administrators (SAs), and end users in support of protecting DOD network infrastructures and resources in the following sites:

- Defense Enterprise Computing Centers (DECCs)
- Defense Enterprise Computing Center - Detachments (DECC-Ds)
- Global Network Operations and Security Centers (GNOSCs)
- Network Operations and Security Centers (NOSCs)
- Regional Network Operations and Security Centers (RNOSCs)
- Systems Support Offices (SSOs)
- DOD Components
- Combatant Commands
- DISA Continuity of Operations and Test Facility (DCTF)
- Other DISA customers

The requirements set forth in this document will be employed at the boundary between DISA private LANs and all WAN connections such as the Non-classified (but Sensitive) Internet Protocol Routing Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet) and the Internet. The document will also assist in identifying external security exposures created when the site is connected to at least one Information System (IS) outside the site's control.

1.4 Authority

The Security Technical Implementation Guides (STIGs) were initially developed to assist the sites in securing their systems against security and infrastructure vulnerabilities. All sites have a vested interest in maintaining system security, as it directly impacts the site's Certification and Accreditation (C&A). Sites are mandated by DISA to have a valid C&A status by the authority derived from *DOD Directive 8500.1, Information Assurance, October 24, 2002,* and the *Computer Security Act of 1987, Public Law 100-235, 8 January 1988.*

1.5 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 Information Assurance Officer (IAO) will adhere to the instruction as written. Only an extension issued by DISA Field Security Operations 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 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 PDI, or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the PDI (i.e., "[N/A: Cat III]").

1.6 DISA Information Assurance Vulnerability Management (IAVM) Program/Vulnerability Management System (VMS) Process

DISA developed and mandated the Vulnerability Compliance Tracking System (VCTS) to notify its commands, agencies, and organizations of new and potential security vulnerabilities. The VCTS meets the DOD mandate to ensure all System Administrators (SAs) receive and act upon Information Assurance Vulnerability Management (IAVM) Program notifications. It provides a mechanism for correction of new vulnerabilities within a specified time period. It also provides

the means, via the Security Readiness Review Database (SRRDB) for scheduling periodic validations of system status. VCTS and the SRRDB have been combined into the Vulnerability Management System (VMS). Users requiring access to VMS should contact the Defense Enterprise Computing Center-Detachment (DECC-D) Chambersburg Help Desk, at: DSN 570-5690, Commercial (717) 267-5690, or email weblog@chamb.disa.mil.

Each site will ensure that all DISA information systems and their SAs register with the VCTS. A DISA information system is a system that is physically located at a DISA site or managed by DISA personnel. The site will be responsible for registering all new systems and all new SAs with the VCTS. The IAO and IAM will be responsible for ensuring response to and/or implementation of the IAVM notice. The Field Security Operations SRRDB tracks the site implementation status of all IAVM alerts, bulletins, and technical advisories. The SRRDB can provide SRR review teams with a list of system specific IAVM notices as well as the applicable fixes and patches. The SRR Team will check each system to ensure IAVM compliance. This document includes detailed information on all IAVM notices issued that apply to this technology. Where appropriate, these IAVM notices are referenced or included in summary format in this document.

- *All DISA information systems will be registered with the VCTS.*
- *System Administrators (SAs) responsible for information systems will be registered with the VCTS.*
- *The IAO and IAM, in coordination with the SA, will be responsible for ensuring response to all IAVM notices within the specified time period.*

1.7 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 have 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.

1.8 Extensions

One of the major changes, with the recent migration of the SRRDB into VMS, is the discontinuation of the previous SRR waiver and exemption process. Instead, sites must submit an on-line request for extension for any SRR finding that cannot be fixed and closed within the

designated timeframe. The same process is used by VCTS. The VMS SRRDB extension process for reviews and approvals will be similar as well.

Deviations from the standards will be allowed as long as:

MAC II controls are not jeopardized.
A true business case justifies each deviation.
The security of the site is not adversely affected.

After a SRR, a report of findings will be presented to the organization. If findings cannot be resolved in a timely manner, an extension may be requested. Justification may include operational reasons, technical conflicts, and insufficient funding. An extension request will identify a plan and timetable for resolving the finding(s). Any supplemental security countermeasures should also be addressed.

1.9 STIG Distribution

Compliance with the applicable STIG is mandatory for systems residing in a DISA facility and for any system directly administered by DISA. 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 MAC II Sensitive level, containing unclassified but sensitive information. In the interest of promoting enhanced security for systems both inside DOD and within the Federal Government's computing environments, DISA encourages any interested DOD activity or party to obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. The DISA FSO URL is http://guides.ritchie.disa.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov address.** The STIGs are available to users that do not originate from a .mil or .gov by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

1.10 Document Revisions

Revisions to this document should be sent via e-mail to **stig_comments@ritchie.disa.mil**. DISA FSO will coordinate all change requests with the relevant DISA Field Security Operations organizations, and other DISA organizations as appropriate, before inclusion in this document.

1.11 Organizational Relationships

Organizational relationships play a significant role in providing infrastructure network security. The site organization must provide a robust and secure environment that protects the software and hardware from unauthorized access. This includes the protection of system-level resources (i.e., applications, database systems, and other utilities used by the DOD user community and/or customers). The sites, in consideration of customer requests for systems administration or operation, must provide a reasonably secure environment for these customers. Owners of the data must define access requirements for their resources (i.e., actual databases, master files, and interactive transactions). It is the responsibility of the data owners to provide an access matrix that reflects subjects (like processes and authorized personnel) and their permission to access resources (like databases and applications). Service Level Agreements (SLAs) must address security and define responsibilities of the sites and the customer.

1.12 Physical/Personnel Security

Although this document does not address physical or personnel security directly, these areas must be given proper consideration and attention. As an example in the case of network operations, it is widely documented how to gain privileged level access to Cisco routers with simply having physical access to the equipment and a laptop or other terminal devices. Proper attention to personnel security is necessary to ensure that only personnel with the proper credentials have access to the network configuration.

- *The site's security officer will ensure that the physical/personnel security requirements are adhered to, as contained in the DISA Computing Services Security Handbook, Section 3.1.5 (see Appendix D) and DOD 5200.1-R Information Security Program & 5200.2-R Personnel Security Program.*

- *The site's security officer will ensure that the DISA Form 41 or similar access authorization form will be used to validate a user's requirement to have a management account on any network device.*

1.13 Related Documentation

This document is one publication in a series of Security Technical Implementation Guides (STIGs) published by DISA Field Security Operations. These documents provide its users with a total INFOSEC protection scheme for their entire architecture. *Appendix A, Related Publications,* lists Government and commercial publications with subject matter related to this document.

1.14 Computer Network Defense (CND) Directive

DOD Directive Number O-8530.1, Computer Network Defense, issued January 8, 2001, specifies that all agencies, commands, activities, and all other organizational entities within the DOD will

follow the rules, guidelines, and instructions as detailed in this directive. Some of the main points within the directive include steps for securing DOD operations, information systems, and computer networks by:

- Monitoring for intrusions, disruption of services, or other incidents that threaten these components

- Organizing, planning, training for, and conducting defense of DOD computer networks using a CND Common Operational Picture (COP), a sensor grid and a capabilities accreditation and certification process

- Providing for robust infrastructure and informational assurance practices through the following:

  - Configuration management, certification and accreditation in accordance with DOD Instruction 5200.40
  - Regular and proactive vulnerability analysis and assessment
  - Adherence to a defense-in-depth strategy
  - Information assurance training, awareness, and certification for all information system and computer network providers, managers, administrators, support personnel and users
  - Dissemination and compliance process for information assurance advisories and alerts
  - The directive also assigns roles and responsibilities for accomplishing the requirements of the CND

- *The NSO will ensure that the Network is in compliance with DOD CND Directive O-8530.1.*

1.15 Security Vigilance

Network Security is dynamic in nature and requires in-depth knowledge and dedication to maintain the overall security of the network infrastructure. Routinely new Security Vulnerabilities are discovered; this makes formerly secure networking environments insecure and open to new attacks. Regardless of what security testing has been performed and what countermeasures have been put in place, keeping pace with updating system patches and resolving vulnerabilities is essential to the overall security of the network infrastructure.

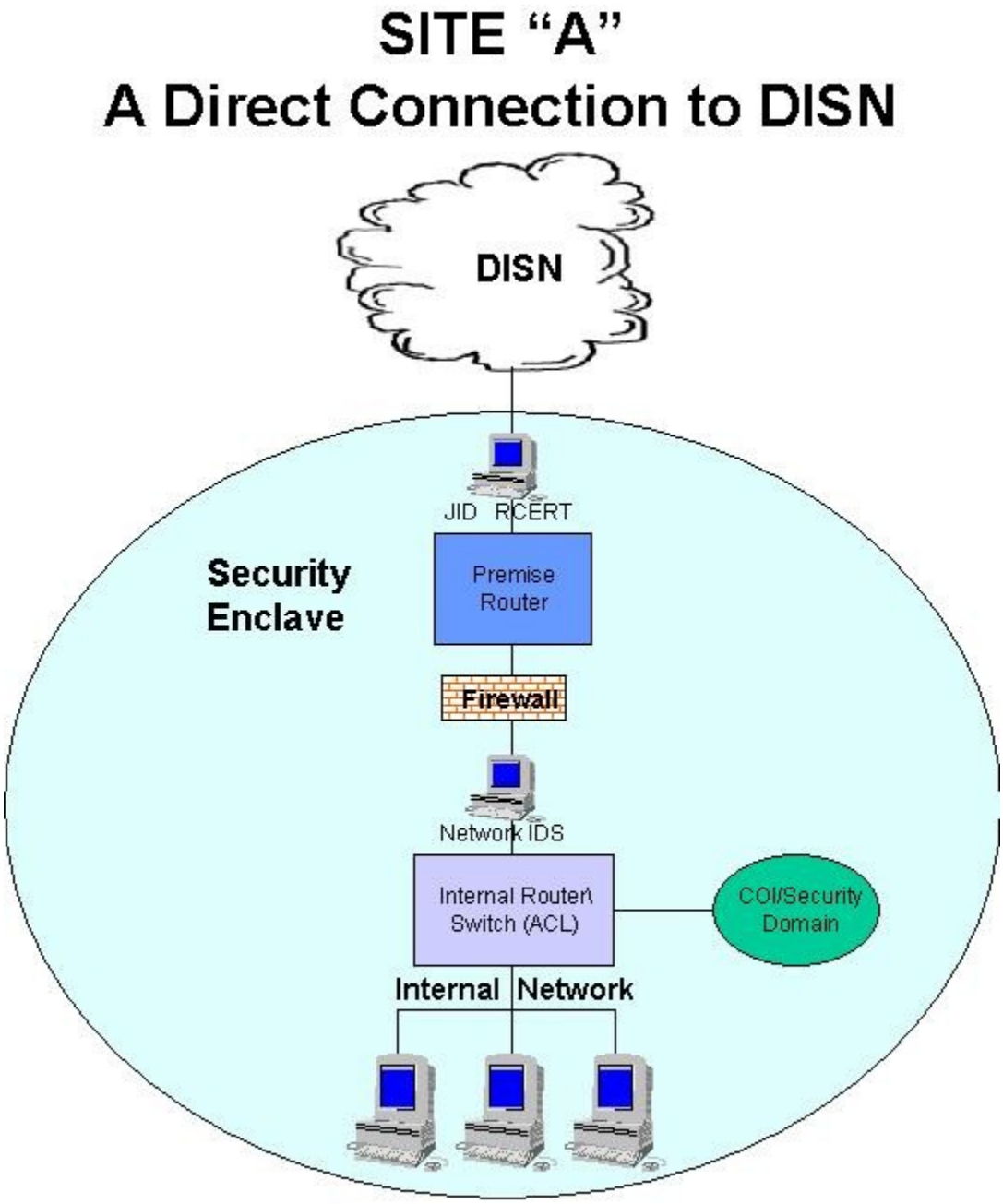
Consequently, conducting periodic vulnerability scans as well as manual self-assessments will enable sites to find and close vulnerabilities prior to exploitation. These scans need to be conducted on a regular basis, such as quarterly, or even monthly for sensitive networks, and when major network changes (examples) are implemented.

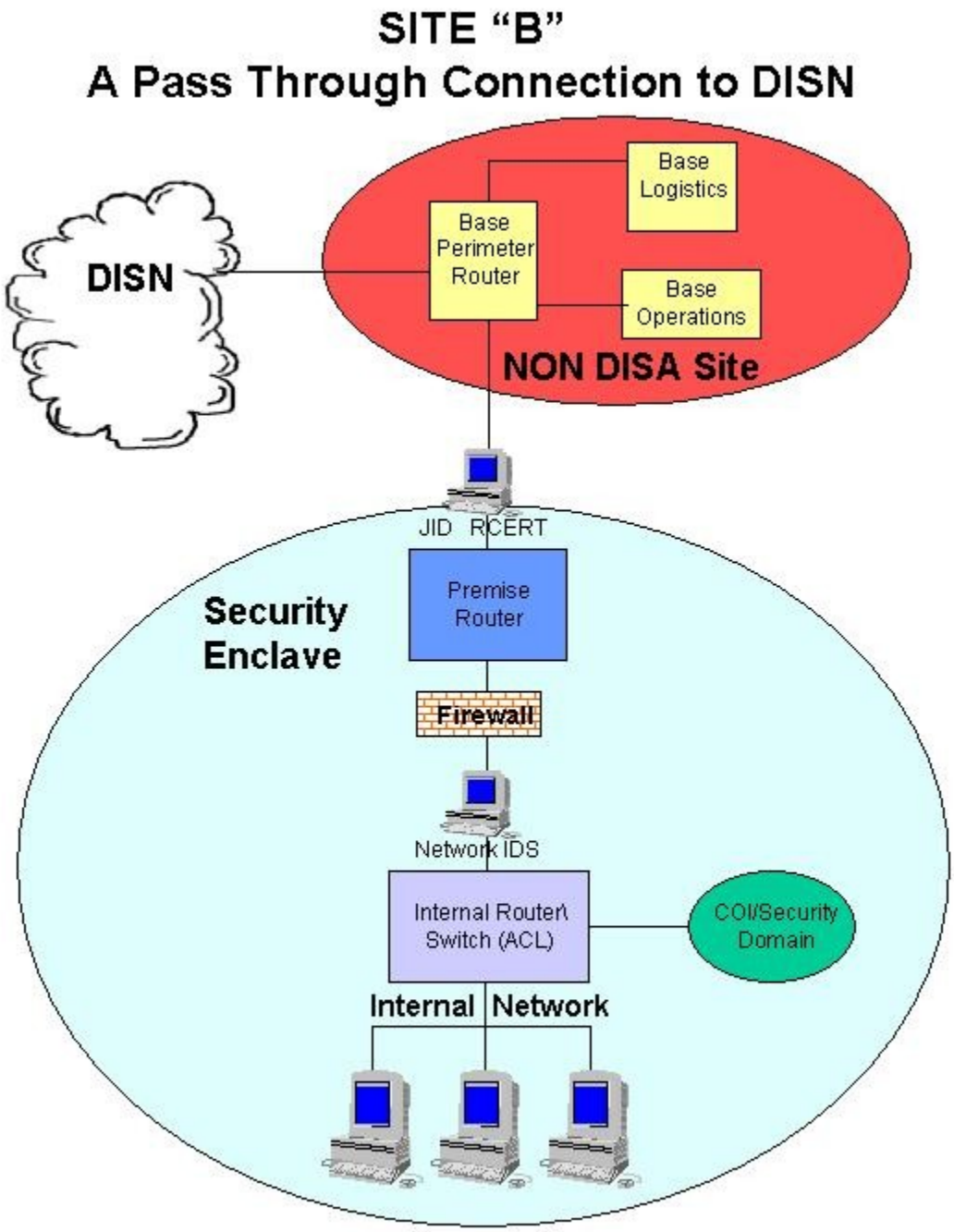
- (NET0020: CAT II*) The IAO will ensure that prior to deploying any network device into the network infrastructure, the system will be configured to meet the appropriate STIG requirements and have a vulnerability scan performed on it.*

This page is intentionally left blank.

2. ENCLAVE ARCHITECTURE OVERVIEW

Enclave Perimeter Security mechanisms are employed at the boundary between a DISA private LAN and a WAN (e.g., Internet, NIPRNet, SIPRNet). These connections are discussed in this document as **LAN to WAN** connections.




SITE "B"
A Pass Through Connection to DISN
DISN
Base Logistics
Base Perimeter Router
Base Operations
NON DISA Site
JID RCERT
Security Enclave
Premise Router
Firewall
Network IDS
Internal Router\ Switch (ACL)
COI/Security Domain
Internal Network

2.1 Enclave Protection Mechanisms

Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A large complex site, such as a DECC, or a DECC-D, may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers. For example, Defense Finance and Accounting Service (DFAS) and Defense Logistics Agency (DLA) may have functionally driven security domains. There might also be technology-driven security domains for OS/390, Unisys, Tandem, etc. Smaller locations may have a single enclave with a single security domain supporting the entire organization. The enclave or system owner will identify security domain requirements in the System Security Authorization Agreement (SSAA).

Procedures outlined in the *DOD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97*, lay out the process for the Enclave Security Architecture as they are applied to specific requirements. Each SSAA will include a description of the architectural implementation of the security requirements identified in this STIG.

STIGs and SRRs provide the specifications, standards, and inspections for each of the key enclave components. In order to comply with the Enclave Architecture the minimum requirements include the following devices or systems:

- External Network Intrusion Detection System
- Router with ACLs
- Application-level Firewall
- Internal Network Intrusion Detection System
- Demilitarized Zone (DMZ)
- Split-DNS

The only approved variance to the Enclave Architecture would be a site that adheres to the Deny by Default rule, does not require access into the Enclave to any user services, or host publicly accessible data (e.g., web servers, ftp servers, etc.). Therefore, the requirement for a DMZ and Split-DNS would not apply to these sites. This does not negate the need for DNS services; therefore, if the site utilizes an internal DNS server it must be configured In Accordance With (IAW) the Domain Name System (DNS) STIG, otherwise the use of host files to handle the internal resolution may be an acceptable solution. Either solution would require the utilization of a primary or secondary DNS server, hosted on the NIPRNet, for all external resolution.

This page is intentionally left blank.

3. NETWORK INFRASTRUCTURE

To assist in the management, auditing, and security of the network infrastructure facility drawings and topology maps are a necessity. Topology maps are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks (wire taps) could take place.

- (NET0090: CAT II) *The NSO will maintain a current drawing of the site's network topology that includes all external and internal links, subnets, and all network equipment.*

3.1 External Network Intrusion Detection System

Network intrusion detection systems (NIDS) provide an additional level of control and visibility into the network infrastructure. Implementing a NIDS on the network's exterior can expose unauthorized or malicious traffic that will most likely be blocked by the premise router and firewall as well as traffic from hackers who may be able to thwart the enclave perimeter protection mechanisms. Network intrusion detection systems can also be used to block suspect attacks that are easily recognized. Perhaps the greatest value that network intrusion detection systems provide is the information about the use and usage of the network. This information provides decision support data to the RCERT or CND Service Provider, can increase the value and efficiency of existing enclave protection mechanisms, and can produce hard evidence and justification for altering the enterprise's security policy.

As depicted in Section 2 ENCLAVE ARCHITECTURE OVERVIEW, an external NIDS must be installed and implemented in front of the premise or border router and must be monitored by the RCERT or a certified CND Service Provider. Placing the external NIDS on the exterior—that is, between the premise router and the node router—will enable the RCERT or CND Service Provider to detect attempted attacks that may otherwise be blocked by the premise router or firewall. A signature-based, anomaly-based, or rules-based NIDS that has been customized to specific NIPRNet or SIPRNet traffic can alert the RCERT or CND Service Provider of suspected threats at the enclave's gateway. The external NIDS can be a JID or any other DISA approved intrusion detection system.

The JID is a suite of software tools that supports the detection, analysis, and gathering of evidence of intrusive behavior occurring on Ethernet or Fiber Distributed Data Interface (FDDI) based networks using IP. In support of these services, JID provides four common operating models:

- Retrospective intrusion analysis
- Near Real-time intrusion detection
- Evidence gathering
- Statistics gathering

The following are guidelines that are applicable to the RCERT or the certified CND Service Provider:

- Will ensure that all external NIDS systems have DOD General Counsel and Department of Justice (DOJ) approved logon-warning banners displayed during each logon process.

- Will ensure that a network monitor will only be used to monitor activity on a system-wide level without the targeting of any specific person(s) until any suspected unauthorized activity has been identified. Once an individual has been identified as possibly being the party responsible for the suspicious activity, the appropriate Law Enforcement Agency (LEA) will be notified and will issue authorization to legally continue monitoring of the individual.

- Will notify the Department of Defense Computer Emergency Response Team (DOD-CERT) about any identified suspicious activity.

- Will ensure that data collected as evidence to support an LEA investigation will be coordinated with the LEA performing the investigation to ensure that it conforms to accepted standards for evidence.

- Will ensure that the media used to store any intended evidence will be handled in accordance with LEA policy and regulations for evidence handling.

- Will ensure that the monitoring system will be configured such that it does not allow incoming network connections from any other system, except from Secure Shell (SSH) for specifically authorized Internetworking Operating System (IP) addresses (i.e., passively monitor the network without accepting Telnet, FTP, e-mail, etc., connections from other systems).

- Will ensure that NIDS operating system and application access will be restricted to specifically authorized personnel.

- NET0100: CAT I) *The NSO will ensure that an external NIDS has been installed and implemented so that all external connections can be monitored.*

- (NET0100: CAT I) *The NSO will ensure that the data from the external NIDS is continuously being monitored by the RCERT or a certified CND Service Provider.*

CAVEAT: If a site does not have a direct link to a NIPRNet or SIPRNet node router—that is, its connection to the NIPRNet or SIPRNet is through an upstream link to another activity's premise router, then this site would not be required to have its own external NIDS if the upstream activity has an external NIDS that is being monitored by the RCERT or a certified CND Service Provider. However, if this site has other external connections such as an Internet Service Provider, this traffic would need to be monitored by a CND Service Provider using an external NIDS.

- (NET0110: CAT III) *The NSO will ensure that the external NIDS is located between the site's NIPRNet or SIPRNet Point of Presence (POP) and the their premise router.*

- (NET0120: CAT III) *The NSO will ensure that the data from the external NIDS is being monitored exclusively by the RCERT or a certified CND Service Provider.*

3.2 External Connections

Connecting to external networks is one of the most complex areas of designing, implementing, and managing a network. An external network can be the NIPRNet or SIPRNet, as well as a network belonging to another DoD activity, a contractor, or even the Internet. An external network is connected to the site's internal network via an external connection that can include but not limited to a dedicated circuit (i.e., DISN Data Services), dial-on-demand Integrated Services Digital Network (ISDN), an Internet Service Provider (ISP) connection, or an Ethernet upstream link to a neighboring service or activity's network on the same base.

Regardless of technology used, each external connection to the site's internal network must be secured such that it does not introduce any risk to the network. Every site should have a security policy addressing filtering of the traffic from those connections. This documentation along with diagrams of the network topology are required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet. Depending on the command, service, or activity, additional approval may be required. SIPRNet connections must also comply with the documentation provided to the SIPRNet Connection Approval Office (SCAO) to receive the SIPRNet Interim Approval to Connect (IATC) or final Approval to Connect (ATC) or as documented in the Interim Approval to Operate (IATO) or Approval to Operate (ATO) signed by the DAA.

Prior to establishing a connection with another activity, the site's policy should require that a Memorandum of Understanding (MOU) or Memorandums of Agreement (MOA) be established between the two sites prior to connecting with each other. This documentation along with diagrams of the network topology is required to be submitted to the CAP for approval to connect to the NIPRNet or SIPRNet. The policy must insure that all connections to external networks should conform equally. A connection to a trusted DoD activity must be treated the same as a connection to the NIPRNet. The security posture of a network is only as good as its weakest link.

- (NET0130: CAT III) *The NSO will ensure that all external connections will be validated and approved prior to connection.*

- (NET0135: CAT II) *The NSO will review all connection requirements on a regular basis to ensure the need remains current, as well as investigate all undocumented network connections discovered during inspections. Unjustified and unapproved connections will be disconnected.*

3.2.1 Leased/Dedicated Lines

DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore unauthorized access must be restricted. Security guidelines concerning leased/dedicated circuits are as follows:

- (NET0140: CAT III) *The NSO will ensure the connection between the CSU/DSU and the local exchange carrier's (LEC) data service jack (i.e., demarc) is in a secured environment.*

- (NET0140: CAT III) *The NSO will ensure the network management modems connected to all Channel Service Units (CSUs)/Data Service Units (DSUs) will be disabled or disconnected when not in use.*

- (NET0150: CAT III) *The IAO will ensure that if NIPRNet access redundancy is required, it is acquired through Defense Information System Network (DISN) Data Services.*

3.2.2 ISP Connections

Direct ISP connections are prohibited unless written approval is obtained from the GIG Waiver Panel or the Assistant Secretary of Defense for Networks & Information Integration (NII) who acts as the DoD CIO as well as the chair for the GIG Panel.

- (NET0160: CAT I) *The IAM will ensure that written approval is obtained from the GIG Waiver Panel or the Assistant Secretary of Defense (NII) prior to establishing a direct ISP connection.*

3.2.3 Backdoor Connections

The term "backdoor link" is used to refer to a link between two customer sites that does not traverse the provider's network (RFC 2764) –in this case, the provider network would be NIPRNet or SIPRNet. Routes over this link are called "backdoor routes". Without taking the proper safeguard steps, this connection could impose security risks to either site. For example, as a result of link availability or routing protocol administrative distances (i.e. the backdoor route is more favorable), it is possible that traffic destined for other networks from site B's network and vise versa could just be passing through Site A's premise router. It is also possible that traffic from Site B's network could be destined for Site A's network. In either case, the premise router external interface providing the backdoor link must have the same ingress filtering applied as an external interface providing a connection to the NIPRNet, SIPRNet, or ISP.

An even greater risk would be a backdoor link established between two sites' internal routers or layer-3 switches. In this case, the traffic between the two sites is bypassing the perimeter that has been established for each network for defense against an attack. Though both networks consider each other a trusted network, the risk becomes evident when one of the networks has been breached leaving the other in a vulnerable position. Backdoor connections bypassing the networks perimeter (i.e., screening router, firewall, IDS, etc) are prohibited unless the connection is mission critical and approved by the DAA or CIO. This unprotected connection could also be to the Internet, NIPRNet, SIPRNet, or any other DoD or contractor network.

- (NET0170: CAT II) *The NSO will ensure that no backdoor connections exist between the site's secured private network and the Internet, NIPRNet, SIPRNet, or other external networks unless approved by the DAA or CIO.*

3.3 Network Layer Addressing

IPv6 is the next generation network layer protocol for the Internet as well as the Global Information Grid (GIG) including the NIPRNet and SIPRNet. Implementation of IPv6 is necessary due to the fundamental constraints of IPv4 that renders it incapable of meeting long-term requirements of both the commercial community and the DoD. As part of the GIG integrated architecture strategy, the migration to IPv6 across DoD networks will consider operational requirements, risks, and costs, while maintaining interoperability within the DoD, across the Federal Government, and among business partners in the commercial sector. Henceforth, as of the memo from the ASD (NII) dated June 9, 2003, IPv4 will continue to be the mandated internetworking protocol for DoD. In addition, all references in this document relating to addressing, address blocks, subnets, prefixing, multicasting, and broadcasting will be exclusively within the IPv4 framework.

The first part of an IP address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy—subnetting supports a three-level hierarchy. The network-number field has been referred to as the "network-prefix" because the leading portion of each IP address identifies the network number. All hosts on a given network share the same network-prefix but must have a unique host-number.

Blocks of network addressees are assigned by the DOD Network Information Center (NIC), to local administrators. Individual IP addresses are then assigned by the local network administrator to hosts, servers, printers and workstations on their LAN.

- (NET0175: CAT I) *The NSO will ensure that IPv6 has not been implemented on any DoD network that transports production or operations traffic.*

- (NET0180: CAT II) *The NSO will ensure all network IP address ranges are properly registered with the **.MIL** Network Information Center (NIC).*

3.3.1 IANA Reserved Addresses

In the past, it has been typical to assign globally unique addresses to all hosts that use IP. In order to extend the life of the IPv4 address space, address registries are requiring more justification than ever before, making it harder for organizations to acquire additional address space blocks. It is the intent of RFC 1918 to promote a strategy that will provide constraint relief to the available globally unique address space that is rapidly diminishing. As documented in RFC 1918 The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space that can be used for private networks:

10.0.0.0	- 10.255.255.255 (10/8 prefix)	Class A
172.16.0.0	- 172.31.255.255 (172.16/12 prefix)	Class B
192.168.0.0	- 192.168.255.255 (192.168/16 prefix)	Class C

Sites will incorporate the use of private network addresses into the site's NIPRNet architecture using the address spaces defined in this section. Implementation of RFC 1918 addresses are not required for the site's DMZ, service network, or any out-of-band management network. A site that uses any of these private addresses can do so without any coordination with IANA or the NIC. Since these addresses are never injected into the global NIPRNet, SIPRNet, or Internet routing system, the address space can simultaneously be used by every organization.

All sites need to be aware that IANA has also reserved the following blocks of IP address space, and the appropriate ACLs need to be applied to filter this traffic.

224.0.0.0	15.255.255.255 (/4 prefix)	Class D Multicast
240.0.0.0	7.255.255.255 (/5 prefix)	Class E
248.0.0.0	7.255.255.255 (/5 prefix)	Unallocated
0.0.0.0	0.255.255.255	Historical Broadcast
255.255.255.255	255.255.255.255	Broadcast
192.0.2.0	0.0.0.255 (/24 prefix)	Test Net
169.254.0.0	0.0.255.255	Link Local
192.0.127.0	0.0.0.255	IANA NS Lab 1
192.0.0.0	0.255.255.255	IANA NS Lab 2
0.0.0.0	1.255.255.255	Unallocated / IANA Reserved
2.0.0.0	0.255.255.255	Unallocated / IANA Reserved
5.0.0.0	0.255.255.255	Unallocated / IANA Reserved
7.0.0.0	0.255.255.255	Unallocated / IANA Reserved
23.0.0.0	0.255.255.255	Unallocated / IANA Reserved
27.0.0.0	0.255.255.255	Unallocated / IANA Reserved
31.0.0.0	0.255.255.255	Unallocated / IANA Reserved
36.0.0.0	1.255.255.255	Unallocated / IANA Reserved
39.0.0.0	0.255.255.255	Unallocated / IANA Reserved
41.0.0.0	0.255.255.255	Unallocated / IANA Reserved
42.0.0.0	0.255.255.255	Unallocated / IANA Reserved
49.0.0.0	0.255.255.255	Unallocated / IANA Reserved
50.0.0.0	0.255.255.255	Unallocated / IANA Reserved
58.0.0.0	0.255.255.255	Unallocated / IANA Reserved
59.0.0.0	0.255.255.255	Unallocated / IANA Reserved
60.0.0.0	0.255.255.255	Unallocated / IANA Reserved
70.0.0.0	1.255.255.255	Unallocated / IANA Reserved
72.0.0.0	7.255.255.255	Unallocated / IANA Reserved
82.0.0.0	1.255.255.255	Unallocated / IANA Reserved
84.0.0.0	3.255.255.255	Unallocated / IANA Reserved
88.0.0.0	7.255.255.255	Unallocated / IANA Reserved
96.0.0.0	31.255.255.255	Unallocated / IANA Reserved

197.0.0.0	0.255.255.255	Unallocated / IANA Reserved
198.18.0.0	0.1.255.255	Unallocated / IANA Reserved
201.0.0.0	0.255.255.255	Unallocated / IANA Reserved
222.0.0.0	1.255.255.255	Unallocated / IANA Reserved
223.0.0.0	0.255.255.255	Unallocated / IANA Reserved

- (NET0182: CAT III) *The NSO will ensure the site incorporates private network addresses into the site's NIPRNet infrastructure using address spaces defined in RFC 1918.*

  Note: RFC 1918 addresses are not required for the DMZ, service network or out-of-band management network.

- (NET0185: CAT II) *The NSO will ensure that all addresses used within the site's SIPRNet infrastructure are authorized .mil addresses that have been registered and assigned to the activity.*

3.3.2 Network Address Translation

Using the private addressing scheme in accordance with RFC 1918 will require an organization to also use Network Address Translation (NAT) for global access. Though NAT works well with the implementation of RFC 1918 addressing scheme, it also has the security benefit of hiding real internal addresses. A sites network address infrastructure should be considered proprietary information and should not be advertised. If potential attackers were able to map the network infrastructure by discovering real client addresses, they would be able to identify resources on the network to attack. The external IP address of the firewall or routable addresses from a NAT pool should be the only address visible to the public.

- (NET0190: CAT III) *The NSO will ensure that a workstation clients' real addresses are not revealed to the public by implementing NAT on the firewall or the router.*

CAVEAT: If the site has implemented an application-level firewall, hiding of the clients' real address can also be done by enabling the proxies to replace the clients' real source address with that of the firewall's external IP address or an address from a NAT pool.

Note: When configuring NAT for the network, almost all installations fall into one of the following scenarios:

The first scenario would be a site that has configured the firewall with one external IP address and has configured the internal network to use RFC 1918 addresses. It may work for a site that does not allow for external connections into the network, but is the least deployed configuration.

The second scenario would be a site that has multiple external IP addresses configured on the firewall, one primary for the site (workstations, printers, etc.), and the others redirected to individual servers. This is common with sites that host Web and FTP sites. The internal network is configured with the RFC 1918 addresses, including the Web or FTP server, but the server's IP address is mapped one to one with a different external IP.

The last scenario would be a system that requires that its real address be used. For these instances, the site will implement RFC 1918 addresses for the entire network with the exception of those hosts. The site will provide written justification for the exclusion of these hosts from the requirement.

In all of the situations above, the intent is to restrict the source and destination range to the smallest range possible. For servers that are open to the public, or an unmanageable subset of the public range (e.g., .mil, .gov, and .com), the site is configured similar to the second scenario, except the source address for these connections would be "any". If the .com users were only a few users, then you could restrict to .mil and .gov and then configure the small amount of .com addresses. The destination IP should be restricted to a single IP or in the case of a cluster or server "farm" it could be restricted to a subnet, yet would still implement port restriction.

3.3.3 DHCP

With an increase in TCP/IP networks, the ability to assign IP client configurations automatically for a specific time period (called a lease period) has alleviated the time consuming process of IP address management. Network administrators can now automate and control from a central position the assignment of IP address configurations using the Dynamic Host Control Protocol (DHCP).

When connected to a network, every computer must be assigned a unique address. However, when adding a machine to a network, the assignment and configuration of network IP addresses has required administrator action. The user had to request an IP address, and then the administrator would manually configure the machine. Mistakes in the configuration process are easy to make, and can cause difficulties for both the administrator making the error, as well as users on the network. In order to simplify the process of adding machines to the network and assigning unique IP addresses manually, the site may decide to deploy DHCP.

If DHCP is used to allocate IP addresses for internal devices, a portion of the network IP addresses needs to be excluded or reserved from the DHCP scope for devices that require manual configuration of IP addresses (e.g., servers, routers, firewalls, and administrator workstations, etc.). The DHCP server is required, at a minimum, to log hostnames or MAC addresses for all clients. In order to trace, audit, and investigate suspicious activity, DHCP servers within the SIPRNet infrastructure must have the minimum duration of the lease time configured to 30 or more days.

Assigning static IP addresses to all routers, firewalls, servers, administrator workstations, printers, and all other communication devices allows for placing ACLs on the router and firewall that protects these devices. These devices because of their role in the infrastructure generally require static IP addresses and with the exception of printers are prime targets for hackers. The printers because of added functionality (i.e. web management, SNMP, etc.) and limited built in security mechanisms pose a unique security risk.

- (NET0195: CAT II) *The NSO will ensure that all routers, firewalls, servers, administrator workstations, printers, and all other communications devices are assigned static IP addresses to the fullest extent possible.*

- (NET0198: CAT III) *The NSO will ensure that the DHCP server is configured to log hostnames or MAC addresses for all clients.*

- (NET0198: CAT III) *The NSO will ensure that any DHCP server used within SIPRNet infrastructure is configured with a minimum duration time for the lease of 30 or more days.*

3.4 General Standards for Communications Devices

The following subsections set security guidance applicable to all communications devices (e.g., routers, switches, firewalls, RAS, NAS, JIDS, IDS, etc.). This guidance will be adhered to in addition to the requirements set forth in the individual sections that provide detailed security requirements for each device.

NOTE: For the purpose of this document the term "remote" applies to anything other than direct console access, unless stated otherwise in the following section.

- (NET0200: CAT II) *In order to identify and combat MAC address spoofing, the NSO will maintain a listing of valid MAC addresses and conduct audits and reviews to identify new addresses.*

  - (NET0210: CAT II) *The NSO will ensure that all network devices (i.e., JIDS, IDS, routers, RAS, NAS, firewalls, etc) will be located in a secure room with limited access. The NSO will have ultimate authority to determine who has access both physically and administratively.*

3.4.1 Passwords

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

- (NET0240: CAT I) *The NSO will ensure all default manufacturer passwords are changed and backdoor accounts removed.*

  - (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 rules outlined in Appendix C, Chairman Joint Chiefs of Staff Manual (CJCSM) and DISA Computing Services Security Handbook References.*

- (NET0270: CAT II) *The IAO will record the passwords used on communications devices and store them in a secured manner.*

3.4.2 Device Management

- (NET0280: CAT III) *The NSO will ensure that image files loaded via the File Transfer Protocol (FTP) process are checked on a monthly basis to ensure the file has not been corrupted or altered.*

- (NET0290: CAT II) *Some communications devices require the use of a downloadable configuration image file for supplying operating parameters and setup configuration. This file can be loaded from a console or via the FTP process. The NSO will ensure that communications between devices and the FTP server are secured. At a minimum, this will be accomplished by restricting communication to known authorized IP addresses.*

- (NET0300: CAT II) *The NSO will disable all network management ports except those needed to support the operational commitments of the sites.*

3.4.2.1 Out-of-band Management

Out-of-band management consists of accessing the communications device via a dial-up circuit or a directly connected terminal device. With the dial-up method, a modem is attached to the console service port and the administrator connects via a standard phone line. This connection is relatively private, since connect times are random and the circuit is disconnected when not in use. The most secure **out-of-band** management is directly connecting a computer or terminal to the service port. This precludes any intentional or accidental reception of information.

A secure **out-of-band** alternative to direct connection can be accomplished by dial-in access to a TACACS+ server via an encryption utility (i.e., SSH). This alternative provides a secure and encrypted connection to an **out-of-band** or closed network.

- (NET0310: CAT II) *The NSO will ensure that the out-of-band or direct connection method for communications device management is used. If direct connection is impractical, the dial-up method is the next best choice, with the secure dial-up into the TACACS+ server inside the secure enclave via an encryption utility (i.e., SSH) being preferred.*

- (NET0310: CAT II*) To ensure the proper authorized network administrator is the only one who can access the device, the NSO will ensure out-of-band access enforces the following four security restrictions:*

  - *Authenticated access control*
  - *Strong two-factor authentication (e.g., Secure ID)*
  - *Encryption of management session*
  - *Auditing*

3.4.2.2 In-band Management

In-band management is accomplished by establishing a SSH session with the device. This method is fast and convenient, but presents some security risks. Accessing the communications device **in-band** makes the session susceptible to all the monitoring and line sniffing vulnerabilities associated with a distributed LAN. For example, the login or privileged password could be intercepted, providing an attacker the capability to exploit a network device.

In-band management is only to be used in situations where out-of-band management will hinder operational commitments, and the IAO has approved in writing the use for that specific purpose. If remote access is used to connect to a network component for administrative access, the most stringent security controls will be implemented as specified in Section 4.1 Levels of Remote Access.

- (NET0320: CAT II) *The network administrator will limit the use of in-band management to situations where the use of out-of-band management would hinder operational commitments or when emergency situations arise. IAO will approve the use of in-band management on a case-by-case documented basis.*

- (NET0320: CAT II) *For in-band management, the NSO will insure that the currently supported version of SSH with all security-related patches applied is utilized.*

- (NET0320: CAT II) *The NSO will ensure that the use of in-band management will be restricted to a limited number (less than ten) of authorized IP addresses.*

- (NET0320: CAT II) *For in-band management, the NSO will implement the use of strong two-factor authentication for all access to all communications devices.*

- (NET0320: CAT II) *The NSO will ensure that all remote administrative access to a network device is secured using one of the following forms of encryption: VPN, SSL, SWA with SSL, IPSec, or SSH.*

3.4.2.3 Port Management

The interface connecting the physical medium to the communications device is predominately via a RJ-45 port. These ports allow electrical signals from the LAN-attached device to communicate with other LAN-attached devices. Port management is essential for adequate LAN security. If inactive ports are left connected, intentional or accidental insertion of an unauthorized device (such as a sniffer or laptop computer) may be accomplished. The two types of port protection are port intrusion and eavesdrop prevention.

Port intrusion protection is the more fundamental of the two procedures. It allows only addresses listed on an approved list of media access control (MAC) addresses to access the network.

Eavesdrop prevention scrambles data so that only authorized users (with corresponding IP addresses or a MAC address) are allowed access to it. Both of these port protection options are cost effective and available from most vendors.

- (NET0330: CAT III) *The NSO will ensure that if port management and port protection services are available on communications devices, they will be activated to the fullest extent possible.*

3.4.3 Warning Banners

- (NET0340: CAT II) *The NSO will ensure that 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 Appendix C, CJCSM and DISA Computing Services Security Handbook References. The NSO will document all devices that do not support warning banners.*

3.5 Routers

Routers process information at the third layer of the OSI model, the Network Layer. They provide a seamless path for the forwarding of data from a node on one network to a node on another network. The networks may be collocated or separated by thousands of miles and when combined they create the openness upon which information sharing is based.

Note: Supplemental guidance specific for Juniper Routers is contained in Appendix I

3.5.1 Route Tables

A router's primary responsibility is to send a packet of data to the intended destination. To accomplish this, each router needs a route table. Each router builds its table based on information from the network and from the router administrators. The router then uses a set of metrics, depending on the contents of the table and its routing algorithm, to compare routes and to determine the best path to a destination.

Routers use four primary mechanisms for building their route tables:

1. **Direct connection.** Any LAN segment to which the router is directly connected is automatically added to the route table.

2. **Static routing.** A router administrator can manually instruct a router to use a given route to a particular destination. This method takes precedence over any other method of routing.

3. **Dynamic routing.** Uses router update messages from other routers to create routes. The routing algorithm associated with the particular routing protocol determines the optimal path to a particular destination, and updates the route table. This method is the most flexible because it can automatically adapt to changes in the network.

4. **Default routing.** Uses a manually entered route to a specific *gateway of last resort* when route is not known by any other routing mechanism. This method is most useful for routers that serve as the sole connection between a small LAN and a large network like the Internet. Routers that depend on a single default gateway usually do not use routing protocols.

TABLE 1. BGP, EIGRP, IS-IS, RIP, AND OSPF

BGP	**Border Gateway Protocol:** A distance vector protocol. Maintains a list of the distance from itself to every known destination in a distance vector table. Based on Classless Inter-Domain Routing (CIDR), BGP supports aggregation and reduction of routing information.
EIGRP	**Enhanced Interior Gateway Routing Protocol:** An advanced distance vector routing protocol. Can route IP, IPX, and Appletalk. Is one of the few multi-protocol routing protocols. The Diffusing Update Algorithm (DUAL) is the heart of EIGRP. DUAL keeps a backup route in mind, in case the primary route goes down. DUAL also limits how many routers are affected when a change occurs to the network. EIGRP updates the routing tables only when there is a specific need to do so, as opposed to pure distance-vector protocols.
IS-IS	**Intermediate System to Intermediate System:** The IS-IS routing protocol is a link state protocol, as opposed to distance vector protocols such as Interior Gateway Routing Protocol (IGRP) and Routing Information Protocol (RIP). Link-state offers several advantages over distance vector protocols. It is faster converging, supports much larger inter-networks, and is less susceptible to routing loops.
RIP	**Routing Information Protocol:** A distance vector protocol that maintains a list of the distances to other networks measured in hops. Limited in scale because any distance greater than 15 hops is inaccessible. Broadcasts updates every 30 seconds to all neighboring RIP routers to maintain integrity. Each update is a full route table.
OSPF	**Open Shortest Path First:** An open, scalable, link state protocol that uses a link speed-based metric to determine the shortest path to each node. Each router maintains a simplified map of the entire network. Updates are sent via multicast, and are sent only when the network configuration changes. Each update only includes changes to the network.

3.5.2 Route Table Integrity

A rogue router could send a fictitious routing update to convince a site's premise router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information of the site's network, or merely used to disrupt the network's ability to effectively communicate with other networks.

There are two approaches that can be used to safeguard the integrity of a route table: static routes and neighbor router authentication. For obvious reasons, defining static routes is the most secure method and is ideal for small stable networks. When using routing protocols to make route table updates due to changes in network topology and connection states, neighbor router authentication must be used to prevent fraudulent route updates from being received. Authentication occurs when routing updates are exchanged between neighbor routers; thereby, ensuring that a router receives routing information only from a trusted source. Neighbor router authentication is supported by all routing protocols listed in Table 1 (except RIP Version 1).

There are two types of neighbor router authentication that can be used: plain text authentication and Message Digest Algorithm Version 5 (MD5) authentication. The message digest is created using the key and a message, but the key itself is not sent, preventing it from being read while it is being transmitted. Plain text authentication sends the authenticating key itself over the network. All of the routing protocols listed in Table 1 support MD5 authentication.

Note: MD5 for IS-IS was introduced in Cisco IOS software version 12.2(13) T and is only supported on a limited number platforms.

As with all secret keys and passwords, it is imperative that you closely guard the authentication keys used in neighbor router authentication. The security benefits of this feature are reliant upon keeping all authentication keys confident by using controlled methods for exchanging the keys as well as changing the keys on a regular basis.

Note: As of this writing, neighbor router authentication will not be required between the site's premise router and a NIPRNet or SIPRNet hub router

- (NET0400: CAT II) *The router administrators will ensure that neighbor router authentication using MD5 has been implemented on all premise routers for the purpose of receiving route table updates from any neighbor or peer router other than a NIPRNet or SIPRNet backbone router.*

- (NET0410: CAT II) *The router administrators will restrict routing table updates to known IP addresses of the neighbor routers with appropriate filtering in the ingress ACL.*

- (NET0420: CAT III) *The NSO will ensure that written procedures for MD5 overall key management will include: key exchange, storage, and expiration.*

3.5.3 Router Accounts

Restricting access to all routers is critical in safeguarding the network. In order to control and authorize access, an authentication server that provides extended user authentication and authority levels will be implemented.

- (NET0440: CAT II) *The router administrators will ensure that all user accounts are assigned the lowest privilege level that allows them to perform their duties.*

- (NET0450: CAT I) *The NSO will ensure that only router administrators and other authorized personnel will be granted access accounts for the router.*

- (NET0460: CAT I) *The router administrators will ensure that each user has their own account to access the router with username and password.*

- (NET0470: CAT II) *The router administrator will immediately remove accounts from the authentication server or router that are no longer required.*

- (NET0480: CAT II) *The IAO will ensure the site utilizes TACACS+, RADIUS, or other DOD approved authentication server for administrative access to the router.*

- (NET0485: CAT II) *The IAO will ensure that when an authentication server is used for administrative access to the router, only one account can be defined locally for use in an emergency (i.e., authentication server or connection to the server is down). The username and password must be sealed in an envelope and stored in a secure container or safe until needed.*

- (NET0490: CAT II) *The NSO will ensure all access points have passwords (e.g., console, auxiliary, vty, etc).*

- (NET0510: CAT II) *The NSO will ensure all router levels (privileged and non-privileged alike) are password protected. Passwords will be created and maintained using accepted password management schemes as outlined in Appendix C, CJCSM and DISA Computing Services Security Handbook References.*

3.5.4 Router Passwords

Individual user account passwords will be set up and maintained in accordance with the guidance contained in *Appendix C, CJCSM and DISA Computing Services Security Handbook References*. There are two password protection types provided by Cisco Internetworking Operating System (IOS): Type 7 and Type 5. Type 7 uses the Cisco defined encryption algorithm, which is regarded as weak in the commercial security community. Type 7 encryption can be applied to the **enable password**, **username**, and **line password** commands using the **service password-encryption** command. Type 5 encryption, which uses a Message Digest 5 (MD5) hash algorithm, is considered a stronger mechanism and is used by the **enable secret** command.

Note: The **service password-encryption** command does not protect the following secret values: SNMP community strings and usernames, RADIUS or TACACS+ keys, and FTP usernames and passwords. Consequently, these values must not be set to any other password.

- (NET0560: CAT I) *The router administrators will ensure that Type 5 encryption is used for enable mode (a.k.a. privileged mode) via **enable secret** password.*

- (NET0590: CAT III) *The router administrators will ensure the **enable secret** password does not match any other user password or any other **enable secret** password (i.e., each router will have its own **enable secret** password).*

- (NET0600: CAT II) *To prevent others from reading passwords when they are displayed on the screen, the router administrators will make sure to ensure the **service password-encryption** option is used.*

- (NET0620: CAT II) *The router administrator will never set the SNMP community string or username, RADIUS or TACAC+ keys, or FTP username or password to any other password.*

3.5.5 Out-of-band Router Management

Router management is performed out-of-band via the console (**con**) port. The con port will be configured to time out, so that if an administrator forgets to log out, the router will log the administrator out automatically. The auxiliary (**aux)** port will be disabled. Users should never connect a modem to the aux port as a backup or remote access method to the router. In addition to the requirements set forth in *Section 3.4.2.1, Out-of-band Management*, the following additional requirements apply to out-of-band router management:

- (NET0630: CAT III) *The router administrators will ensure that the router's aux port is disabled.*

- (NET0640: CAT II) *The NSO will ensure modems are not be used for remote administration.*

- (NET0650: CAT II) *The router administrators will ensure the router console port is protected from casual use and is configured to time out after 15 minutes of inactivity.*

- (NET0660: CAT III) *The router administrators will disable router interfaces that are not in use.*

3.5.6 In-band Router Management

The following connection schemes are supported for in-band router administration:

1. **Remote Internal only with authentication, authorization, and accounting (AAA).** Administration can be performed on the router from a trusted internal network only, and AAA is used for access control. The router administrator will use the currently supported version of SSH with all security-related patches applied for remote administration.

2. **Remote Internal only.** Administration can be performed on the router from the internal network only. The router administrator will use the currently supported version of SSH with all security-related patches applied for remote administration.

   Remote administration with telnet is inherently dangerous because anyone with a network sniffer and access to the right LAN segment can acquire the router account and password information. Remote administration security issues center on protecting the paths that the session will use to access the router. The options listed above are listed in the order that best protects the router and allows for accounting of router activities. This section will discuss remote internal only. Cisco has added support for the SSH protocol starting with IOS 12.0, and it will be used for encrypting administrative connections. There have been some security vulnerabilities found with SSH 1.x, but with vendor patches it will provide a high level of encryption protection.

   - Remote external access (e.g., dial-up) will not be used to administer the routers except as outlined in Section 3.4.2.1, Out-of-band Management.

Access lists must limit which hosts may connect to the router through the Virtual Teletype (VTY) ports. Additionally, the IP addresses, which will be restricted to administrators only, must be on an internal interface. In addition to the requirements set forth in *Section 3.4.2.2, In-band Management*, the following additional requirements apply to In-band router management:

Note: In-band management is only to be used in situations where Out-of –band management has been deemed to hinder operational commitments, and the IAO has approved in writing the use for that specific purpose.

- (NET0670: CAT II) *The router administrators will ensure that the VTY ports only accept connections from internal network interfaces and be restricted to authorized IP addresses.*

- (NET0680: CAT II) *The router administrators will ensure all VTY ports are restricted to SSH.*

- (NET0685: CAT II) *The NSO will ensure the timeout for unattended Virtual Terminal (VTY) ports is set for no longer than 15 minutes via the* ***exec-timeout*** *command.*

- (NET0690: CAT IV) *The router administrators will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*

3.5.7 Router Global Configuration Commands

Cisco routers support a large number of network services at various layers of the OSI model. Some of these services can be restricted or disabled, thus improving security without degrading the operational use of the router. Some of these services are application layer protocols that allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations, but which are detrimental to

network security. The best security practice for routers is to only support the services and protocols needed by the network to meet operation commitments.

Turning off a network service on the router itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the **Boot Protocol (bootp)** protocol is employed, but some other host is acting as the **bootp** server. In this case, the router's **bootp** server needs to be disabled.

In many cases, Cisco IOS supports turning a service off entirely, or restricting access to particular network segments or sets of hosts. If a particular portion of a network needs a service but the rest does not, then the restriction features should be employed to limit the scope of the service.

Turning off an automatic network feature usually prevents a certain kind of network traffic from being processed by the router or prevents it from traversing the router. For example, IP source routing is a little-used feature of IP that can be utilized in network attacks.

Table 2 below lists some of the services offered on Cisco IOS 11.2, 11.3, and 12. This list has been kept short by including only those services and features that are security-relevant and may need to be disabled.

Cisco issues new IOS versions and upgrades on a regular basis, making it an administrative nightmare to keep all the routers on a large network up to date. Newer versions of the IOS fix bugs and vulnerabilities that existed in the older versions, and add new security features. To guard against security weaknesses identified in the older versions of the IOS, the router administrator will implement the minimum required IOS Release 12.3.

Note: See Appendix I for Juniper router configuration requirements.

- (NET0700: CAT II) *The router administrator will, at a minimum, deploy Cisco IOS Version 12.3, or the most current general deployment (GD) release, and address all applicable IAVM vulnerabilities.*

- *The router administrator will secure their routers by following the instructions listed in Table 2, Overview of IOS Features to Disable or Restrict.*

TABLE 2. OVERVIEW OF IOS FEATURES TO DISABLE OR RESTRICT

FEATURE	*DESCRIPTION*	*DEFAULT*	*REQUIREMENT*
Cisco Discovery Protocol (CDP	Proprietary layer 2 protocol between Cisco devices	Enabled	Disable (NET0710: CAT III)
TCP small servers	Standard TCP network services: Echo, chargen, etc.	11.3: Disabled 11.2: Enabled	Disable (NET0720: CAT III)
UDP small	Standard User Datagram	11.3: Disabled	Disable

FEATURE	*DESCRIPTION*	*DEFAULT*	*REQUIREMENT*
servers	Protocol (UDP) network services: Echo, discard, etc.	11.2: Enabled	(NET0720: CAT III)
Finger	UNIX user lookup service; allows remote listing of users.	Enabled	Disable (NET0730: CAT III)
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	Disable (NET0740: CAT II)
Bootp server	Service to allow other routers to boot from this one.	Enabled	Disable (NET0750: CAT III)
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	Disable (NET0760: CAT II)
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	Disable (NET0770: CAT II)
Proxy ARP	Router will act as a proxy for layer 2 address resolution.	Enabled	Disable (NET0780: CAT II)
IP directed broadcast	Packets can identify a target LAN for broadcasts.	Enabled	Disable (NET0790: CAT III)
IP unreachable notifications	Router will explicitly notify senders of incorrect IP addresses.	Enabled	Disable (NET0800: CAT II)
IP mask reply	Router will send an interface's IP address mask in response to an ICMP mask request.	Disabled	Disable (NET0800: CAT II)
IP redirects	Router will send an ICMP redirect message in response to certain routed IP packets.	Enabled	Disable (NET0800: CAT II)
Network Time Protocol (NTP) service	Router can act as a time server for other devices and hosts.	Enabled	Set the NTP server address (minimum of two servers will be utilized). (NET0810: CAT III)
Domain Name Service	Routers can perform DNS name resolution.	Enabled	Set the DNS server address. (NET0820: CAT III)

3.6 Access Control Lists (ACLs)

Cisco IOS uses access lists to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of Cisco routers makes very heavy use of access lists for restricting access to services on the router itself as well as for filtering traffic passing through the router.

Sites will implement router ingress and egress filter ACLs based on a policy of **Deny by Default.** All services and protocols required by the site for operational commitments and thus permitted by the ACLs will be in accordance with the guidelines contained in *Appendix G, Required Filtering Rules*.

Note: Those ports and services that are noted as conditional are permitted as long as they meet the specific condition. Several of these must be restricted by source or destination address. Connections initiated by clients from external networks for services such as http, dns, smtp, and ftp must be restricted to only those servers residing in the DMZ or service network.

The site will enable logging on all ACL statements that block access. This feature will provide valuable information about what types of packets are being denied and can be used to enhance the sites intrusion detection capabilities.

- (NET0830: CAT I) *The router administrator will implement router ACLs on all interfaces based on a policy of Deny by Default.*

CAVEAT: If the site has implemented a firewall on the perimeter based on a policy of Deny by Default, this finding can be downgraded to a Category II. If the site has implemented a firewall on the perimeter based on a policy of Deny by Default and has a documented plan to implement router ACLs based on a policy of Deny by Default, this can be downgraded to a Category III.

Note: When verifying compliance with the Deny-by-Default requirement, first verify that the ACL ends with the *deny any* (implied or exlicit) rule as the last line in the ACL. Then verify that what is permitted by the ACL is IAW Appendix G of this STIG. This requirement applies to all internal and external interfaces.

If the router is in a Deny-by-Default posture, and what is allowed through the ACL is IAW Appendix G of this STIG, then all requirements related to ports being blocked would be satisfied. These ports would be covered under the Deny-by-Default rule as long as a permit rule was not created for them.

When the site is in a allow-all posture, all lines in the ACL need to be verified for compliance with Appendix G of the Network Infrastructure STIG, and all ports that are mandated to be blocked will have to have a rule created to block these ports. Furthermore, the router will still be given a finding for not being in the Deny-by-Default posture.

- (NET0840: CAT II) *The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in Appendix G, Required Filtering Rules, for all services and protocols required for operational commitments.*

- *(NET0845: CAT II) Bind the ingress ACL filtering packets entering the network to the external interface (inbound) and the egress ACL filtering packets leaving the network to the internal interface (inbound).*

- (NET0850: CAT III) *The router administrator will ensure that deny statements in an ACL have a log statement that follows to ensure any attempts to access the port will be logged.*

3.6.1 Filtering Traffic to Router

Access lists are used in a variety of ways to control access to services on the router itself. While it is possible to incorporate access controls for these services into the access lists placed on interfaces, it is typically easier and more reliable to use the specialized facilities that IOS makes available to apply access controls directly to the services themselves. For more information about unneeded services on the router, see *Section 3.5.8, Router Global Configuration Commands.*

SNMP Service:
A Cisco router can be configured to act as a client for SNMP. When SNMP service is enabled on a router, network management tools can use it to gather information about the router configuration, route table, traffic load, and more. SNMP will only be used on the internal network interfaces.

- (NET0890: CAT II) *The router administrator will restrict SNMP access to the router to only the allowed IP addresses.*

- (NET0900: CAT II) *The router administrator will ensure SNMP is used only on the internal network interfaces.*

- (NET0925: CAT II) *The router administrators will ensure SNMP will be enabled in the read only mode; Read/Write will not be enabled unless approved by the IAO.*

3.6.2 Filtering Traffic through the Router

3.6.2.1 IP Address Spoof Protection

Inbound Traffic

In Software Release 11.1, Cisco introduced the ability to assign inbound access lists to an interface. This allows a network administrator to filter packets before they enter the router instead of as they leave the router. Inbound access lists can be used to prevent some types of IP address spoofing, whereas outbound access lists alone will not provide sufficient security. For background information on anti-spoofing, refer to the Joint Task Force Computer Network Operations (JTFCNO) 0101.

- (NET0940: CAT I) *The router administrators will restrict the router from accepting any inbound IP packets with a source address that contain an IP address from the internal network, any local host loop back address (127.X.X.X), the link-local IP address range (169.254.0.0), or any reserved private addresses in the source field*.

Outbound Traffic

Egress filtering rules will be applied denying all outbound traffic with an illegitimate address in the source address field. This is to prevent the network from being part of a Distributed Denial of Service (DDoS) attack.

Unicast Reverse Path Forwarding, available with Cisco routers running IOS 12.0 or higher, provides another mechanism for IP address spoof protection. When Unicast RPF is enabled on an interface, the router examines all packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified. If Unicast RPF does not find a reverse path for the packet, the packet is dropped. This "look backwards" ability is available only when Cisco Express Forwarding (CEF) is enabled on the router as it uses the CEF table.

- (NET0950: CAT I) *The router administrators will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or enabling Unicast Reverse Path Forwarding .*

3.6.2.2 Exploits Protection

SYN Flood Attack

The first packet in the TCP three-way handshake sets the SYN bit. When a host receives an initial SYN packet requesting a provided service, the host responds with a packet setting the SYN and ACK bits, and waits for an ACK from the initiator of the connection request. If the initiator never responds to the host, the host will eventually time out the connection. However, while the host is still waiting for the ACK to complete the connection, the half-open connection consumes resources on the host—that is, entries in the connection table.

If there is an attack, the source address in these SYN packets is forged and probably unreachable. In most cases, the source address will either be an unregistered address or the address of a host the attacker knows does not exist. Therefore, the attacked host will never receive a response to its request to complete the initial three-way handshake and must wait to time out thousands of connections. During the wait, the server must ignore legitimate requests since its connection table is full.

In intercept mode, the router responds to the incoming SYN request on the server's behalf with a SYN-ACK and waits for an ACK from the client. If an ACK is received, the original SYN packet is sent to the server, and the router completes the three-way handshake with the server on behalf of the client and joins the two half-connections together transparently. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

In watch mode, the router allows the SYN requests through to the server. If the session fails to establish itself during specified period of time, the router sends a reset (RST) to the server to clear the connection. The amount of time the router waits is configurable with the **ip tcp intercept watch-timeout** command.

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset. To optimize router resources, it is recommended to reduce this to 10 seconds using the following command:

ip tcp intercept watch-timeout 10

By default, the software still manages a connection for 24 hours after no activity. It is recommended to change this to 60 seconds using the following command:

ip tcp intercept connection-timeout 60

TCP intercept is available on all Cisco Routers with IOS Version 11.3 or greater. Most firewalls can also provide protection against SYN flood attacks using the similar concept of "proxying" or "watching" the connection until the three-way handshake is complete. SYN flood protection must be implemented on either the premise router or the firewall located on the sites' network perimeter. If the router will be providing the SYN flood protection using the TCP intercept software, it is the site's option to implement this feature in either intercept or watch mode.

- (NET0960: CAT II) *The router administrators will use the TCP Intercept command to protect servers from any TCP SYN flood attacks from an outside network.*

CAVEAT: If the site has implemented SYN flood protection for the network using the perimeter firewall, there is not an additional requirement to implement it on the router.

Smurf Attack

The Smurf Attack involves sending a large amount of ICMP Echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. If a router is positioned to forward broadcast requests to other routers on the protected network, then the router needs to be configured to prevent this forwarding from occurring. This blocking can be achieved by denying any packets destined for broadcast addresses.

- (NET0970: CAT II) *The router administrators will prevent Smurf attacks by configuring the router to deny packets destined for broadcast addresses.*

ICMP Message Types and Traceroute

There are a variety of ICMP message types. Some are associated with programs (e.g., the ping program works with message types Echo Request and Echo Reply). Others are used for network management and are automatically generated and interpreted by network devices.

ICMP Message Number	ICMP Message name	Configuration recommendation
0	Echo Reply	Allow inbound only
3	Destination Unreachable	Allow inbound only
4	Source Quench	Allow both directions
5	Redirects	Denied both directions
8	Echo Request	Allow outbound only
11	Time exceeded	Allow inbound only
12	Parameter problem	Allow both directions
30	Traceroute	Allow outbound only

With Echo packets an attacker can create a map of the subnets and hosts behind the router. Also, an attacker can perform a denial of service attack by flooding the router or internal hosts with Echo packets. With ICMP Redirect packets, the attacker can cause changes to a host's routing tables. Otherwise, the other ICMP message types should be allowed inbound except message types Echo Request and Redirect.

- (NET0980: CAT II) *The router administrators will block inbound ICMP traffic message types Echo Request and Redirect to reduce the chance of denial of service attacks.*

For outbound ICMP traffic, the router administrator should allow the message types Echo Request, Parameter Problem, and Source Quench, and block all other message types unless needed for operational commitments. With Echo packets, users will be able to ping external hosts. Parameter Problem packets and Source Quench packets improve connections by informing about problems with packet headers and by slowing down traffic when it is necessary.

- (NET0990: CAT II) *The router administrator will block outbound ICMP traffic message types Echo Reply, Destination Unreachable, Time Exceeded, and Redirect to reduce the chance of denial of service attacks.*

Another program that deals with certain ICMP message types is **traceroute**. Traceroute is a utility that prints the IP addresses of the routers that handle a packet as the packet hops along the network from source to destination. On UNIX and Linux operating systems, traceroute uses UDP packets and causes routers along the path to generate ICMP message types **Time Exceeded** and **Unreachable**. An attacker can use traceroute response to create a map of the subnets and hosts behind the router, just as they could do with ping's ICMP Echo Reply messages.

Therefore, block inbound traceroute by including a rule in the inbound interface access list to block ports 33400 through 34400 that are the UDP ports commonly used by traceroute.

- (NET1000: CAT III) *The router administrators will block all inbound traceroutes to prevent network discovery by unauthorized users.*

Distributed Denial of Service (DDoS) Attacks

Several high-profile DDoS attacks have been observed on the Internet. While routers cannot prevent DDoS attacks in general, it is usually sound security practice to discourage the activities of specific DDoS agents (a.k.a. zombies) by adding access list rules that block their particular ports. Sites will utilize automated scanning for DDoS tools on all servers, routers, and other communications devices.

- (NET1010: CAT I) *The router administrators will block known DDoS attack ports in accordance with Appendix G, Required Filtering Rules.*

The example below shows access list rules for blocking several popular DDoS attack tools.

TRINOO DDoS systems
```
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log
```

Back Orifice systemb
```
access-list 170 deny udp any any eq 31337 log
```

Stacheldraht DDoS system
```
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
```

TrinityV3 system
```
access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
```

T0rn rootkit system
```
access-list 170 deny tcp any any eq 47017 log
```

Subseven DDoS system and some variants
```
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

3.6.3 Logistics for Configuration Loading and Maintenance

There are two basic approaches for configuration loading and maintenance—online editing and offline editing. Each has its advantages and disadvantages. Online editing provides for syntax

checking but provides limited editing capability and no comments. Offline editing provides the ability to add comments, allows for the use of better editors, and guarantees all settings will be visible, but provides no syntax checking. It is important to keep the running configuration and the startup configuration synchronized, so that if there is a power failure or some other problem, the router will restart with the correct configuration. If there is a need for old or alternative configurations, they should be stored offline. In this situation, it is only necessary to manage the startup configuration since the running configuration is identical.

Cisco configuration save utilities will also not save default values. Because each Cisco IOS release changes the default values for some of the commands, tracking the configuration can become very difficult. However, if the offline method is used, this will leave passwords in the clear. The recommended approach is a hybrid of the two, ensuring that the encrypted strings for the passwords are placed into the configuration file.

If you set passwords in an offline configuration file, then they will be stored in the clear and transferred in the clear. Instead, it is best to type the passwords while online (using the console) and then copy the encrypted strings to the offline configuration. This is especially true for the **enable secret** password. The example below shows how an encrypted **enable secret** setting would appear in an off-line configuration file. You can obtain the encrypted string by setting the password manually on the router console, then displaying the running configuration, and then copying and pasting the encrypted string into your offline configuration file.

With the configuration files offline, the files must be transferred to the router in a secure method. The possible methods for transferring files to a router have increased with newer IOS releases. The primary mechanisms available are tftp and ftp (available for IOS 12.0 and newer). The most secure method for transferring configuration files is FTP. The IOS allows the FTP username and password to be stored in an encrypted format as part of the configuration. The **FTP** command will transparently insert this username and password when connecting to the FTP server. Access controls can also be used to control the IP address from which the file transfer can be performed.

- (NET1030: CAT III) *The router administrator, when saving and loading configurations will always ensure that the running and startup configurations are synchronized.*

- (NET1040: CAT IV) *The router administrator will ensure at least the current and previous router configurations will be stored in a secured location to ensure a proper recovery path.*

- (NET1050: CAT III) *On the system where the configuration files are stored, the router administrators will use the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).*

- (NET1050: CAT III) *The IAO will ensure only authorized router administrators will be given access to the stored configuration files.*

- (NET1060: CAT I) *The router administrators will not store unencrypted router passwords in an offline configuration file.*

- (NET1070: CAT II) *When performing remote router administration, the router administrators will use the FTP protocol to transfer the configuration files to and from the router.*

- (NET1080: CAT II) *The router administrators will ensure that the FTP username and password are configured as part of the IOS configuration using the **IP FTP** command.*

- (NET1090: CAT III) *The router administrators will use ACLs to limit access to the FTP server.*

3.6.4 Router Change Management

People and organizations are forever moving and changing work locations. This sometimes requires updates to router tables. The point-of-contact (POC) for each router is usually recorded with the domain registration authority for troubleshooting purposes. However, this can open up the change request process to possible spoofing. A person can impersonate the authorized POC and request updates that can deny or stop services altogether.

- (NET1110: CAT II) *The NSO will ensure all router changes and updates will be documented in a manner suitable for review.*

- (NET1110: CAT II) *The NSO will ensure request forms will be used to aid in recording the audit trail of router changes requested.*

- (NET1110: CAT II) *The NSO will ensure changes and modifications to routers will be audited so that they can be reviewed.*

- (NET1110: CAT II) *The router administrator will ensure current paper or electronic copies of router configurations will be maintained in a secure location.*

- (NET1110: CAT II) *The NSO will ensure only authorized personnel, with proper verifiable credentials, will be allowed to request changes to routing tables or service parameters.*

3.6.5 DOD Ports and Protocols Technical Guidance

The understanding of mutually accepted risk within the NIPRNet community seeks to provide maximum interoperability while maintaining an emphasis on security. The logic is that all participants inside the NIPRNet share a common level of risk to their systems, defined by the protections established at the NIPRNet/Internet boundary, and the minimum level of protection found at all internal enclave boundaries to the NIPRNet backbone. To mitigate this threat, DOD is in the process of establishing a NIPRNet ports and protocols security document. This document, when approved, will establish the DOD community policy for firewall and router implementations for the NIPRNet. It will provide detailed configuration settings for known identified combinations of ports, protocols, and services (PPS). It will recommend security countermeasures for minimizing the vulnerabilities for use of risky ports, protocols, and services that are used by essential applications.

- The router administrators will comply with the DOD Ports and Protocol Technical Guidance on all routers once the policy is approved.

3.6.6 SYSLOG

Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. It provides the network administrator the ability to send log messages from all of the communication devices on a network to a central host for examination and storage.

Level	Level Name	Description	Example
0	**Emergencies**	Router becoming unusable	IOS could not load
1	**Alerts**	Immediate action needed	Temperature too high
2	**Critical**	Critical condition	Unable to allocate memory
3	**Errors**	Error condition	Invalid memory size
4	**Warnings**	Warning condition	Crypto operation failed
5	**Notifications**	Normal but important event	Interface changed state, up or down
6	**Informational**	Information message	Packet denied by access list
7	**Debugging**	Debug message	Appears only when debugging is enabled

- (NET1120: CAT III) *The NSO will ensure a centralized syslog server will be deployed and configured by the syslog administrator to store all syslog messages for a minimum of 30 days and then stored offline for one year.*

- (NET1130: CAT III) *The syslog administrator will configure syslog messages levels 0 through 6 for collection. Level 7 messages can optionally be configured during debugging.*

- (NET1140: CAT III) *The syslog administrator will secure the syslog servers in accordance with the appropriate operating system STIG(s).*

- (NET1150: CAT III) *The syslog administrator will configure the syslog server to accept messages from only authorized devices (restricting access via source and destination IP address).*

3.7 Firewalls

Perimeter filtering rules can be applied to any internal firewall device or router and should be implemented to the fullest extent possible. This is necessary in order to minimize the internal threat and protect the enclaves. Allowing only approved IP addresses through the perimeter router will control access to required ports and services. The Enclave firewall rules should be based on applications being used within internal Enclave; all non-required ports and services should be blocked to the most restrictive rules possible and what is allowed through the firewall needs to be configured IAW Appendix G (*"that which is not expressly allowed is denied"*).

- (NET1160: CAT I) *The IAM will ensure that a firewall has been implemented to protect the entire facility and has been configured with a deny-by-default policy and that what is allowed is in accordance with Appendix G of this document.*

3.7.1 Firewall Architecture

The Dual-Homed with Screened Subnet Firewall Architecture will be used (see *Figure 1* below). This firewall is set up as a gateway with three network interface cards (NICs)—one connected to the external network through a router, one to the internal network, and one to the DMZ (if applicable). Packet forwarding is disabled on the gateway and information is passed at the application level or the network layer, depending on the type of firewall used. The firewall/gateway can be reached from all sides, but traffic cannot directly flow across it unless that particular traffic is allowed to pass to the requested destination.

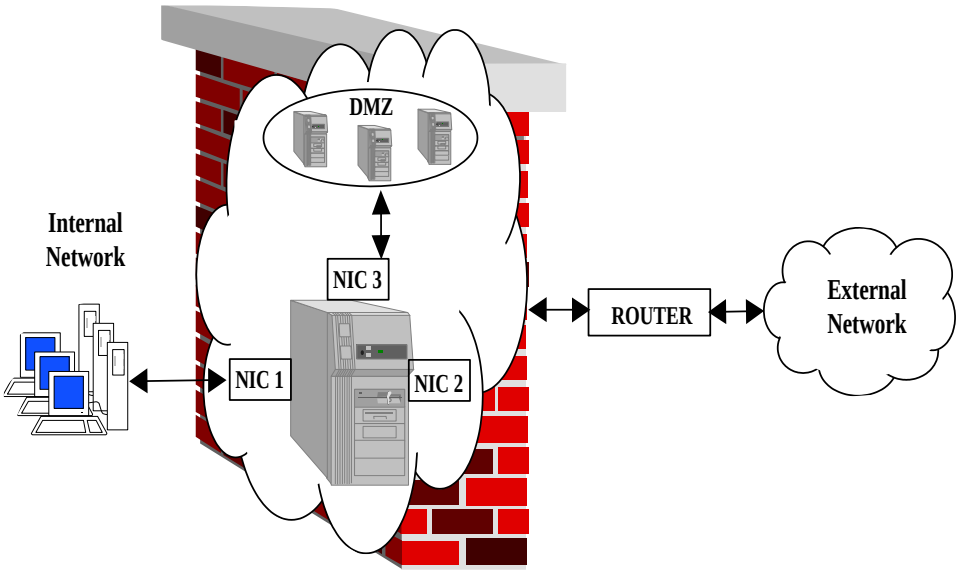


FIGURE 1. DUAL HOMED WITH SCREENED SUBNET (DMZ)

- (NET1170: CAT II) *The IAM will ensure that only firewalls that have been submitted (under review or obtained validation) for review against the DoD Application-Level for Medium Robustness Environments Protection Profile (PP) are placed in the network infrastructure.*

- (NET1170: CAT II) *The IAM will ensure firewalls that do not attain EAL4 or higher rating will not be used unless justified by a mission requirement and approved by the EMCB.*

- (NET1180: CAT II) *The NSO will ensure that the Dual-Homed with Screened Subnet (DMZ) Firewall Architecture is implemented.*

- (NET1190: CAT II) *All networks will use application-level firewalls to secure connections to the Internet, NIPRNet, SIPRNet, or other external networks. The IAM will ensure prior to purchase that the application-level firewall(s) will, at a minimum, include proxies for the following network applications:*

  - *Simple Mail Transfer Protocol (SMTP)*
  - *HyperText Transfer Protocol (HTTP)*
  - *Secure HyperText Transfer Protocol (SHTTP)*
  - *Network News Transfer Protocol (NNTP)*
  - *Telnet*
  - *File Transfer Protocol (FTP)*
  - *Secure Shell (SSH)*
  - *RealAudio*

- (NET1190: CAT II) *The NSO will ensure that if network applications\services are needed, they are proxied at the firewall using the application proxies provided by the manufacturer to avoid bypass or circumvention of DISA-managed firewalls (i.e., generic/plug proxies will not be used in lieu of vendor provided proxies.)*

- (NET1190: CAT II) *The Firewall Administrators (FA) will implement generic/plug proxies for all applications\services that do not have a vendor provided proxy (i.e., all applications\services must be proxied.) All generic/plug proxies will be reported in the DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT to include operation requirement and mitigation being performed (e.g., restricted to source and destination).*

3.7.2 Firewall Placement

A firewall can be placed at several locations to provide protection from attacks. Each implementation will differ depending on several key factors, including the sensitivity of the networks, the network infrastructure, and the type of network traffic. Usually firewalls are used to protect the boundaries of a network, although at times they can be used to separate an internal security domain from the rest of an enclave. There are three main points at which a firewall can be implemented within a network—at LAN-to-WAN connections, at LAN-to-LAN connections, and at WAN-to-WAN connections.

The Enclave requirement to place an application-level firewall at the perimeter can be accomplished by multiple scenarios to include the following:

- An application-level firewall at the perimeter to protect the whole Enclave to include the Security Domains

- A non application-level firewall at the perimeter (e.g., stateful inspection, hybrid, packet-filter) with an application-level firewall protecting every Security Domain (including the DMZ) with no IP addressable systems or devices operating in the area between the non application-level firewall and the Security Domain's firewall

- (NET1200: CAT II) *The IAO will ensure, when protecting the boundaries of a network, the firewall will be placed between the internal network (NIC 1) and the perimeter router (NIC 2) and the DMZ (NIC 3).*

3.7.3 Reporting

A firewall implementation description, as outlined in *DISA Instruction 630-230-31, Supplement 2.3,* will be developed and maintained for each DISA-managed firewall.

- (NET1210: CAT III) *The IAO will ensure the SSAA will be updated to reflect the installation or modification of the site's firewall.*

- (NET1210: CAT III) *If the configuration of the firewall cannot be maintained in accordance to DISA Instruction 630-230-31, Supplement 2.3, the FA or NSO will request an extension.*

- (NET1210: CAT III) *The NSO will establish policies outlining procedures to notify DOD-CERT or the respective RCERT when suspicious activity is observed.*

3.7.4 Identification & Authentication

Identification and authentication is one of the major functions provided by the firewall. While users on the inside of a firewall are often considered trusted, external users who require access to the internal network must be authenticated. At a minimum, the firewall must support a secure, strong user authentication system (e.g., SecureID, Radius, or TACACS+).

Note: In-band management is only to be used in situations where Out-of –band management has been deemed to hinder operational commitments, and the IAO has approved in writing the use for that specific purpose.

- (NET1220: CAT II) *The NSO will ensure the firewall will uniquely identify and authenticate the identity of a user before granting access to the firewall's administration interface.*

- (NET1220: CAT II) *The NSO will ensure all user and administrator accounts are assigned the lowest privilege level that allows them to perform their duties.*

- (NET1220: CAT II) *The NSO will ensure the firewall is set to lock out accounts after three unsuccessful logon attempts. If a firewall account is locked, then the NSO or NSO representative is required to unlock the account.*

- (NET1220: CAT II) *Only the FA(s) will be allowed to authenticate on the firewall administration interface remotely.*

- (NET1220: CAT II) *The IAO will ensure only authorized personnel, as defined by the local commander or IAM, have permission to change security settings on the firewall.*

- (NET1220: CAT II) *The IAO will ensure that all firewalls that support public key certificates are be interoperable with DOD Security Management Infrastructure (SMI) and Public Key Infrastructure (PKI).*

3.7.5 Configuration

The firewall must protect the private network from external attacks. The firewall will be maintained with the currently supported version of the firewall software and the Operating System (OS) with all security-related patches applied. The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches. Content Vector Protocol (CVP) compliant applications run AntiVirus software and scanning products that block hostile code (i.e., viruses, malicious code, Java applets) from entering the network. Transactions from the Internet are sent by the firewall directly to this server where they are scanned for hostile code, then returned to the firewall for delivery to your users.

- (NET1240: CAT II) *The NSO will ensure that the firewall is be able to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.*

CAVEAT: If the site has implemented SYN flood protection for the network using the premise router, it is not an additional requirement to implement this on the firewall.

- (NET1250: CAT II) *The FA will ensure the firewall is secured in accordance with the appropriate operating system STIG.*

- (NET1250: CAT II) *The FA will ensure the firewall will not utilize any services or capabilities other than firewall software (i.e., DNS servers, e-mail client or servers, ftp servers, web servers, etc.), and if these services are part of the standard firewall suite, they will be either uninstalled or disabled.*

- (NET1250: CAT II) *The FA will use the currently supported version of the firewall software and the OS, with all security-related patches applied.*

- (NET1260: CAT III) *The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.*

- (NET1260: CAT III) *The IAO will ensure that gateway content security checking of all inbound packets will be performed using a CVP compliant program in conjunction with the firewall (Two such products, Norton AV for Firewalls and McAfee Webshield, are available on the DOD-wide virus detection tool site,* http://www.cert.mil/.) *If CVP is not supported by the firewall, then a SMTP content security checking gateway will be installed as well as content security checking software on the e-mail server.*

- (NET1270: CAT III) *The FA will ensure that upon initial start-up of the firewall or recovery from an interruption in firewall service, the firewall will not compromise its resources or those of any connected network.*

3.7.6 Auditing and Administration

The firewall must be administered by qualified personnel who are specifically trained in the operation and administration of the firewall. At least two firewall administrators will be identified for each DISA-managed firewall. Follow the auditing and administration rules below:

- (NET1280: CAT III) *Firewall log data will be reviewed on a daily basis by the firewall administrator (FA), or other qualified personnel, to determine if attacks or inappropriate activity has occurred.*

- (NET1280: CAT III) *The FA will ensure the firewall logs will be retained online for a minimum of 30 days and then stored offline for one year.*

- (NET1280: CAT III) *The NSO will ensure the firewall, including system software, configuration data, database files, and log data, will be backed up weekly and whenever configuration changes occur.*

- (NET1290: CAT II) *The NSO will ensure the firewall is configured to alert the administrator of a potential attack or system failure.*

- (NET1300: CAT III) *The FA will ensure the following capabilities will be enabled on the firewall:*

  - *Log unsuccessful authentication attempts.*

  - *Stamp audit trail data with the date and time when recorded.*

  - *Record the Source IP, Destination IP, protocol used, and the action taken.*

  - *Log administrator logons, changes to the administrator group, and account lockouts.*

  - *Protect audit logs from deletion and modification.*

- *The firewall will provide the ability to record a readable audit log of security-related events, with accurate dates and times, with the capability to search and sort the audit log based on relevant attributes.*

- (NET1310: CAT II) *The FA will comply with the requirements contained in Section 3.4.2.2, In-band Management, for all forms of remote firewall administration.*

3.7.7 Implementation and Description Report

The CIO maintains a repository of firewall configuration data of all managed firewalls. To aid the CIO in keeping the repository up to date, FAs must report all new firewall installations, or modifications to current managed firewalls to the CIO for approval using the DISA Enclave Security Implementation Description Report.

- (NET1320: CAT II) *The CIO is responsible for maintaining a repository for the reported configuration data of all DISA-managed firewalls. Extensions submitted for exceptions to this guidance require DISA FSO review. Upon review, recommendations will be forwarded to the CIO for final disposition. (See Appendix H for example report format)*

- (NET1320: CAT II) *The FA will submit a DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT upon completion of a new installation. The FA will report all existing DISA-managed firewalls that have not been reported to the CIO.*

- (NET1320: CAT II) *The IAO will ensure the DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT is submitted to the CIO when modifications to the current DISA-managed firewall are incorporated. (Examples of a reportable change or modification include new releases of OS or firewall software, new firewall hardware, and new protocols and services through the firewall.)*

- (NET1320: CAT II) *The NSO will submit a request for a extension, along with the DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT, for all changes in the configuration of a firewall that differ from the authorized filtering rules. (Normal ACL changes are not to be reported.)*

3.8 Network Intrusion Detection (NID)\Real Secure

DISA has dedicated funding, equipment, applications, and training to complement the Global Information Grid IA security initiative. The use of the Internet Security Systems, Inc. (ISS), RealSecure Network Intrusion Detection System (IDS), or other NID is a layer of security that can be used to support the GIG.

All DISA locations will install, maintain, and operate a Network IDS inside of their network enclaves. The Enclave Network IDS will monitor internal network traffic and provide near real-time alarms for network-based attacks. Either the RCERT or the local staff may control the enclave Network IDS rules and attack signatures; however, OP7 will provide second-level technical support and configuration management. The site may establish a support agreement

with the RCERT for monitoring. The local staff is responsible for initial response to real-time alarms. Significant incidents are reported to the site's RCERT. Extensions will be granted by the Enclave Management Control Board (EMCB) on a case-by-case basis.

- (NET1330: CAT I) *The Network IDS administrator will ensure a Network IDS is installed and operational with all external connections (e.g., LAN and WAN) being monitored.*

- (NET1340: CAT II) *The NSO will ensure that the site's network IDS policy is IAW this STIG.*

- (NET1340: CAT II) *The NSO will establish policies outlining procedures to notify DOD-CERT or the respective RCERT when suspicious activity is observed.*

- (NET1340: CAT II) *The NSO will ensure that the data collected on the Network IDS is reviewed only by trusted System Administrators and security personnel who have a legitimate need-to-know.*

- (NET1340: CAT II) *The NSO will ensure that authorized reviewers of Network IDS data are identified in writing by the site's commander.*

- (NET1340: CAT II) *The NSO will ensure that any unauthorized traffic is recorded and audited for further investigation.*

- (NET1340: CAT II) *The NSO will establish backup and anti-virus update procedures for the Network IDS.*

- (NET1350: CAT III) *The Network IDS administrator will subscribe to the X-press update notification or similar service offered by the IDS vendor.*

- (NET1350: CAT III) *The Network IDS administrator will update the Network IDS when software is provided by Field Security Operations for the RealSecure distribution, and for all other Network IDS software distributions when a security-related update is provided by the vendor.*

3.9 Data Outlets

Each device connected to an infrastructure data outlet has a corresponding attachment within a communications closet or computer room. These attachments must be monitored to ensure no inactive data outlet is left attached.

- (NET1360: CAT II) *The NSO will ensure that all data outlets not in use are detached in the communications closet and/or disabled from the network infrastructure.*

3.10 Switch\Intelligent Hubs

The most common method of infrastructure wiring today is accomplished using twisted pair cabling in a star topology. Using this convention, all wires are run from a central point (usually a communications closet or computer room) out to each work area. The resulting concentration of wires is connected to an electronic switch/hub or hub that functions as a common bus. This type of device traditionally operates at the OSI layer 2, data link layer, which is the layer responsible for sending and receiving data. Data exchange is based on the hardware address encoded on the host's Network Interface Card (NIC).

Switch\Intelligent Hubs are similar to standard hubs with the additional capabilities of device management and dividing the network into smaller more controllable segments. This provides the means to segment network traffic into separate, smaller segments versus using one large common shared connection. This technology has the capability to enhance throughput by reducing packet collisions and improves security by restricting data to a particular LAN segment.

3.10.1 Switch\Intelligent Hubs Management

Most Switch\Intelligent Hubs have management interfaces, which usually provide three types of logon accounts—Administrator, Diagnostics, and User. Permissions for these accounts are generally tiered, for example. The Administrator logon provides full access to all functions, the Diagnostic user has access to diagnostic features, and the User account has view only access.

Many Switch\Intelligent Hubs have non-volatile memory to store operating parameters and settings, such as Internet Protocol (IP) addresses and default routers. This information is critical to the integrity of the network.

- (NET1370: CAT II) *The NSO will ensure management interface accounts that are not used are assigned passwords according to guidelines as defined in Appendix C, CJCSM and DISA Computing Services Security Handbook References, and then disabled.*

- (NET1370: CAT II) *The NSO will ensure that each management account is assigned a unique individual password.*

- (NET1370: CAT II) *The NSO will ensure that the network management/maintenance sections of the switch/hub will be password protected for both viewing and modification.*

The initial passwords assigned by the switch/hub manufacturer will be changed by the network administrator in accordance with the procedures as outlined in *Appendix C, CJCSM and DISA Computing Services Security Handbook References*.

3.10.2 Virtual Local Area Networks (VLANs)

VLAN technology is an efficient way of grouping users into workgroups to share the same network address space regardless of their physical location on the network. Users can be organized into separate VLANs according to their department, location, function, application,

physical address, logical address, or protocol. Regardless of organization method used, the goal with any VLAN is to group users into separate communities that share the same resources; thereby, enabling the majority of their traffic to stay within the boundaries of the VLAN.

Network nodes of the same VLAN can communicate with other nodes in the same VLAN using layer-2 switching. In order to communicate with other VLANs, the nodes in one VLAN need to go through a layer 3 device. Broadcast frames are switched only between nodes within the same VLAN. This logical separation of users and traffic results in better performance management (i.e., broadcast and bandwidth utilization control) as well as a reduction in configuration management overhead enabling networks to scale at ease.

There can be several VLANs defined on a single switch, while on the other hand a VLAN can span across multiple switches. VLAN spanning is enabled by trunked links connecting the switches and frame tagging such as IEEE 802.1q or Cisco's Inter-Switch Link (ISL) protocol. Trunk links can carry the traffic of multiple VLANs simultaneously. Therein lies a potential security exposure. Trunk links have a native or default VLAN that is used to negotiate trunk status and exchange VLAN configuration information. Trunking also enables a single port to become part of multiple VLANs—another potential security exposure. Within the switch fabric, switches use frame tagging to direct frames to the appropriate switch and port. Frame tagging assigns a VLAN ID to each frame prior to traversing a trunked link. Each switch the frame traverses must identify the VLAN ID and then determine what to do with the frame based on its filter table. Once the frame reaches the exit to the access link, the VLAN ID is removed and the end device receives the frame. The frame tagging is another technology that can be exploited as a result of a poor VLAN implementation design.

As briefly noted above, despite the benefits of the VLAN architecture to simplify network maintenance and improve performance, there are security issues that need to be addressed. The two major areas of exploitation is the use of VLAN1 and VLAN "hopping".

In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly. Best practices for VLAN-based networks is create a dedicated management VLAN, prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

VLAN "hopping" occurs when a tagged frame destined for one VLAN is redirected to a different VLAN, threatening network security. The redirection can be initiated using two methods: "tagging attack" and "double encapsulation". Frame tagging attacks allow a malicious user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port's trunk mode were configured as *auto* (enables a port to become a trunk if the connected switch it is negotiating trunking with has its state set to *on* or *desirable*) and were to receive a fake DTP packet specifying *trunk on* or *desirable*, it would become a trunk port and it could then start

accepting traffic destined for all VLANs that belong to that trunk group. The attacker could start communicating with other VLANs through that compromised port. Insuring that trunk mode for any non-trunking port is configured as *off* can prevent this type of attack.

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port. To insure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

An additional security best practice in a VLAN-based network is to place all disabled ports into an unused VLAN; thereby thwarting unauthorized access using both physical and logical barriers.

- (NET1375: CAT II) *Do not use VLAN 1 for in-band management traffic. Assign a dedicated management VLAN to keep management traffic separate from user data and network device protocol traffic.*

- (NET1375: CAT II) *Do not configure the management VLAN on any trunk or access port that doesn't require it.*

- (NET1376: CAT II) *Do not use VLAN 1 for user VLANs.*

- (NET1377: CAT III) *Prune VLAN 1 from all trunk and access ports that do not require it.*

- (NET1378: CAT II) *Disable trunking on all access ports (do not configure trunk on, desirable, nonegotiate, or auto—only off).*

- (NET1378: CAT II) *When trunking is necessary, a dedicated VLAN must be configured*.

- (NET1379: CAT III) *To further reduce the risk of unauthorized access, disabled ports should be placed in an unused VLAN (do not use VLAN1).*

4. REMOTE ACCESS

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. This section sets the security guidance applicable to all remote access communications methods and access levels. This guidance will be adhered to, in addition to the requirements set forth in the individual sections that provide detailed security requirements for remote access.

4.1 Levels 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.

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 Telnet or TN3270, which accesses 3270 and 5250 based applications over TCP/IP, 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 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.

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. 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.

To ensure security within a classified environment, strict controls must be in place prior to any remote access to the classified network or resource. NSA, DISA, and the DOD have stringent policies on the access, storage, location, and containment of all classified data and processing. Furthermore, it is prohibited to allow non-DoD personnel to obtain remote access capability to any DoD network.

- (NET1380: CAT III) *For End-User access, the IAO will limit the use of clear text Telnet, TN3270, and other terminal emulator TCP/IP sessions and should employ encryption to the fullest extent possible. The site should devise a plan to eliminate the use of clear text sessions and move to an encrypted form of communication.*

- (NET1400: CAT I) *The ISSO will ensure that an NSA Certified remote access security solution such as the Remote Access Secure Program (RASP) 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 secure solution will support Key Exchange Algorithm (KEA).*
  - *The secure solution will support Palladium Fortezza Modems.*
  - *Each modem will have a valid X.509 V1 Certificate issued.*
  - *The Fortezza card will be kept in the user's possession at all times or stored in accordance with policy applicable to classified storage.*
  - *The modem will be stored separately from the computer when not in use.*

4.2 Remote Access Agreement

This Secure Remote Computing 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 (See Appendix C of the Secure Remote Computing STIG, Checklist Example, for a security checklist example). This is to inform and remind the user of the potential security risks inherent with remote access methods.

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 site's network that the user is accessing regardless of the location from which they are establishing a connection.

Site Responsibilities

- (NET1410: CAT III) *The IAM will develop a computer security checklist to be completed and signed by the remote user.*

- (NET1415: CAT II) *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.*

Remote User Responsibilities:

Remote user responsibilities are outlined in the Secure Remote Computing STIG.

4.3 Authentication, Authorization, and Accounting (AAA)

An Authentication, Authorization, and Accounting (AAA) server manages user requests for access to 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.

A shared secret key that is never sent over the network authenticates all communications between a RADIUS client and server. 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. 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.

Note: 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 was riddled with Year-2000 bugs and has been largely succeeded by Novell Directory Services (NDS).

Originally described in RFC 1492, TACACS has been reengineered over the years by Cisco and is supported on many routers and network access servers found in enterprise networks today. TACACS+ has many enhancements made to the original TACACS and Extended TACACS

(XTACACS). 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.
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.

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)

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.

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.

- (NET1418: CAT II) *The NSO will ensure that 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.

- (NET1418: CAT II) *The NSO will ensure that NetWare Bindery is not used by a RADIUS server to authenticate remote users accessing a Novell network.*

- (NET1420: CAT II) *The NSO will ensure that all remote users are required to use a form of two-factor authentication to access any network resource.*

- (NET1425: CAT III) *The NSO will ensure that the remote access infrastructure (i.e. authentication server, RAS/NAS device, VPN gateway) will log session connectivity and termination, userid, assigned IP address, and success or failure of all session events.*

- (NET1430: CAT III) *The NSO will ensure that 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.*

- (NET1435: CAT III) *The NSO will ensure that 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.*

- (NET1435: CAT III *The NSO will ensure that the 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.*

- (NET1435: CAT III *The NSO will ensure that the audit logs are viewed on a daily basis and set to alarm or notify the administrator of moderate to severe security events that may be detected.*

4.4 Dial-up Communications

Using either PSTN (public switched telephone network) or ISDN (Integrated Services Digital Network) lines, dial-up remote access is still one of the most cost effective and flexible solutions available today. With boosts in data throughput through increases in modem speeds and gains in data compression algorithms, as well as effective resource sharing though modem pooling, there are a number of applications that are well suited for dial-up communications. This section will focus on opportunities along with the risks associated with the dial-in remote access application that can be implemented within a site's network infrastructure enabling personnel at remote locations to gain access to its resources.

4.4.1 Modems

Implementing a dial-up technology—whether dialing out or dialing in—introduces additional security concerns for the network infrastructure. Each modem is a potential gateway for uninvited users, either by chance or malicious intent, to gain access to the attached network. Modems can provide an unchecked gateway to sensitive data within the DOD's computing

boundaries. Keeping accurate records of all authorized modems used for both dial-in and dial-out is a good practice that promotes sound configuration management and an awareness of all network access points. Workstations with modems present a possible backdoor into a computer network. Configuring workstations to insure that their modems will operate only when the Network Interface Card (NIC) is disabled will help to mitigate the associated risk.

- (NET1460: CAT III) *The NSO will ensure all infrastructure modems are physically protected to prevent unauthorized device changes. If an unauthorized person has physical access to a site's modems, the settings can be changed to affect the security of a system.*

- (NET1460: CAT III) *The NSO will maintain a listing of all modems by model number, associated phone number, and location. Only Government-authorized modems will be installed at DOD sites.*

- (NET1470: CAT III) *The NSO will ensure that all modem phone lines will be restricted to single-line operation and configured to their mission required purpose (inward dial only or outward dial only) without any special features (e.g., call forwarding).*

4.4.2 Remote Access Server/Network Access Server

A Remote Access Server (RAS) or 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 Kbps. 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.

Callback features are an attempt to protect the network by providing a service that disconnects an incoming call and reestablishes the call, dialing back to a predetermined number. Upon establishment of the callback connection, the communications device will require the user to authenticate to the system.

Configuring a focal point of access is vital to the overall security of a remote access infrastructure. In addition, only services that are absolutely needed for end users to conduct business should be allowed through the firewall from this access point. Hence, a sound approach would be to place dial-in users under the same access policy as those connecting via VPN. This can easily 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 network while still providing protection for the remote access server.

- (NET1530: CAT III) *The NSO will use the communications server's Automatic Number Identification (ANI) option, if available, to verify users' phone numbers. The NSO, or authorized security personnel, will maintain ANI logs in a manner prescribed by the IAO, to provide a call audit trail. This information, maintained by those responsible for the operation of the site's telephone equipment, will be compared against the stored directory information in the PBX or telephone directory listings, to verify the callers' authenticity.*

- (NET1535: CAT III) *The Network Administrator (NA) will ensure that if callback procedures are used, upon establishment of the callback connection, the communications device will require the user to authenticate to the system.*

- (NET1540: CAT II) *The NSO will ensure that remote access server cards will not be used to provide remote access services unless they have the ability to support authentication servers.*

- (NET1550: CAT II) *The NSO will ensure that remote access server cards will not be installed and implemented on any Windows domain controller.*

- (NET1590: CAT II) *The NSO will ensure the RAS/ NAS device is not configured to utilize any services or capabilities that are not required to support the server or remote access.*

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

- (NET1600: CAT II) *The NSO will ensure that all methods used to manage and access the RAS/NAS device complies with those requirements outlined in section 3.4.2 Device Management.*

4.4.3 Dial-in Connectivity: SLIP and PPP

Serial Line Internet Protocol (SLIP) and 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 using a modem. 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 MTU (maximum transmission unit) and MRU (maximum receive unit). 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 PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), 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 (Digital Encryption Standard (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 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 that 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 that CHAP with MD5 or MS-CHAP with MD4 encryption is used to authenticate the remote client.*

4.5 Remote Client to VPN Gateway

DoD activities can out-source dial-up access to their networks using a cost-effective, easy to implement, and protocol-independent solution that requires minimal changes their network architecture and policy. As discussed in section 5.2, a VPN is a network secured by encryption and authentication and is layered on existing public networks such as the Internet. A remote client uses the Internet and NIPRNet as the backbone for VPN connectivity to a DoD local area network. There are three tunneling protocols that can be used to create connectivity between a remote client and a VPN gateway: Point-to-Point-Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec. The later being the most secured and the required method for VPN connectivity between a remote client and a DoD network.

PPTP is Microsoft‘s solution for remote access VPN using RSA RC4 encryption and CHAP or MS-CHAP authentication. Both encryption and authentication are done within PPP. The PPP packets are then encapsulated within IP packets to create the tunnel. PPTP uses an enhanced Generic Routing Encapsulation (GRE) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets within IP. With PPTP, a remote user makes a dialup connection to an ISP NAS. The ISP provides a connection through its WAN and the Internet to a PPTP server residing in a DoD LAN. All encryption is done on the PPTP client and the decryption is done on the PPTP server creating a secured tunnel between the PPTP client and the PPTP server. The NAS can act as a PPTP client if the remote client is not PPTP aware; thereby, only providing a PPP session between the remote client and the NAS device at the ISP point of presence. For the obvious reason, the most secured implementation is to use a PPTP-enabled remote client to insure that there is a secured tunnel between the remote client and the DoD LAN.

Based on Microsoft‘s PPTP and Cisco’s Layer 2 Forwarding Protocol (L2F), an L2TP VPN implementation model is similar to PPTP with one major difference—there is no encryption of the PPP packets so it must depend on IPSec or some other technology for encryption. Authentication is performed within PPP using PAP, CHAP, or Extensible Authentication Protocol (EAP).

IPSec provides two main facilities for creating VPN connections: an authentication-only function referred to as an Authentication Header (AH) and a combined authentication/encryption function called Encapsulating Security Payload (ESP) which can operate either in transport mode or tunnel mode.

In transport mode, IPSec encrypts only the data component of the IP packet to be transported: application headers, TCP/UDP headers and data are encrypted, the IP headers are readable. The

authentication data is calculated on the basis of values in the IP header (and some other things). The original IP header is therefore maintained and an additional IPSec header is appended. The advantage of this mode of operation is that only a few bytes are added to each packet. On the other hand, it is possible for attackers to analyse the data traffic in VPN, since the the IP headers are not modified. The data itself however is encrypted, so one can only determine how much data is being exchanged by which stations, but not what data.

In tunnel mode, the entire IP packet is encrypted and provided with a new IP header and IPSec header. The advantage lies in that, in those LANs that should be connected to a VPN, a gateway can be configured such that it accepts IP packets, changes them into IPSec packets and then sends them over the Internet to the gateway on the target network, which restores and forwards the original packet. Moreover, attackers can thereby only determine the start- and end point of an IPSec tunnel.

- (NET1620: CAT I) *With the exception of direct dial-in to the LAN, the NSO will ensure that all remote user access will be via VPN.*

- (NET1625: CAT II) *The NSO will ensure that VPN gateways terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).*

- (NET1630: CAT II) *The NSO will ensure that remote access via VPN will use IPSec ESP in tunnel mode. For legacy support, L2TP may be used if encryption is provided by IPSec or another technology that utilizes at a minimum a FIPS 140-2 approved data encryption algorithm such as AES or 3DES.*

- (NET1635: CAT II) *The NSO will ensure that all VPN implementations adhere to Section 5.2.1, VPN, in the Network Infrastructure STIG.*

This page is intentionally left blank.

5. NETWORK MANAGEMENT AND SUPPORT SERVICES

5.1 NETWORK MANAGEMENT

Managing a network with automated tools is becoming a necessity as networks become more complex. These automated processes can be used to monitor network performance and activity as well as to provide reports about the network. Network management models are built around network elements and are configured to monitor the attributes and functions associated with them. A network management configuration generally involves a managing process that runs on a management workstation. The managing process collects performance and other relevant data about the network or about particular nodes on the network.

Network management is generally implemented as a high-level application, so that the management software uses well-established protocol suites, such as the TCP/IP and the seven-layer OSI Reference Model, to move its information around.

5.1.1 The IP Management Model

The major components within the TCP/IP based model are Structure of Management Information (SMI), Management Information Base (MIB), and SNMP. The SMI specifies how information about managed objects is to be represented. The MIB contains the definitions and values for the managed objects relevant to a particular network. The information for the MIB component is acquired and updated by a management agent, a program whose task is to determine and report the information desired by a management program. Continued expansion of a generic MIB has been abandoned in favor of a scheme that allows extensions for specific networking products to be defined as separate nodes. SNMP is the protocol used to transmit management information.

5.1.2 Network Management Security Implications

This document focuses on the IP management service. SNMP, by virtue of what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device parameters, unauthorized users can cause damage rather easily.

SNMP has three basic commands that can supply potentially network-damaging information to individuals:

- ***GET*** *For MIB variable polling, used by the management station to create threshold alarms, provide system settings, and show other device information.*

- ***SET*** *For altering a variable's value from the management station, possibly triggering an intended side effect such as causing the managed device to reset a counter or to reboot.*

- ***TRAP*** *For agents to asynchronously notify the management station of a significant event, such as a change in the availability status of a communication link.*

SNMPv2 and later releases support the use of Message-Digest 5 (MD5) protocol to ensure sender authenticity and message integrity by creating a hash value of the Protocol Data Unit (PDU). It can also incorporate a time stamp to avoid possible replay attacks. To achieve confidentiality of the PDU transmission, SNMPv2 and later uses Symmetric Privacy Protocol, which currently calls for the messages to be encrypted using the Digital Encryption Standard (DES). The communicating SNMP devices know the same symmetric DES key and can communicate freely across the network.

A would-be attacker can send SNMP GET sequences to routers, bridges, printers, or other devices polling for information. This individual could flood a particular device with so many GETs that all the processing time is used up, causing a denial of service. Using the TRAP, an unauthorized user could send an erroneous PDU to the router signaling that a circuit is down, thus causing packets to be rerouted or not delivered. A router's table or ACL could be overwritten by the **SET** command, allowing an unauthorized workstation access past the ACL router. On hosts using SNMP to communicate with the management station, commands can be sent to change an ARP cache table or even reboot the machine.

- (NET1650: CAT II) *The NSO will ensure IPSec is used to secure traffic between the network management workstation on DISA-managed LANs and all monitored devices sent via the Internet, NIPRNet, SIPRNet, or other external network.*

- (NET1660: CAT I) *The NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) will be used across the entire network infrastructure.*

  CAVEAT: If the site is using Version 1 or Version 2 with all of the appropriate patches to mitigate the known security vulnerabilities, this finding can be downgraded to a Category II. If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category III.

- (NET1665: CAT I) *The NSO will ensure that all SNMP community strings are changed from the default public values of public and private. Community names or usernames will not match any other password value on any other network device. They will be protected in the same way as any password is protected and will subscribe to the password standards as defined in Appendix C, CJCSM and DISA Computing Services Security Handbook References.*

- (NET1670: CAT III) *The IAO will establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:*

  - *Community string and username expiration period.*
  - *Community string and username creation will comply with the password requirements outlined in Appendix C, CJCSM and DISA Computing Services Security Handbook References.*
  - *SNMP community string and username distribution including determination of membership*

- (NET1675: CAT II) *The NSO will ensure that both privileged and non-privileged modes are used on all devices. Different community names will be used for* ***read-only*** *access and* ***read-write*** *access.*

- (NET1680: CAT II) *The NSO will ensure a list of specific IP addresses allowed to send messages to the network management system (NMS) is specified.*

- (NET1710: CAT III) *The NSO will ensure that security alarms are set up within the managed network's framework. At a minimum, these will include the following:*

  - ***Integrity Violation:*** *Indicates that network contents or objects have been illegally modified, deleted, or added.*

  - ***Operational Violation:*** *Indicates that a desired object or service could not be used.*

  - ***Physical Violation:*** *Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.*

  - ***Security Mechanism Violation:*** *Indicates that the network's security system has been compromised or breached.*

  - ***Time Domain Violation:*** *Indicates that an event has happened outside its allowed or typical time slot.*

- (NET1720: CAT III) *The NSO will ensure that alarms will be categorized by severity using the following guidelines:*

  - ***Critical*** *and* ***major*** *alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.*

  - *A* ***major*** *alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.*

- *A **minor** alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.*

- *A **warning** alarm is used to signal a potential problem that may affect service.*

- *An **indeterminate** alarm is one that requires human intervention to decide its severity.*

5.1.3 Network Management Station

At the center of the network management structure is the management station. Applications such as HP's OpenView and Cabletron's Spectrum provide the user interface to the various levels of network management mentioned above. All facets of the management umbrella are controlled from here. It is extremely important that this workstation be protected as follows:

- (NET1730: CAT II) *The NSO will ensure that the management workstation is located in a secure environment.*

- (NET1740: CAT II) *The NSO will ensure that only those accounts necessary for the operation of the system and for access logging will be maintained.*

- (NET1750: CAT III) *The NSO will ensure a record is maintained of all logons and transactions processed by the management station. Include time logged in and out, devices that were accessed and modified, and other activities performed.*

- (NET1760: CAT I) *Access to NMS will be restricted to authorized users with appropriate userids and passwords. Encryption will be used for passwords and entire network management sessions (e.g., system encryption or SSH client).*

- (NET1770: CAT II) *The NSO will ensure connections to the NMS are restricted by IP Address to only the authorized devices being monitored.*

- (NET1780: CAT II) *The NSO will ensure all accounts will be assigned the lowest possible level of access/rights necessary to perform their jobs.*

- (NET1780: CAT II) *The NSO will ensure default passwords will be changed at initial configuration, prior to being deployed, and will comply with the password standards as outlined in Appendix C, CJCSM and DISA Computing Services Security Handbook References.*

5.2 Virtual Private Networks (VPNs)

5.2.1 Site-to-site VPN

A Virtual Private Network (VPN) is a distributed collection of networks or systems that are interconnected via a public and/or private network (i.e., the Internet or the NIPRNet) but protect their communications using encryption. In effect, a VPN is a private secure distributed network that is *transported* or *tunneled* across a public and/or private network. 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.

- (NET1800: CAT II) *The NSO will ensure VPNs are established as tunnel type VPNs, which terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router). The placement of the VPN is to maintain the security of the enclave and the requirement that all traffic must pass through the Enclave Security Architecture. This is not to say that encrypted data (e.g., SSL, SSH, TSL) that entered the VPN tunnel must also be unencrypted prior to leaving the tunnel. However, the data would still have to pass through the respective application proxy on the firewall. If a host-to-host VPN is required, it will be established between trusted known hosts.*

  Note: A DOD site that enters into an agreement to establish a VPN with an outside security enclave/domain will retain administrative oversight and control privileges on the IPSEC/VPN device within their security enclave.

- (NET1810: CAT III) *The IAM will ensure that the site retains administrative oversight and control privileges on the IPSEC/VPN device within their security enclave.*

- (NET1820: CAT II) *The IAM will require the customer to provide an Intrusion Detection System (IDS) capability for any VPN established that bypasses the site's current IDS capability.*

A VPN solution can be cheaper than conventional networks that run over WAN connections. VPN devices and software provide not only encryption functions but also network access control to secure Internet tunnels between remote sites. A VPN must provide privacy and integrity of data as it traverses the public network. At a minimum it should provide for the following:

- **User Authentication** — The solution must verify a user's identity and restrict VPN access to authorized users. In addition, the solution must provide audit and accounting records that reflect who, what, and when information was accessed.

- **Address Management** — The solution must assign a client's address on the private net, and must ensure that private addresses are kept private.

- **Data Encryption** — Data carried on the public network must be rendered unreadable to unauthorized users on the network. The VPN solution must also generate and refresh encryption keys for the client and server.

5.2.2 Contractor-to-Company Site VPN

Contractors working at DOD locations that require the ability to connect to their company network, using client-side VPN software installed on their government machine, will adhere to the following guidance:

- (NET1840: CAT III) *The remote user will enter into a written agreement with the DOD site that will allow the site to maintain administrative oversight and control privileges of the computer.*

- (NET1840: CAT III) *The SA and the NSO will ensure that 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.*

- (NET1840: CAT III) *The remote user will ensure the computer will be secured in accordance with the appropriate operating system STIG.*

- (NET1840: CAT III) *The remote user will ensure virus protection software is installed on the system with the latest anti-virus engine and signature updates.*

- (NET1840: CAT III) *The remote user will employ a DOD-CERT approved personal firewall on the system that is used to access the site network.*

- (NET1840: CAT III) *The remote user will ensure all communication to/from the site network will employ at a minimum a FIPS-140-2 approved encryption algorithm (i.e., 3DES, AES).*

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense (DOD) Directive 8500.1, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

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

Department of Defense CSC-STD-002-85, "DOD Password Management Guideline," 12 April 1985.

Department of Defense CM-400-260-01, “Software Requirements Specification (SRS) for the Network Management (NM) Functional Area Of The Defense Information Infrastructure (DII),” 8 July 1997.

DOD Directive Number 3020.26, Continuity of Operations (COOP) Policy and Planning, May 26, 1995.

DOD Instruction Number 3020.39, Integrated Continuity Planning for Defense Intelligence, ASD (C3I), August 3, 2001.

DOD Directive Number O-8530.1, Computer Network Defense (CND), January 8,2001.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991, and Supplements 1 and 2, not dated.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

National Security Agency (NSA), “Router Security Configuration Guide” (Current Edition)

ASD (NII) Memo, “Internet Protocol Version 6” (IPv6), June 9, 2003.

Field Security Operations Publications

DISA Computing Services Security Handbook
DNS STIG
NIPRNet STIG
Secure Remote Computing STIG
STIG on Enclave Security
UNIX STIG
Web Application STIG
WIRELESS STIG

Commercial and Other Publications

William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security, Repelling the Wily Hacker. Addison-Wesley Publishing Company, 1994.

J. Reynolds, and J. Postel, Assigned Numbers, RFC 1700, October 1994.

World-Wide Web References

Network Information Center (NIC) - http://www.internic.net

Electronic Industry Association/ Telecommunications Industry Association (EIA/TIA) - http://www.eia.org

Global Engineering Documents - http://global.ihs.com

TN3270 Server For Channel Interface Processor (CIP)- http://www.cisco.com

Role of Backbone Solutions - http://www.cisco.com

Advanced Peer-to-Peer Networking - http://www.cisco.com

Cisco Channel Interface Processor - http://www.cisco.com

Cisco Field Notices - http://www.cisco.com/warp/public/770/index.shtml

Cisco Security Advisories - http://www.cisco.com/warp/public/707/advisory.html

Cisco White Papers Website - http://www.cisco.com/warp/public/126/index.shtml

CERT Coordination Center - http://www.cert.org

CERT Alerts (from 1988) - http://www.cert.org/nav/alerts.html

DOD-CERT Home Page - http://www.cert.mil

NIPRNet Connection Approval Process - http://cap.nipr.mil

APPENDIX B. LIST OF ACRONYMS

AAA Authentication, Authorization, and Accounting
ACL Access Control List
ARP Address Resolution Protocol
ATM Asynchronous Transfer Mode

BGP Border Gateway Protocol
BIND Berkeley Internet Name Domain
BOOTP Boot Protocol

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)
CJCSM Chairman Joint Chiefs of Staff Manual
COOP Continuity Of Operations
CS Communication Server

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
DMZ Demilitarized Zone
DNS Domain Name Service
DOD Department of Defense
DOD-CERT Department of Defense-Computer Emergency Response Team

EAL Evaluated Assurance Level
EIA/TIA Electronic Industry Association/Telecommunications Industry Association
EIGRP Enhanced Interior Gateway Routing Protocol

FA Firewall Administrator
FDDI Fiber Distributed Data Interface

FIPS Federal Information Processing Standard
FTP File Transfer Protocol
FSO Field Security Office
FSO Field Security Operations

GD General Deployment
GIG Global Information Grid
GNOSC Global Network Operations and Security Center

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
IDS Intrusion Detection System
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
IS-IS Intermediate System to Intermediate System
IAM Information Assurance Manager
IAO Information Assurance 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

MD5 Message-Digest Five Algorithm
MIB Management Information Base

NA Network Administrator
NAT Network Address Translator
NIC Network Information Center
NID/JID Network Intrusion Detector/Joint Intrusion Detector
NIPRNet Non-classified (but Sensitive) Internet Protocol Routing Network
NMS Network Management System
NSA National Security Agency
NSO Network Security Officer
NTP Network Time Protocol

OS Operating System
OSI Open Systems Interconnection
OSPF Open Shortest Path First

PKI Public Key Infrastructure
POC Point-of-Contact
POP Point-of-Presence
PPP Point-to-Point Protocol
PR Perimeter Router or Premise Router

RA Registration Authority
RADIUS Remote Authentication Dial-in User Service
RCERT Regional Computer Emergency Response Team
RFC Request for Comments
RIP Routing Information Protocol
RNOSC Regional Network Operations and Security Center (formerly ROSC)
RPC Remote Procedure Call

SA System Administrator
SHTTP Secure Hyper Text Transfer Protocol
SIPRNet Secret Internet Protocol Router Network
SLA Service Level Agreement
SLIP Serial Line Interface Protocol
SMTP Simple Mail Transfer Protocol
SNA System Network Architecture
SNMP Simple Network Management Protocol
SOP Standard Operating Procedure
SSAA System Security Authorization Agreement
SSH Secure Shell
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
TTY Teletype
TSIG Transaction Signatures

UDP User Datagram Protocol

VCTS Vulnerability Compliance Tracking System
VMS Vulnerability Management System
VLAN Virtual LAN
VTY Virtual Teletype/Terminal

WAN Wide Area Network
WESTHEM Western Hemisphere
WWW World Wide Web

APPENDIX C. CJCSM AND DISA Computing Services SECURITY HANDBOOK REFERENCES

The references below are excerpts from *CJCSM 6510.01* and the *DISA Computing Services Security Handbook,* and are provided for the convenience of the readers/users of this STIG.

- The following is an excerpt from *Section 3.13, Passwords*, in the *Handbook*. The excerpt is provided as an adjunct to *DISA Computing Services Security Handbook* references.

3.13 Passwords

1. General.

a. Passwords provide the identification and authentication (I&A) function required of a C2 trusted level system. However, passwords become a vulnerability rather than a protection if misused or poorly maintained.

b. Ideally, only the user and the system know a password. The IAO will issue a temporary password that the user will change on initial access to the system. Temporary passwords will meet password structure requirements and will be varied. If a user forgets a password, the IAO will have to delete the existing account and reissue a new temporary password.

c. Users must sign a receipt for their initial password. The receipt must contain an acknowledgment that the user understands the responsibility to protect the password and has received guidance on password selection (if user selected). Password receipts must be kept on file for as long as a user has access. The receipt can be combined with access request forms. This requirement is now fulfilled with the DISA Form 41. These forms do not need to be stored at the DECC/Dets. It is recommended that they be filed at the local IAO level.

2. Password Structure.

a. Passwords will generally be a minimum of eight characters. The pertinent STIG will be consulted for the requirement of each operating system.

b. No words found in standard dictionaries will be used.

c. At least one upper case letter, lower case letter, numeric, and special character will be used.

d. Repeating, consecutive characters will not be used.

3. Password Maintenance. The following are minimum standards. Refer to the appropriate STIG for standards specific to the operating system.

a. Passwords must be changed every 90 days.

b. Passwords cannot be reused within 10 password changes.

c. Passwords cannot be changed more than once every 24 hours without the intervention of the IAO.

d. If software allows, set it to enforce the above rules.

e. The password file must be encrypted, if possible, and protected from unauthorized access.

4. Password Classification.

a. Passwords for unclassified but sensitive systems will be marked, "**FOR OFFICIAL USE ONLY**."

b. Passwords for classified systems, operating in the dedicated or systems high mode, will be marked, "**FOR OFFICIAL USE ONLY**."

c. Passwords for classified systems, operating in the multi-level mode, depend on what other security measures are in place. If physical security or COMSEC measures separate the levels of classification, the passwords may be marked, "**FOR OFFICIAL USE ONLY**." However, if the password is the only measure separating the levels of classification, the password must be classified to the level of that user.

5. Password Storage.

a. If it is necessary to maintain a password list, it must be kept under key lock. *Although a list of all passwords for a classified system is FOUO, it is recommended the list be stored as classified.*

b. Users are encouraged not to keep a copy of their written password, but it is often necessary to have it available. It should be protected as follows to prevent loss and to detect a compromise.

(1) Do not store the password where it is easily accessible to your computer.

(2) Do not keep the password and user ID together.

(3) Store the password in a locked drawer or cabinet. However, this is not effective if the same key opens most of the drawers in the office area.

(4) Keep the password in your wallet.

(5) Seal the password in an envelope and sign across the seal to detect tampering.

6. Password Dissemination.

a. Passwords must be given to the user via a secure means. The user ID and password should never be transmitted, together in the clear. There is no one solution, but many possible alternatives. A risk management approach should be used and the less secure the means, the less time the password should remain active before the change. If the user is not able to change passwords, the most secure methods should be employed.

b. The ideal situation would involve the IAO personally giving the user their initial, one-time password and the user immediately changing that password.

c. Other acceptable solutions include:

(1) Sending the user ID and password by mail.

(2) Giving the user ID and password over a secure phone.

(3) Sending the user ID and password by an encrypted E-mail. The password to unencrypt will be sent by a separate message, without referencing what this password is for.

(4) Centrally managed system may predetermine default password, such as the password of the week or a list of 25 different passwords. These can be mailed to local IAOs ahead of time. When an account is established centrally, the local IAO will be notified that the password for the week of the 17th was used or password #12. The local IAO can then personally give the user their one-time password.

d. Other methods of disseminating passwords should be submitted to FSO for approval.

7. Password Vaults.

a. A password vault is a utility program that stores multiple passwords under a master password. This eliminates the problem of users forgetting multiple passwords or having to write them down.

b. The use of a password vault will only be considered if:

(1) Passwords are stored by a minimum of 128-bit encryption.

(2) The vendor provides a Vendor Integrity Statement. *See Section 3.23.*

(3) The IAO or IAM approves the software and use of this product is reflected in the accreditation.

3.26 CJCSM Warning Banners

1. The purpose of the warning banner is two-fold. First, it warns unauthorized users, surfing the net, that unless they are authorized they should not proceed. It is like an electronic **No Trespassing** sign that allows us to prosecute those who do trespass. Secondly, it warns both authorized and unauthorized users that they are subject to monitoring to detect unauthorized use. This provides the informed consent that again allows us to prosecute those who abuse the system.

2. The requirement for a LOGON Warning Banner was disseminated through DOD-CERT Bulletin 93-17, subject: LOGON Warning Banner for DOD Interest Computer Systems. The bulletin referenced guidance from the Deputy Assistant Secretary of Defense for Security Countermeasures and Counterintelligence (DASD/SCM/CI). Other clarifying guidance has also been distributed.

3. The banner should be installed so that it appears before a LOGON screen or before any identification of the system. An escape should also be provided to allow the individual to end the LOGON attempt (e.g., **PRESS ENTER TO LOG ON TO SYSTEM OR ESCAPE TO ABORT SESSION**). If the banner cannot be installed before the LOGON process due to the configuration of the system, install the banner as soon as possible.

4. Below is the latest version of the warning banner provided by CJCSM 6510.01 dated 15 March 2002. Previously approved versions are acceptable, but should be updated when possible.

> This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including internet access), are provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system, may be monitored.
>
> Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

APPENDIX D. DOD-CERT INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM)

The DOD-CERT publishes computer security vulnerability Alerts, Bulletins, and Technical Advisories of interest to the site community on as needed basis. The DOD-CERT vulnerability notifications that are of general interest to the network or at least partially applicable are listed below. The severity of the vulnerability is categorized as follows:

- Vulnerability Alerts (high – pose an immediate potentially severe threat)
- Vulnerability Bulletins (medium – significant enough that non-compliance could escalate a threat)
- Technical Advisories (low – if there is any risk in escalation it can be mitigated)

The subsequent list is current as of the date of publication of this document. However, the list will become obsolete upon publication of the next DOD-CERT vulnerability notification. It is strongly recommended that each IAO regularly browse the DOD-CERT web page (http://www.cert.mil) and update the current list. It should be noted that the listing and text of DOD-CERT vulnerability notifications are not accessible from a workstation unless its IP address is in the **.mil** domain. The DOD-CERT will, however, distribute the information to members of a mailing list. The registration instructions for this mailing list are on the DOD-CERT web page.

Information Assurance Vulnerability Alerts:

2002-A-snmp-006	Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications
2002-A-snmp-005(1)	Multiple Simple Network Management Protocol Vulnerabilities in Enclaves Devices
2002-A-snmp-004(1)	Multiple Simple Network Management Protocol Vulnerabilities in Perimeter Devices
2002-A-snmp-003(1)	Multiple SNMP Vulnerabilities in Servers and Applications
2002-A-snmp-002	Multiple SNMP Vulnerabilities in Enclaves and Devices
2002-A-snmp-001	Multiple SNMP Vulnerabilities in Devices
2002-A-0004	Multiple Vulnerabilities in OpenSSL
2001-A-0013(1)	SSH CRC32 Remote Integer Overflow Vulnerability
2001-A-0009(1)	Gauntlet Firewall for UNIX and WebShield CSMAP and smap/smapd Buffer Overflow Vulnerability
2001-A-0003(1)	Sun Solaris SNMP to DMI Mapper Daemon Vulnerability
2001-A-0001(2)	Buffer Overflows in Multiple Versions of BIND
2000-A-0003	Gauntlet Firewall for UNIX and WebShield Cyberdaemon Buffer Overflow Vulnerability
98-09	Vulnerabilities in CISCO Routers
98-03	Multiple Vulnerabilities in BIND

Information Assurance Vulnerability Bulletins:

2002-B-SNMP-001	Multiple Simple Network Management Protocol Vulnerabilities in Enclaves Devices
2001-B-0003	%U Encoding Intrusion Detection System Bypass Vulnerability
2001-B-0002	Vulnerability in HP Openview and IBM Tivoli NetView
2001-B-0001(1)	CISCO SNMP Read-Write ILMI Community String Vulnerability
2000-B-0008	BIND 8.2.2 P Denial of Service Vulnerabilities
2000-B-0003	Multiple Buffer Overflows in Kerberos Authenticated Services
2000-B-0001	BIND NXT Buffer Overflow

Information Assurance Technical Advisories:

2003-T-0005	Cisco IOS EIGRP Announcement ARP Denial Of Service Vulnerability
2003-T-0010	Cisco Catalyst CatOS Authentication Bypass Vulnerability
2003-T-0011	Various Vulnerabilities in Cisco VPN 3000 Concentrators
2003-T-0001	Multiple Vendor SSHv2 Vulnerability
2003-T-0005	Cisco IOS EIGRP Announcement ARP Denial of Service Vulnerability
2002-T-snmp-003	Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications
2002-T-snmp-002	Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications
2002-T-snmp-001	Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications
2002-T-0014	Cisco Trivial File Transfer Protocol (TFTP) Long Filename Vulnerability
2002-T-0011	OpenSSH Vulnerabilities in Challenge Response Handling
2002-T-0010	Denial of Service Vulnerability in ISC-BIND 9
2002-T-0004	Kerberos Telnet Protocol Vulnerability
2002-T-0002	Multiple Vulnerabilities in CISCO SN 5420 Storage Routers
2001-T-0018	Short Password Vulnerability in SSH Communications Security
2001-T-0017	OpenSSH UseLogin Multiple Vulnerabilities
2001-T-0011	CISCO IOS Discovery Protocol flaw
2001-T-0010	CISCO PIX Firewall Authentication DoS
2001-T-0003(1)	CISCO IOS Software TCP Initial Sequence Number Randomization Improvements
2000-T-0015.1	BMC Best/1 Version 6.3 Performance Management System Vulnerability
2000-T-0015	BMC Best/1 Version 6.3 Performance Management System Vulnerability
2000-T-0005	IP Fragment Assembly DoS Vulnerability
1999-T-0011	Fragmented IGMP Vulnerability
1999-T-0010a	ICMP Router Discovery Protocol Vulnerability
1999-T-0009	Gauntlet Firewall 5.0 DoS Vulnerability
1999-T-0002	Back Orifice 2000

The Computer Emergency Response Team (CERT)Coordination Center is part of the Networked Systems Survivability program in the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. The CERT Coordination Center studies Internet security vulnerabilities, provides incident response services to sites that have been the victims of attack, publishes a variety of security alerts, researches security and survivability in wide-area-networked computing, and develops information to help improve site security. CERT is very similar in purpose and function to the DOD-CERT organization. However, there are sufficient differences in approach to warrant that each IAO regularly browse the CERT web page (http://www.cert.org) as well as the DOD-CERT web page for additional information.

This page was intentionally left blank

APPENDIX E. REMOTE DIAGNOSTICS

Remote Diagnostics is used for maintenance and monitoring of devices. When diagnostics are needed, the device will connect to an approved remote diagnostics facility using dial home capabilities.

The purpose of this guidance is to clarify the issue of vendor diagnostics via modems/circuits as well as the security guidelines that should be utilized when using this technology.

Dial Home Diagnostics Guidelines

1. Dial-in access should be disabled. Only dial-out access should be used.

2. The connection is established via firmware to a predetermined number and only hardware operational status information is transferred to the facility.

Remote Diagnostics Guidelines

When the vendor needs access to perform remote maintenance, the following guidelines should be used:

1. When the vendor needs access, they should call the appropriate Government representative for approval.

2. If the Government representative approves the connection, the vendor is notified and the modem is configured to accept incoming connection. The system will be configured to use dial-back calling to a pre-determined number at the vendor's location.

3. If operationally feasible without further impacting user/production processing, the machine should be isolated from the network prior to initiating the connection.

4. All maintenance performed on the machine as well as configuration changes will be documented in the monthly vendor support report.

The above steps comply with the *STIG on Enclave Security* and the *Network Infrastructure STIG*.

This page was intentionally left blank.

APPENDIX F. JID GUIDANCE

DEPARTMENT OF JUSTICE LETTER ON LEGALITIES OF KEYSTROKE MONITORING

U.S. Department of Justice
Criminal Division
Office of the Assistant Attorney General
Washington, DC 20530

OCT 7 1992

Mr. James H. Burrows
Director, Computer Systems Laboratory
National Institute of Standards & Technology
U.S. Department of Commerce
B-154 Technology
Gaithersburg, Maryland 20899

Dear Mr. Burrows:

It has come to our attention that keystroke monitoring, a process whereby computer System Administrators monitor both the keystrokes entered by a computer user and the computer's response, is being conducted by government agencies in an effort to protect their computer systems from intruders who access such systems without authority. We recognize that the unauthorized use of computers, particularly the insertion into a computer system of malicious code (e.g., viruses or worms) and backdoors (programming code that allows an intruder to reenter a system even if compromised passwords are changed), poses a serious threat to the integrity of that system and that keystroke monitoring is the most feasible means to assess and to repair the damage done by such activity. However, we have reviewed the legal propriety of such monitoring for the activities of intruders and, since you are responsible for providing computer security guidance to the federal government, I wish to share our legal conclusions with you. I would also appreciate it if you would, to the extent and in the manner you deem appropriate, circulate this letter to your colleagues in the federal government who are confronted with the keystroke monitoring issue.

The legality of such monitoring is governed by 18 U.S.C. § 2510 et seq. That statute was last amended in 1986, years before the words “virus” and “worm” became a part of our everyday vocabulary. Therefore, not surprisingly, the statute does not directly address the propriety of keystroke monitoring by System Administrators.

Attorneys for the Department have engaged in a review of the statute and its legislative history. We believe that such keystroke monitoring of intruders may be defensible under the statute. However, the statute does not expressly authorize such monitoring. Moreover, no court has yet had an opportunity to rule on this issue. If the courts were to decide that such monitoring is improper, it would potentially give rise to both criminal and civil liability for System Administrators. Therefore, absent clear guidance form the courts, we believe it is advisable for System Administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to only authorized users will not be sufficient to place outside hackers on notice.

An agency's banner should give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during the effort to monitor the intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). We also understand that System Administrators may in some cases monitor authorized users in the course of routine system maintenance. If this is the case, the banner should indicate this fact. An example of an appropriate banner might be as follows:

```
This system is for the use of authorized users only.
Individuals using this computer system without
authority, or in excess of their authority, are
subject to having all of their activities on this
system monitored and recorded by system personnel.
In the course of monitoring individuals improperly
using this system, or in the course of system
maintenance, the activities of authorized users may
also be monitored.  Anyone using this system
expressly consents to such monitoring and is advised
that if such monitoring reveals possible evidence of
criminal activity, system personnel may provide the
evidence of such monitoring to law enforcement
officials.
```

Obviously, each agency may want to tailor the banner to its precise needs. In addition to giving notice to users that keystroke monitoring may occur, the System Administrator might decide that the banner should also contain a statement explaining the need for such monitoring (e.g., "To protect the system from unauthorized use and to insure that the system is functioning properly, System Administrators monitor this system.").

Lastly, we would note that the long-term monitoring of individuals using a system without authority, or in excess of their authority, should not be conducted routinely. The monitoring of such individuals should be limited to the extent reasonable and necessary to determine whether and how the system is being abused. Once that determination is made, the matter should-be reported to law enforcement for consideration as to whether court orders authorizing continued monitoring should be obtained.

In sum, we believe that each banner should be crafted by the agency involved to fulfill its specific needs. **At a minimum**, however, those individuals who are using computers without or in excess of their authority, and those authorized users who are subject to monitoring, should be told expressly that by using the system they are consenting to such monitoring.

Your cooperation in this matter is appreciated.

Sincerely,

Robert S. Mueller, III
Assistant Attorney General
Criminal Division

By:

<signed>

John C. Keeney
Deputy Assistant Attorney General
Criminal Division

This page is intentionally left blank.

APPENDIX G. REQUIRED FILTERING RULES

The information in this appendix is supplied with the following caveats relative to the filtering guidance:

The table contains deviations from RFC 1700.

The table contains guidelines for implementing filtering rules (allow, deny, or conditional) at the Enclave and Security Domain perimeters.

Those ports and services that are noted as conditional are permitted as long as they meet the specific condition. Several of these must be restricted by source or destination address. Connections initiated by clients from external networks for services such as http, dns, smtp, and ftp must be restricted to only those servers residing in the DMZ or service network

Compatibility with existing applications is not known; therefore, the site should perform testing on a non-production system or network prior to deployment.

The TCP/UDP Port and Service Filtering Guide includes ports and services where documentation of problems was found and also any ports and services that are thought to be in use at any site. On the other hand, this does not mean that there are no documented problems with any unlisted ports—only that none were found. A great number of these ports and services are listed in RFC 1700. Internet Assigned Number Authority (IANA) maintains a web site that includes the most recent additions to the ports and services list. See http://www.iana.org/assignments/port-numbers. The DOD Ports and Protocol Technical Guidance is a valuable source that can be utilized in filtering traffic.The publicly accessible data (no FOUO) is at http://www.cert.mil/portsandprotocols/; the guide itself can be found at http://pnp.cert.smil.mil.

A Deny-by-Default (*"deny that which is not expressly permitted")* packet filtering policy is the only approved implementation of firewalls and premise or border router ACLs. With this type of policy implemented, all of the services that are vital to the organization must have a filtering rule that allows entry into the network.

KEY TO TABLE ENTRIES	
Allow	Without this service the system may not be fully functional. Allow, if required. Further security controls may be necessary to adhere to local security policy.
Deny	Possible source of entry for exploitation. If absolutely necessary, submit documenting rationale and alternate protection used.
Cond	Conditional. Allow only where service is needed with controls such as source and destination IP addresses, filtering, and strong authentication. Deny if not needed.

This page is intentionally left blank.

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
0.0.0.0			Deny		access-list 101 deny ip 0.0.0.0 0.255.255.255 any log	Historical Broadcast
255.255.255.255			Deny		access-list 101 deny ip host 255.255.255.255 any log	Broadcast
127.0.0.0			Deny		access-list 101 deny ip 127.0.0.0 0.255.255.255 any log	Local Host
10.0.0.0/8			Deny		access-list 101 deny ip 10.0.0.0 0.255.255.255 any log	Private Network
169.254.0.0/16			Deny		access-list 101 deny ip 169.254.0.0 0.0.255.255 any log	Link Local Networks
192.0.2.0/24			Deny		access-list 101 deny ip 192.0.2.0 0.0.0.255 any log	Test Net
192.168.0.0/16			Deny		access-list 101 deny ip 192.168.0.0 0.0.255.255 any log	Private Network
224.0.0.0/4			Deny		access-list 101 deny ip 224.0.0.0 15.255.255.255 any log	Class D Multicast
240.0.0.0/5			Deny		access-list 101 deny ip 240.0.0.0 7.255.255.255 any log	Class E Reserved
248.0.0.0/5			Deny		access-list 101 deny ip 248.0.0.0 7.255.255.255 any log	Unallocated
172.16.0.0/12			Deny		access-list 101 deny 172.16.0.0 0.15.255.255 any log	Private Network
192.0.0.192			Deny		access-list 101 deny 192.0.0.192 0.0.0.255 any log	HP Printer Default IP Address
192.0.127.0			Deny		access-list 101 deny ip 192.0.127.0 0.0.0.255 any log	IANA NS Lab 1
192.0.0.0			Deny		access-list 101 deny ip 192.0.0.0 0.255.255.255 any log	IANA NS Lab 2
0.0.0.0			Deny		access-list 101 deny ip 0.0.0.0 1.255.255.255 any log	Unallocated / IANA Reserved
2.0.0.0			Deny		access-list 101 deny ip 2.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
5.0.0.0			Deny		access-list 101 deny ip 5.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
7.0.0.0			Deny		access-list 101 deny ip 7.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
23.0.0.0			Deny		access-list 101 deny ip 23.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
27.0.0.0			Deny		access-list 101 deny ip 27.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
31.0.0.0			Deny		access-list 101 deny ip 31.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
36.0.0.0			Deny		access-list 101 deny ip 36.0.0.0 1.255.255.255 any log	Unallocated / IANA Reserved
39.0.0.0			Deny		access-list 101 deny ip 39.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
41.0.0.0			Deny		access-list 101 deny ip 41.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
42.0.0.0			Deny		access-list 101 deny ip 42.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
49.0.0.0			Deny		access-list 101 deny ip 49.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
50.0.0.0			Deny		access-list 101 deny ip 50.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
58.0.0.0			Deny		access-list 101 deny ip 58.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
59.0.0.0			Deny		access-list 101 deny ip 59.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
60.0.0.0			Deny		access-list 101 deny ip 60.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
70.0.0.0			Deny		access-list 101 deny ip 70.0.0.0 1.255.255.255 any log	Unallocated / IANA Reserved
72.0.0.0			Deny		access-list 101 deny ip 72.0.0.0 7.255.255.255 any log	Unallocated / IANA Reserved
82.0.0.0			Deny		access-list 101 deny ip 82.0.0.0 1.255.255.255 any log	Unallocated / IANA Reserved
84.0.0.0			Deny		access-list 101 deny ip 84.0.0.0 3.255.255.255 any log	Unallocated / IANA Reserved
88.0.0.0			Deny		access-list 101 deny ip 88.0.0.0 7.255.255.255 any log	Unallocated / IANA Reserved
96.0.0.0			Deny		access-list 101 deny ip 96.0.0.0 31.255.255.255 any log	Unallocated / IANA Reserved
197.0.0.0			Deny		access-list 101 deny ip 197.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
198.18.0.0			Deny		access-list 101 deny ip 198.18.0.0 0.1.255.255 any log	Unallocated / IANA Reserved
201.0.0.0			Deny		access-list 101 deny ip 201.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
222.0.0.0			Deny		access-list 101 deny ip 222.0.0.0 1.255.255.255 any log	Unallocated / IANA Reserved
223.0.0.0			Deny		access-list 101 deny ip 223.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
Streaming Audio\Video			Deny	Deny		
Traceroute		UDP	Deny	Cond	Access-list 101 deny udp any any range 33400 34400 log	Traceroute utility
Reserved	0	TCP; UDP	Deny	Deny		
TCPMux	1	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 1 log	TCP Port Multiplexer. Rarely used.
RJE	5	TCP, UDP	Deny	Deny	access-list 101 deny tcp any any eq 5 log	Remote Job Entry
Echo	7	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 7 log access-list 101 deny tcp any any eq 7 log	The echo service can be useful to determine if a machine is alive. A higher level equivalent of ICMP echo (ping). Can be used to probe network configuration and used for DoS attacks. CERT/CC 96-01 Denial of Service
Discard	9	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 9 log access-list 101 deny udp any any eq 9 log	The dev/null of the Internet. Harmless.
Systat	11	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 11 log	Occasionally connected to netstat, w, or ps; a.k.a., user's protocol. Returns active users.
Daytime	13	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 13 log access-list 101 deny udp any any eq 13 log	Time of day. Time has been used in generation of cryptographic keys. CERT/CC 96-01 Denial of Service
Netstat	15	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 15 log	Network status. Obsolete since 1994.
qotd	17	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 17 log	
MSP, v2	18	TCP	Deny	Deny	access-list 101 deny tcp any any eq 18 log	Message Send Protocol. See RFC 1312 for security considerations.
Chargen	19	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 19 log	Character Generator. CERT/CC 96-01 Denial of Service (UDP)
FTP-passive Data	20,21	TCP	Deny	Deny		
FTP-active Data	20,21	TCP	Deny	Cond	access- list 101 deny tcp any any eq 21 log	Ftp control channel. Allow only to your ftp server. Data channel for ftp. Hard to filter. Relevant CERT/CC Advisories: 97-27, 97-16, 94-08, 94-07, 93-10, 93-06, 99-13, DOD CERT 1999-B-0003.
SSH	22	TCP	Cond	Allow		Secure shell remote login protocol . Allow inbound to only authorized servers
Telnet	23	TCP	Cond	Allow		Telnet. Relevant CERT/CC Advisories: 95-14, 95-03. Use destination IP filtering and strong authentication. NOTE: Telnet sends passwords in the clear.
SMTP	25	TCP	Cond	Cond		Simple Mail Transfer Protocol. See CERT/CC Advisory 95-05 for sendmail vulnerabilities. Deny except for traffic to or from known mail servers.
Time	37	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 37 log access-list 101 deny tcp any any eq 37 log	Time of day in machine-readable format. CERT/CC 96-01 Denial of Service (UDP).
Whois	43	TCP; UDP	Deny	Allow	access-list 101 deny tcp any any eq 43 log	Internet user name directory service.
Nickname(whois)	47	TCP	Deny	Deny	access-list 101 deny tcp any any eq 47 log	Network and security administrators require access to whois information.
Login host protocol	49	TCP	Cond	Cond		Login Host Protocol. See CERT/CC Advisories 97-21, 97-15, 97-06, 94-09, 93-12, 91-08 and DOD CERT Bulletins 94-19, 93-24. RFC 1700 TACACS
RE-Mail-CK	50	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 50 log	
DNS	53	TCP; UDP	Cond	Cond		Domain Name Service. Block all DNS zone transfers except for authorized addresses. CERT/CC 99-14, DOD CERT 2000-A-01.
DNSSEC	53	TCP; UDP	Deny	Cond		
TACACS-DS	65	TCP	Cond	Cond		TACACS-Database Service. Control access to authenticate clients.
Bootps	67	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 67 log	Bootstrap protocol server. Not required and exploitable.

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
Bootpc	68	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 68 log	Bootstrap protocol client. Not required and exploitable.
Tftp	69	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 69 log	Trivial File Transfer Protocol. CERT/CC Advisories 91-18, 91-19.
Gopher	70	TCP	Deny	Cond	access-list 101 deny tcp any any eq 70 log	Gopher server. Not required and exploitable. See CERT/CC Advisory 93-11 and DOD CERT Bulletin 93-21. Needed to access Congressional Gopher Server.
NETRJS	71-74	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any range 71-74 log	Remote Job Service
RJE	77	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 77 log	Any Private RJE service
Finger	79	TCP	Deny	Deny	access-list 101 deny tcp any any eq 79 log	Finger. See CERT/CC Advisory 93-04 and DOD CERT Bulletin 93-06.
HTTP	80	TCP	Deny	Cond		Hyper Text Transfer Protocol. Deny incoming except to DMZ, proxy outgoing. DOD-CERT 1999-A-10, 1999-A-9, 1999-A-7, 1999-B-1, 1999-T-6, 1999-T-3, CERT/CC 2000-02.
LINK	87	TCP	Deny	Deny	access-list 101 deny tcp any any eq 87 log	Commonly used by hackers. A nice place for an alarm.
Kerberos	88	TCP/UDP	Cond	Cond		If kerberos authenticated logons are allowed (whether directly or via inter-realm authentication), this port must be open. Otherwise, it should be blocked. CERT/CC 96-03.
Supdup	95	TCP	Deny	Deny	access-list 101 deny tcp any any eq 95 log	SUPDUP. Hackers port. Good place for an alarm.
Hostname	101	TCP	Deny	Deny	access-list 101 deny tcp any any eq 101 log	
X.500/MTA	102	TCP	Cond	Cond		ISO-Directory.
X.400	104	TCP	Cond	Cond		X.400 Electronic Mail
X.400-SND	104	TCP	Cond	Cond		X.400 Electronic Mail
RTELNET	107	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any 107 log	Remote Telnet Service
POP-2	109	TCP	Deny	Deny	access-list 101 deny tcp any any eq 109 log	Post Office Protocol – Version 2. CERT/CC Advisory 98-11, 98-07, 97-09.
POP-3	110	TCP	Deny	Deny	access-list 101 deny tcp any any eq 110 log	Post Office Protocol – Version 3. CERT/CC Advisory 98-11, 98-07, 97-09.
Sun Remote Procedure Call (RPC)	111	TCP/UDP	Cond	Cond	access-list 101 deny tcp any any eq 111 log access-list 101 deny udp any any eq 111 log	SUN Remote Procedure Call. See CERT/CC Advisories 98-11, 95-17, 94-02, and DOD CERT Bulletins 98-08a, 95-49, 95-50.
Auth	113	TCP	Deny	Deny	access-list 101 deny tcp any any eq 113 log	IP authentication service. Identifies the username associated with a TCP connection. Can be spoofed. Sends full name from /etc/passwd if remote listening to IDENTD. DOD-CERT Bulletin 95-43. Incoming Ident connections to Ident daemon running on firewall can normally be permitted.
SFTP	115	TCP	Deny	Deny	access-list 101 deny tcp any any eq 115 log	Simple FTP.
UUCP-path	117	TCP	Deny	Deny	access-list 101 deny tcp any any eq 117 log	UUCP Path Service. See CERT/CC Advisory 92-06.
NNTP	119	TCP	Cond	Cond		Network News Transfer Protocol (nntp). Access should only be given through local nntp server and proxied. CERT/CC 97-08, DOD-CERT 97-02.
ERCP	121	TCP	Cond	Cond		Encore Expedited Remote Procedure Call.
NTP	123	TCP; UDP	Cond	Cond		Network Time Protocol. Required by DMS and other systems. Direct the router to at least two (2) different, reliable, NTP servers to ensure accuracy and availability of time information. CERT/CC 96-01 Denial of Service (UDP).
Statsrv	133	TCP	Deny	Deny	access-list 101 deny tcp any any eq 133 log	Statistics Service. See CERT/CC Advisory 97-26 and DOD CERT Bulletin 96-12.
MS-RPC	135	TCP; UDP	Deny	Deny		MS Remote Procedure Call. Required for MS Outlook, etc. Exploitable.
NetBIOS	137-139	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any range 137-139 log access-list 101 deny udp any any range 137-139 log	NETBIOS Name Service. Exploitable. Brute forcible if improperly configured. Susceptible to denial of service. NETBIOS Datagram Service. Exploitable.

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
						NETBIOS Session Service. Exploitable. Block at the premise if not mission required.
IMAP2	143	TCP	Deny	Deny	access-list 101 deny tcp any any eq 143 log	Internet Mail Access Protocol v2. CERT/CC 98-11, 98-07.
News	144	TCP	Cond	Cond		Block as if X-11.
SQL-Net	150	TCP	Cond	Cond		SQL-Net. IP filter.
SGMP	153	TCP	Cond	Cond		This was SNMP's predecessor.
SNMP	161	TCP/UDP	Deny	Cond		Simple Network Management Protocol. Exploitable. Block SNMP service to unauthorized users.
SNMP-TRAP	162	TCP/UDP	Cond	Cond		SNMPTRAP. Exploitable.
XDMCP	177	TCP; UDP	Deny	Deny	access-list 101 deny udp any any eq 177 log	
BGP	179	TCP	Deny	Deny	access-list 101 deny tcp any any eq 179 log	Border Gateway Protocol. Not allowed for internal enclave. However, required for connection to the NIPRNet.
SRMP	193	TCP	Cond	Cond		Spider Remote Monitoring Protocol.
IRC	194	TCP	Deny	Deny	access-list 101 deny tcp any any eq 194 log	Internet Relay Chat Protocol. See CERT/CC Advisory 94-14 and DOD CERT Bulletin 93-33.
IMAP3	220	TCP	Deny	Deny	access-list 101 deny tcp any any eq 220 log	Interactive Mail Access Protocol v3. See CERT/CC Advisory 98-11, 98-07, 97-09.
ICI (CMOS Interactive Communications Interface)	251	TCP	Cond	Cond		CMOS Interactive Communications Interface.
RAP	256	TCP	Cond	Cond		
SET	257	TCP; UDP	Cond	Cond		Secure Electronic Transaction. Use IP filtering.
LDAP	389	TCP	Cond	Cond		Lightweight Directory Access Protocol. Use IP filtering and authentication.
LDAP	390	TCP	Cond	Cond		Lightweight Directory Access Protocol. Use IP filtering and authentication.
HTTPS	443	TCP	Cond	Cond		HTTP protocol over TLS/SSL. DOD-CERT 1999-A-9.
SMB	445	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 445 log	MS directory services. Created as a new transport for SMB in W2K, replaces 137, 138, 139.
IsaKMP	500	UDP	Cond	Cond		Key Management Protocol. (IPSec)
Rexec/Biff	512	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 512 log access-list 101 deny udp any any eq 512 log	Remote process execution. Biff: Dangerous and buggy service.
Rlogin	513	TCP	Deny	Deny	access-list 101 deny tcp any any range 512-514 log access-list 101 deny udp any any range 512-514 log	Remote login. See CERT/CC Advisories 97-06, 95-15, 94-09.
Rwho	513	UDP	Deny	Deny	access-list 101 deny tcp any any range 512-514 log access-list 101 deny udp any any range 512-514 log	Remote who command. Maintains database of who is logged in to machines on a local network.
Rsh	514	TCP	Cond	Cond		Similar to exec, but automatic authentication is performed for login server.
Syslog	514	UDP	Deny	Deny	access-list 101 deny udp any any eq 514 log	Can gain access to audit logs. Exploitable. See CERT/CC Advisory 95-13.
LPD/LPR	515	TCP	Cond	Cond	access-list 101 allow tcp xxx.xxx.xxx.xxx eq 515	Line printer spooler. See CERT/CC Advisories 97-19, 95-15. Limit to authorized servers only.
Talk	517	UDP	Deny	Deny	access-list 101 deny udp any any range 517-518 log	Actual talk protocol uses random TCP ports. See CERT/CC Advisory 97-04 and DOD CERT Bulletin 97-07.
Ntalk	518	UDP	Deny	Deny	access-list 101 deny udp any any range 517-518 log	Same as talk.
RIP	520		Deny	Deny	access-list 101 deny udp any any eq 520 log	Outsiders can gain access to routing tables. Exploitable.
RPC	530	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 530 log	Courier. Experimental.

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
UUCP	540	TCP	Deny	Deny	access-list 101 deny tcp any any eq 540 log	UNIX-to-UNIX copy. Historically a dangerous service, and mostly obsolete on the Internet. See CERT/CC Advisory 92-06.
UUCP - rlogin	541	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 541 log	
Klogin	543	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 543 log access-list 101 deny udp any any eq 543 log	See CERT/CC Advisory 97-06.
Kshell	544	TCP; UDP	Cond	Cond		
NNTP(SSL)	563	TCP; UDP	Deny	Cond		nntp protocol over TLS/SSL (was snntp)
Ipp	631	TCP; UDP	Cond	Cond		IPP (Internet Printing Protocol)
LDAPS	636	TCP; UDP	Deny	Cond		LDAP protocol over TLS/SSL (was sldap).
LDAPS	637	TCP; UDP	Deny	Cond		LDAP protocol over TLS/SSL (was sldap).
Flexlm	744	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 744 log access-list 101 deny udp any any eq 744 log	Flexible License Manager. See CERT/CC Advisory 97-01.
kerberos-adm	749	TCP, UDP	Deny	Deny	access-list 101 deny tcp any any eq 749 log	Kerberos Administration
ftps-data	989	TCP; UDP	Cond	Allow		ftp protocol, data, over TLS/SSL
Ftps	990	TCP; UDP	Cond	Allow		ftp protocol, control, over TLS/SSL
telnets	992	TCP; UDP	Cond	Cond		telnet protocol over TLS/SSL
IMAP (SSL)	993	TCP	Cond	Cond		Imap4 protocol over TLS/SSL
Ircs	994	TCP; UDP	Cond	Cond		irc protocol over TLS/SSL
Pop3 (ssl)	995	TCP	Cond	Cond		Pop3 Protocol over SSL
Netspy	1024	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 1024 log	Trojan Port
Listener/Rasmin	1025	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1025 log	
ICQ	1027	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1027 log	ICQ chat
ICQ	1029	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1029 log	ICQ chat
ICQ	1032	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1032 log	ICQ chat
Xtreme	1090	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1090 log	
Psyber S.S.	1170	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1170 log	Voice streaming audio.
Ultors Trojan	1234	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1234 log	Ultors Trojan
Sub Seven	1243	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1243 log	Sub Seven Trojan
VooDoo Doll	1245	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1245 log	
PDA	1333	TCP	Deny	Cond		PerDiemAmazing. Travel orders and vouchers.
Back Orifice DLL	1349	UDP	Deny	Deny	access-list 101 deny tcp any any eq 1349 log	
Lotusnotes	1352	TCP	Cond	Cond		Lotus Notes. IP filtering based on client and server location.
SQL Server	1433	TCP	Cond	Cond		
FTP99CMP	1492	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1492 log	
ICA	1494	TCP	Cond	Cond		Citrix Independent Computing Architecture.
MS NetMtg	1503	TCP	Cond	Allow		Microsoft Net Meeting. T.120 teleconferencing protocol.
SQL*Net	1521-1535	TCP	Cond	Cond		Oracle SQL-Net.
DD/AM	1541-1575	TCP	Cond	Cond		
Shivka-Burka	1600	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1600 log	
SQL*Net	1601	TCP	Cond	Cond		

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
Icabrowser	1604	TCP/UDP	Cond	Cond		
PPTP	1723	TCP; UDP	Cond	Cond		
SQL*Net	1748	TCP	Cond	Cond		
SpySender	1807	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1807 log	
Shockrave	1981	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1981 log	
BackDoor	1999	TCP	Deny	Deny	access-list 101 deny tcp any any eq 1999 log	
Remotely Anywhere/ Open Windows	2000	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 2000 log access-list 101 deny udp any any eq 2000 log	Remotely Anywhere. Block if not mission essential.
Trojan Cow	2001	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2001 log	Remotely Anywhere. Block if not mission essential.
Ripper	2023	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2023 log	
NFS	2049	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 2049 log	NFS server daemon. CERT/CC Advisories 98-12, 96-09, 94-15, 94-02, 93-15, 92-15, 91-21, and DOD CERT Bulletin 1999-A-6, 1999-01, 94-41.
Bugs	2115	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2115 log	
Deep Throat	2140	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2140 log	
SubSeven21	2222	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2222 log	
JCALS	2223	UDP	Cond	Cond		
Compaqdiag	2301	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any eq 2301 log	
Striker	2565	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2565 log	
WinCrash	2583	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2583 log	
Listen	2766	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2766 log	
Phineas P.	2801	TCP	Deny	Deny	access-list 101 deny tcp any any eq 2801 log	Phineas Phucker Trojan
Redberry-RIM	3101	TCP	Deny	Cond		
XP terminal service	3398	TCP; UDP	Cond	Cond	Access-list 101 deny ip any any eg 3398 log	XP Remote desktop and remote assistance port. Block if not mission essential.
Lockd	4045	UDP	Deny	Deny	access-list 101 deny udp any any eq 4045 log	
Audit	5402	TCP	Cond	Cond		
WASP	5403	TCP	Cond	Cond		
WASP	5404	TCP	Cond	Cond		
Calendar	5730	TCP	Deny	Deny	access-list 101 deny tcp any any eq 5730 log	Netscape calendar.
WinVNC	5800	UDP	Deny	Deny	access-list 101 deny udp any any eq 5800 log	
WinVNC	5900	TCP	Deny	Deny	access-list 101 deny tcp any any eq 5900 log	
X11	6000-6063	TCP/UDP	Cond	Cond		Block the entire range of X11 ports, if possible.
MS CHAT	6665	TCP	Deny	Deny	access-list 101 deny tcp any any eq 6665 log	
IRC\ SubsSeven	6665-6669	TCP	Deny	Deny	access-list 101 deny tcp any any range 6665-6669 log	Internet Relay Chat. May or may not be a security risk per se, but some channels attract the sort of network people who send out ICMP Destination Unreachable messages. See CERT/CC Advisory 94-14 and DOD CERT Bulletin 94-33.
SubSeven	6711-6712	TCP	Deny	Deny	access-list 101 deny tcp any any range 6711-6712 log	Sub Seven Trojan
SubSeven	6776	TCP	Deny	Deny	access-list 101 deny tcp any any eq 6776 log	Sub Seven Trojan
MS CHAT listen Also subseven21	7000	TCP	Deny	Deny	access-list 101 deny tcp any any eq 7000 log	Remote Grab Trojan.
PNM	7070	TCP	Cond	Deny		Streaming audio. Also referred to as RealAudio.
Cisco Catalyst Switch	7161	TCP; UDP	Deny	Cond		Block if applicable. Cisco Catalyst Switch. Field Notice: Cisco Catalyst Supervisor

TCP/UDP PORT AND SERVICE FILTERING GUIDE						
SERVICE	**PORT**	**PROTOCOL**	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
			In-Bound	**Out-Bound**		
						Remote reload
Alt. HTTP	8008	TCP; UDP	Deny	Cond		Alternate HTTP Port.
Alt. HTTP	8080	TCP; UDP	Deny	Cond		Alternate HTTP Port.
Old SWA Port	8999	TCP	Cond	Cond		
CS Listener (Oracle)	9000	TCP	Cond	Cond		
SWA	9023	TCP	Cond	Cond		
SWA	9024	TCP	Cond	Cond		
SWA-3	9025	TCP	Cond	Cond		Secure Web Access.
SWA-4	9026	TCP	Cond	Cond		Secure Web Access.
NetBus	12345-12346	TCP	Deny	Deny	access-list 101 deny tcp any any range 12345-12346 log	Netbus Trojan
Stacheldraht	16660	TCP	Deny	Deny	access-list 101 deny tcp any any eq 16660 log	DDoS
DMS X.500	17003	TCP	Cond	Cond		
Trinoo	27444	UDP	Deny	Deny	access-list 101 deny udp any any eq 27444 log	DDoS
Trinoo	27665	TCP	Deny	Deny	access-list 101 deny tcp any any eq 27665 log	DDoS
Defense Travel Service	31017	TCP	Deny	Cond	Access-list 101 deny tcp any any eq 31017	Only needed for outbound connections
Trinoo	31335	UDP	Deny	Deny	access-list 101 deny udp any any eq 31335 log	DDoS
Back Orifice	31337-31338	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any range 31337-31338 log	DDoS
RPC Services	32700-32900	TCP; UDP	Deny	Deny	access-list 101 deny tcp any any range 32700-32900 log	
Trinity V3	33270	TCP	Deny	Deny	access-list 101 deny tcp any any eq 33270 log	DDoS
Trinity V3	39168	TCP	Deny	Deny	access-list 101 deny tcp any any eq 39168 log	DDoS
Torn rootkit system	47017	TCP	Deny	Deny	access-list 101 deny tcp any any eq 47017 log	DDoS
Stacheldraht	65000	TCP	Deny	Deny	access-list 101 deny tcp any any eq 65000 log	DDoS
PC Anywhere	65301	TCP	Deny	Deny	access-list 101 deny tcp any any eq 65301 log	PC Anywhere. Block if not mission essential.

This page is intentionally left blank.

APPENDIX H. DISA ENCLAVE SECURITY IMPLEMENTATION DESCRIPTION REPORT

TO: DISA Chief Information Officer (CIO)

FROM: Site Name/Site Code

DATE: dd mm yyyy

SUBJECT: DISA Enclave Security Implementation Description Report

PREPARER: Name/Site Code/DSN

1. DISA Organization reporting the modification (e.g., addition, removal or relocation of hardware or software) in site/system configuration:

2. Brief description of the modification (e.g., new subnet added, new lab installed, changing vendor product or altering required settings):

3. Technical POC for this Request (IAO, IAM, System Administrator [SA] or Firewall Administrator [FA]) who will be responsible for submitting this template to the CIO for follow-up questions:

Name:
Office:
Phone:
Title:
E-mail address:

4. Appropriate administrator (e.g., SA, FA) for this request (include the qualifications and skills of the individual):

Name:
Office:
Phone:
Title:
E-mail address:

5. Location where modification will be made (i.e., building, room number, street address, city, state). State the physical protection conditions (i.e., Sensitive Compartmented Information Facility [SCIF], Network Operations Center).

6. Vendor of hardware or software product(s) affected, model number, version number, and release of underlying OS or system software (e.g., Solaris 2.5.1, Windows NT 4.0). Include the use of third-party products used in association with the modification (e.g., firewall, virus scanning, intrusion detection, etc.).

7. Attach a copy of the architecture diagram. The diagram will identify all assets associated with the site or system being modified. This will include networks assigned, IP addresses of applicable components, etc. A system-wide diagram showing other assets in the environment or other connections to external networks will be included.

8. Identify (a) how the assets are protected against unauthorized access (e.g., *(physical security requirements are in para 5? physical* security,*)* administrative access to the equipment, ports and services that are required or denied, etc.), (b) how the new configuration will be periodically examined or tested to ensure the modification continues to operate in the approved configuration, (c) the roles and responsibilities associated with the modification (e.g., DISA organization management, designated FA, users).

9. Attach only updated portions of the SSAA that reflect the modification.

Site Signature Block

APPENDIX I. JUNIPER ROUTER SPECIFIC REQUIREMENTS

Juniper routers specific requirements are listed below. These are requirements that are net covered under the router sections, and are in addition to the applicable requirements covered in that section.

- The Juniper Router Administrators will deploy Juniper JUNOS 5.5 or current general deployment (GD) release.

- Juniper Administrators will ensure that custom classes are created. No user will belong to any of the pre-defined classes (superuser, super-user, operator, read-only, and unauthorized). All custom classes will be configured to time out after fifteen minutes of inactivity.

- Juniper Administrators will remove the ability to start shell from all custom classes except the super-local class. The ability to authenticate as root will be removed from all custom classes to include the super-local class. This ability will only be authorized when logged into the router locally via a console port or management interface.

- The Juniper administrators will provide the router with a unique identifier (i.e., hostname).

- The Juniper administrators will configure the domain name for the router, this domain name would be the name registered with the .MIL NIC.

- Juniper administrators will tag each log entry destined to the central syslog server with a unique identifier.

- Juniper administrators will ensure that the sending of protocol redirect messages is disabled. These packets may cause memory problems for other network devices due to the fact that they may try to store all of the messages. These messages can cause more problems than they resolve.

- The Juniper Router Administrator will ensure the router is configured to discard source-routed packets (prior to the packet being sent to the RE).

- The Juniper Router Administrator will ensure Unicast reverse path forwarding (uRPF) is enabled on the router. URPF check is a tool to reduce forwarding of IP packets that may be spoofing an address. An uRPF check performs a route table lookup on an IP packet's source address, and checks the incoming interface. The router determines whether the packet is arriving from a path that the sender would use to reach the destination. If the packet is from a valid path, the router forwards the packet to the destination address. If it is not from a valid path, the router discards the packet. Juniper routers should be enabled with Unicast RPF.

- The Juniper Router Administrators will ensure the number of concurrent SSH sessions and the maximum number of sessions established in 1 minute is rate limited. These parameters can be useful in protecting against some DOS attacks on the SSH port.
- When performing remote router administration, the Juniper Router Administrators will use the SCP protocol to transfer the configuration files to and from the router. The secure copy

protocol uses the SSH encryption and authentication infrastructure to securely copy files between hosts. The JUNOS software can use SCP with the file copy operational mode command. Verify that the only service enabled is SSH, thereby ensuring that SCP is the only (and default) transfer protocol.

- Juniper administrators will ensure all access is restricted to SSH version 2 connections and that remote root authentication is removed. All access to the router, whether in-band or out-of-band (excluding direct console access), will be done via an SSH connection.

- The Juniper Router Administrators will ensure that a copy of a known stable configuration will be stored on the hard drive prior to any software upgrade.

- The Juniper administrator's software upgrade and release procedures will define all steps for the upgrade, reference vendor documentation related to updating the device, and provide testing procedures for validating the device after the upgrade.

- The Juniper Router Administrators when saving and loading configurations will always ensure that the candidate configuration is synchronized with the current configuration.

- The Juniper Router Administrators will ensure that the router will create a core dump in the event of a crash. A Core dump will help troubleshoot the problem.

- Juniper administrators will create a user account named "remote" and set a login class of "unauthorized" for this user.

- The Juniper Router Administrators will configure the router to send all syslog messages to include "any" facility with a severity level of "info" to a central syslog server.

- The Juniper Router Administrator will configure a firewall filter to protect the router's loopback interface.

- Juniper Administrators will configure the router to restrict all NTP messages in the loopback filter.

- Juniper administrators will ensure either SNMP version 3 or SNMP version 2 is used in read-only mode, if read-write is needed it must be approved in writing by the DAA.

- Juniper administrators will restrict SNMP (if used) access to the router to only the allowed IP addresses.

- Juniper administrators will ensure SNMP (if used) will only be used on the internal interfaces.

- Juniper administrators will set passwords on the open diagnostic ports to the SSB (System and Switch Board – M20 specific) System Control Board – M40 specific), and SFM

(Switching and Forwarding Module – M40e specific), as well as the PIC authentication global command that controls access to the PIC console ports.

- Juniper administrators will ensure that the management port (fxp0) is disabled if not being utilized for managing the router.

- Juniper Administrators will disable router interfaces that are not in use.

- Juniper administrators will specify a root password, since by default, the password is blank. The root password will be unique for each router and will not be set to any other password/value on the router. The router will accept the plaintext password and encrypt it. The password will not be stored in plaintext.

- Juniper administrators will ensure that the auxiliary port has not been enabled; since modems are not authorized for remote management of routers and the console port is pre-configured for vt100 terminal emulation.

- Juniper administrators will employ TACACS+ or RADIUS as a means to secure the Juniper router network. With several methods of authentication, trying the preferred process first is important. If the preferred method (TACACS+ or RADIUS) fails, an emergency local account can be used.

- The Juniper administrators will ensure that a shared secret key is established and shared between the router and the TACACS+\Radius server.

- The Juniper administrators will define standard accounts on the TACACS+ or RADIUS server and the user password will be setup accordingly.

- The Juniper Administrators will ensure only the minimum number of emergency local accounts will be set up on the router. Accounts with a password assigned (emergency local account and root) must be examined. All other user accounts are associated with a TACACS+ or RADIUS account and will not have passwords assigned to them on the router.

- Juniper Administrators will employ strong two-factor authentication (Two-Factor Authentication is a security process that confirms user identities using two distinctive factors —**something you know**, such as a Personal Identification Number (PIN), and **something you have**, such as a smart card or token, or **something you are**, such as retina scan or finger print) for all managed network devices.

- The Juniper administrators will establish a timeout of 3 seconds and 3 retry attempts for every radius\TACACS+ server supporting the router.

- Juniper administrators will ensure the following services that are disabled by default on the router have not been enabled: telnet, rlogin, ftp, finger

- Juniper administrators will ensure the number of concurrent SSH sessions and the maximum number of sessions established in 1 minute is rate limited. These parameters can be useful in protecting against some DOS attacks on the SSH port. It is also advised to limit the number of SSH connections, and connection attempts within a minute. Although this is site dependent, it should be kept to a minimum. The maximum for both limits is 250, but the default is 75 connections; it will be set to 5 or less. The connection attempts default to 150 within one minute; it will be set to 10 or less.

- Juniper administrators will set the clock to the correct time zone. This is essential for troubleshooting, forensics, evidence, and syncing time with the other routers. The default time zone is Universal Coordinated Time (UTC). UTC is the same as Greenwich Mean Time (GMT), which is based at the prime meridian (0 degrees longitude) of the Earth. So, if it is not specified then the administrator must understand that they will be running at UTC.

- Juniper administrators will set the source address of the loopback address for all of outgoing packets originating from the router. By restricting the source address to just the loopback address, the physical interface addresses are protected.

APPENDIX J. ADDENDUM TO THE NSA GUIDE TO E-MAIL SECURITY

FILE EXTENSIONS TO BE BLOCKED/FILTERED

Reference page 12, Countermeasure 7, of the *NSA Guide to E-mail Security in the Wake of Recent Malicious Code Incidents*. The following table contains a list of mail attachments that will be blocked/filtered at the mail server.

FILE TYPE	*DESCRIPTION*
ACM	Audio Compression Manager Driver (Windows) and Windows System File
ADE	Microsoft Access Project Extension
ADP	Microsoft Access Project
ASP	Active Server Page
AVB	Inoculan Anti-Virus Virus Infected File
BAS	Visual Basic® Class Module
BAT	Batch File
BIN	BINARY FILE
CFM	Cold Fusion File
CHM	Compiled HTML Help File
CLASS	Java Class File
CLA	Java Class File (usually .CLASS but can be shortened)
CMD	Windows NT® Command Script
CNT	Microsoft system content files for the help index and other purposes
CNV	MS Word Data Conversion File
COM	MS-DOS® Application
CPL	Control Panel Extension
CRT	Security Certificate
CSS	Cascading Style Sheet file (MIME)
CS*	COREL SCRIPT

FILE TYPE	*DESCRIPTION*
DLL	Dynamic Link Library
DRV	Device Driver
EXE	Application
GMS	Corel Global Macro Storage
HLP	Windows® Help File
HTA	HTML Applications
HTT	Hypertext Template
INF	Setup Information File
INI	Initialization file
INS	Internet Communication Settings
ISP	Internet Communication Settings
JAVA	Java Source Code
JS	JScript® FILE
JSE	JScript Encoded Script File
JSP	Java Server Pages
LNK	Shortcut
MDB	Microsoft Access Application
MDE	Microsoft Access MDE Database
MHT*	MS® MHTML DOCUMENT (ARCHIVED WEB PAGE)
MPD	Mini Port Driver
MPG	Motion Picture Graphics
MP3	MPEG Audio Layer 3 (AC3)
MSC	Microsoft Common Console Document
MSI	Windows Installer Package
MSP	Windows Installer Patch

FILE TYPE	*DESCRIPTION*
MST	Visual Test Source File
OCX	Object Linking and Embedding (OLE) Control Extension
OV*	Program Overlay File (.OVL)
PCD	Photo CD Image
PIF	Shortcut to MS-DOS Program
PL	PERL
REG	Registration Entries
PHP	Personal Home Page
RPM	RealAudio Files
SCR	Screen Saver
SCT	Windows Script Component
SHB	Corel Show presentation or Document shortcut file
SHS	Shell Scrap Object
SHTM	Server Side Include
SHTML	Server Side Include
SYS	System Device Driver
TLB	Remote Automation Truelib Files
TSP	Windows Telephony Service Provider
URL	Internet Shortcut (Uniform Resource Locator)
VB	VBScript File
VBE	VBScript Encoded Script File
VBS	VBScript Script File
VXD	Virtual Device Driver
WBT	WinBatch Script
WIZ	Wizard FileSystem Device Driver

FILE TYPE	*DESCRIPTION*
WS	Windows Scripting File
WSC	Windows Script Component
WSF	Windows Script File
WSH	Windows Scripting Host Settings File
.386	Windows Enhanced Mode Driver or Swap File

Sites that operationally require the passing of any of these files can optionally use an archiving utility to exchange them as Zip or Tar files.

The following file extensions should be blocked if the site does not encourage the exchange of any files, or the site can choose to selectively block some or all of the following files depending on operational commitments.

FILE TYPE	*DESCRIPTION*
CD*	Corel Graphic and Corel Draw Template
CPT	Corel PhotoPaint
DO*	Documents
DVB	AutoCAD
EML	MS Outlook Express Electronic Mail
HTM	Hypertext Markup Language (HTML)
HTML	Hypertext Markup Language (HTML)
MPP	MS Project File
MPT	MS Project Template File
MSG	Program Message, OzWin Message/Mail File, MS Mail Message
NWS*	MS Outlook Express News File
VS*	Visio Drawing
WBK	Word Backup and WordPerfect Workbook
WPD	Corel Word Perfect
XL*	Spreadsheets

FILE TYPE	*DESCRIPTION*
SMM	Ami Pro Macro
SHW	Corel Presentation
POT	PowerPoint Template
PP*	PowerPoint File
QPW	Corel Quatro Pro
ORB	MS Office Binder
RTF	Rich Text Format

Sites should configure the E-mail server to place a message into the original email informing the recipient of the change to the message and the file name of the text file that lists all the deleted files.

An example of an inserted message:

> *---------- This text was added by the Exchange mail relay ----------*
>
> *This notification was inserted in order to inform you of CHANGES that have occurred to this email message. This action may cause the original text to appear as an attachment.*
>
> *Due to the impact from several email-borne viruses, restrictions have been placed on the types of attachments that will be allowed through the site's E-mail system from the Internet. The types of file attachments that are restricted include exe, vbs, and several other types. At the instruction of Field Security Operations (FSO), these attachments were removed from the message and deleted.*
>
> *A list of files that were removed may be found in a text attachment added to this message which is named "removed.txt".*
>
> *---------- End of text added by an Exchange mail relay ----------*