INTERNET PROTOCOL TELEPHONY & VOICE OVER INTERNET PROTOCOL

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 2

21 APRIL 2006

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

This page is intentionally left blank.

SUMMARY OF CHANGES

V2R2 21 APRIL 2006

Section 3.1 Protecting VoIP Critical Servers

VoIP0280: Changed Severity from CAT II to CAT III

Section 3.2 Physical Security

VoIP0050: Modified requirement to note that the requirement does not apply to end instruments.

Section 3.3 Protection of System And Instrument Configuration

VoIP0060: Changed severity from CAT II to CAT III

Section 3.4 VoIP Instrument/Terminal Registration

VoIP0065: Changed severity from CAT II to CAT III
VoIP0068: Changed severity from CAT I to CAT II

Section 3.5.2.1 Voice VLAN

VoIP0100: Changed severity from CAT I to CAT II

Section 3.6 IP Soft Phones

VoIP0130: Changed severity from CAT I to CAT II
VoIP0135: Changed severity from CAT I to CAT III
VoIP0150: Changed severity from CAT I to CAT III
VoIP0160: Changed severity from CAT I to CAT II
VoIP0165: Changed severity from CAT I to CAT II

Section 3.7.1 Local Voice to Data Network and VLAN to VLAN Protection

VoIP0090: Changed severity from CAT I to CAT III
VoIP0095: Changed severity from CAT I to CAT II

Section 3.9.2 VoIP Firewall Management

VoIP0250: Removed requirement for configuring management in accordance with Network Infrastructure STIG. Similar reuirement stated in VoIP0245.

V2R1 29 AUGUST 2005

GENERAL CHANGES:

Updated the title of the STIG
Generally reorganized the document

SECTION CHANGES:

Forward and acknowledgements

Deleted in accordance with normal STIG template added acknowledgement to the intro.

SECTION 1. INTRODUCTION

Rewrote this section.
VoIP0010: deleted this PDI, as it is redundant to requirements in section 3.
VoIP0020: Moved the requirement to section 3.
VoIP0030: Moved the requirement to section 3.

Section 1.1 Background

Added this section and generally rewrote it using verbiage from the DSN PMO.

Sections 1.2, 1.3 Background, Scope, and Purpose

Removed the Purpose section and included appropriate verbiage in the Introduction.
Moved all requirement descriptions and bullets to other sections as appropriate.

Section 1.2 Scope

Rewrote this section.

Section 1.3 Authority

Updated the section to reflect the current FSO Section 1 template authority verbiage and added verbiage to include DODI 8100.3 information. Defined the Mission Assurance Category acronym MAC as in MAC II.

Section 1.4 Writing Conventions

Updated to the current FSO STIG writing convention verbiage.

Section 1.5 DISA Information Assurance Vulnerability Management (IAVM)

Updated to the current FSO STIG IVAM verbiage. Moved the VMS explanation and requirements to section 3.
Removed the section regarding extensions.

Section 1.6 Vulnerability Severity Code Definitions

Added the section on severity codes.

Section 1.7 STIG Distribution

Updated to the current FSO STIG distribution verbiage.

Section 1.7.1 STIG Distribution to DSN Vendors

Added this section regarding distribution information for DSN vendors.

Section 1.8 Document Revisions and Support

Updated to the current FSO STIG document revision verbiage and added STIG support verbiage.

SECTION 2. IP TELEPHONY OVERVIEW

Removed first paragraph merged its content into section 1 Introduction.

Sections 2.1 through 2.4 and subsections

Rewrote these sections and subsections for accuracy and clarity.
Improved Figures 2.1 and 2.2.

Section 2.2.2 Session Initiation Protocol (SIP)

Rewrote this section for accuracy and clarity.

Section 2.2.3 Media Gateway Control Protocol (MGCP)

Rewrote this section for accuracy and clarity. Moved the second paragraph to Section 3.
VoIP0040, moved this requirement to Section 3.

Section 2.3.3 VoSIP and SVoIP.

Added this section.

Section 2.4.4 Additional Vulnerabilities

Added this section.

SECTION 3. SECURING THE VOIP ENVIRONMENT

Corrected grammatical errors and rewrote portions for added clarity.
Figures 3.1: Redrew for accuracy and clarity
VoIP0050: Added this requirement regarding proper network design and compliance w/ GSCR appendix 3.
VoIP0020: Moved the requirement from section 2. Rewrote for clarity regarding compliance with Network and Enclave STIGs.
VoIP0030: Moved the requirement from section 2. Regarding VoIP system inclusion in the site SSAA.
VoIP0035: Added this requirement regarding compliance with the DSN STIG.

Section 3.1 Protecting VoIP Critical Servers

This section was section 3.7 and was revised for clarity.
VoIP0280: revised for clarity.

Section 3.1.1 Vulnerability Management

Added this section.
VoIP0281: Added this PDI.

Section 3.2 Physical Security

This section was section 3.1. Rewrote for clarity.
VoIP0050: elevated this PDI to CAT I.
VoIP0060: relocated this PDI to the newly created section 3.2.

Section 3.3 Protection of System And Instrument Configuration

Added this section. Included VoIP0060 from section 3.1.
VoIP0060: Rewrote for clarity and generality.
VoIP0061, 62: Added these PDIs.
Section 3.4: VoIP Instrument/Terminal Registration.
Added this section.
VoIP0065, 66, 67, and 68: Added these PDIs.

Section 3.5 Local Enclave Data and Voice Network Segregation

This section was part of section 3.2. Re-titled.
Added this section. Used the first paragraph from old section 3.2 and rewrote for clarity and grammar and expanded the discussion.

Section 3.5.1 IP Address Segregation

This section was part of section 3.2 Revised for clarity.
VoIP0080: added a caveat for SIPRNet to this PDI.
VoIP0082: added this PDI regarding the use of DHCP.
VoIP0085: added this PDI for SIPRNet address block separation.

Section 3.5.2 Local Network Voice / Data Segregation Using VLANs

This section was part of section 3.3. Re-titled.
Rewrote the section for clarity.

Section 3.5.2.1 Voice VLAN

This section was part of section 3.3.
Expanded and rewrote for clarity.
VoIP0101, 102, 103, 105, 111: Added these PDIs.
VoIP0100, 110: rewrote these PDIs for clarity.

Section 3.5.2.2 Voice VLAN Access

This section was part of section 3.3.
Added discussions on port security, 802.1x, and VPMS.
VoIP0122: added this PDI regarding VoIP phone PC ports.
VoIP0125: added this PDI regarding switch port security.

Section 3.6 IP Soft Phones

This section was part of section 3.4.
Rewrote this section for clarity, also reorganized the PDIs.
VoIP0130: Was VoIP0140: rewrote this PDI for clarity regarding DAA approval and adding a requirement for documented evidence and raised it to CAT I.
VoIP0135: Was VoIP0150: rewrote this PDI for clarity regarding local Soft Phone policy and raised it to CAT I.
VoIP0140: added this PDI regarding OS STIG compliance and raised it to CAT II.
VoIP0150: Was VoIP0130: rewrote this PDI for clarity regarding use of Soft Phones on a LAN and changed to a CAT I.
VoIP0160: rewrote this PDI for clarity regarding use of remote Soft Phones and raised it to CAT I.
VoIP0165: added this CAT I PDI regarding Soft Phones in call centers.
Eliminated redundant verbiage regarding PC ports on VoIP phones and filtering of traffic between the voice and data VLANs.

Section 3.7 Network Protection And Traffic Control

Added this section as an overarching topic for subsequent sections.

Section 3.7.1 Local Voice to Data Network and VLAN to VLAN Protection

Added this section. Used part of section 3.5
Expanded and rewrote for clarity.

VoIP0090: Rewrote this PDI and raised it to CAT I. Eliminated the requirement for NAT between Voice and data VLANs and clarified the requirement for a stateful firewall.
VoIP091, 95, 115, 116: Added these PDIs. 2 of which are CAT I.

Section 3.7.2 WAN Connectivity and LAN-WAN Protection

Added this section.

Section 3.7.2.1 Current Policy

VoIP0900: Added this PDI regarding the required use of media gateways for trunking.
VoIP0901: Added this PDI regarding VoIP WAN connections needing DAA approval.

Section 3.7.2.2 Firewall Requirements and Control

This section was 3.5. Rewrote for clarity.
VoIP0180: Rewrote this PDI for clarity regarding firewalls on VoIP WAN Connections.
VoIP0190 (old): Eliminated this PDI specific to H323 ports. The requirement was a given.
VoIP0190 (new): Reused this PDI number for requirements regarding NAT.
VoIP0200: Rewrote this PDI for clarity regarding dedicated firewalls on VoIP WAN Connections.
Table 3.2: added DHCP, SIP, and RTP/RTCP Port.
VoIP0230: clarified this PDI regarding the timing source.
VoIP0245: added this PDI regarding web access through the VoIP firewall.

Section 3.8 Call Privacy and Confidentiality

This section was 3.9. Re-titled it and rewrote for clarity.
VoIP0300: Rewrote this PDI for clarity regarding encryption on WAN connections.

Section 3.9 VoIP Systems Management

Added this section to group management requirements.
VoIP0295: Added this PDI referencing the DSN STIG for system management requirements.

Section 3.9.1 Remote Access Management of VoIP Servers

This section was 3.8.
VoIP0260: Deleted this PDI.

Section 3.9.2 VoIP Firewall Management

This section was 3.6. Rewrote for clarity.
VoIP0210: Rewrote this requirement for clarity.
VoIP0250: Rewrote this PDI to reference the Network Infrastructure STIG.

Section 3.10 Voice Mail Services

This section was 3.10. Rewrote for clarity.
VoIP0320: removed this PDI since it duplicated previous requirements.
VoIP0330, 0340: rewrote for clarity and changed to CAT II.
VoIP0310: changed to CAT II.

Section 3.11 Wireless VoIP

This section was 3.11.

Section 3.12 Securing MGCP

Added this section for the associated requirements. It was part of section 2.2.3.
VoIP0040: relocated this PDI from the original subsection 2.2.3.

Section 3.13 VoIP Connection to the Defense Switched Network (DSN)

This section was 3.12.

APPENDIX A. RELATED PUBLICATIONS

Added a heading for industry publications at the bottom and relocated the 3 publications that were at the top to this new section.
Added the following government publications DODI 8100.3; (NIST) SP 800-58; DSN GSCR.
Deleted NIST “Security Considerations for Voice Over IP Systems” (Draft), October 2003. – Replaced by SP 800-58.

APPENDIX B. GLOSSARY OF TERMS

This section was Appendix F.
Merged with the DSN STIG glossary. Thus added too many to list here.
Added ALG, C2VG, FCP, FNBDT, HAIPIS, NID, NIDS, PTT, RTP, STU, SVoIP, VoSIP, SVoSIP, SCIP.

APPENDIX B (OLD). CISCO PLACEHOLDER

Deleted this placeholder. Information planned for this section will be placed in an addendum to the STIG.

APPENDIX C (OLD). NORTEL PLACEHOLDER

Deleted this placeholder and appendix. Information planned for this section will be placed in an addendum to the STIG.

APPENDIX D (OLD). AVAYA PLACEHOLDER

Deleted this placeholder and appendix. Information planned for this section will be placed in an addendum to the STIG.

APPENDIX E (OLD). INTERIM VOICE OVER INTERNET PROTOCOL POLICY MESSAGE

Deleted this appendix and message since it is superceded by DSN APL certification efforts.

1. INTRODUCTION

The *Internet Protocol Telephony & Voice over Internet Protocol Security Technical Implementation Guide (IPT & VoIP STIG)* is published as a tool to assist in securing networks and systems supporting *Voice over Internet Protocol (*VoIP) technology for the purpose of converging voice and data networks by the use of IPT. When applied to Department of Defense (DOD) networks and systems, this document must be used in conjunction with the Defense Switched Network (DSN) STIG, since it contains specific requirements for DOD telecommunications systems and systems connected to the DSN. Additionally, this STIG must be used in conjunction with other STIGs relating to Operating Systems (OSs), databases, Web servers, network infrastructure, enclaves, etc. as appropriate to secure the underlying platforms of the IPT system.

Networks or applications, supporting IPT must possess a level of security that must be maintained over the entire network from terminal device to terminal device. In order to meet the security requirements of these systems, the network must be designed, implemented, maintained, and operated in a secure manner, providing end-to-end security from the VoIP terminal device to the VoIP applications required for operation, including applicable host platforms, the supporting VoIP network devices, and associated support software (e.g., Structured Query Language (SQL) server, Internet Information Services (IIS) web server, etc.).

VoIP is a process that enables the transfer of voice data over a packet switched network as opposed to the traditional circuit-switched network. IPT, if implemented properly, holds the promise of converged networks and unified communications. In some cases this technology will enable organizations to converge voice and data networks, which will reduce costs and enable new applications that integrate voice and data services. However, with this technology come many security issues and concerns that will be discussed later in this document. Section 2 will present a very high level overview of the technology and predominant protocols used, in order to provide a basic understanding of IPT and VoIP. This overview will not provide detailed information of all vendor specific proprietary protocols or implementations of VoIP technology.

For the purpose of this document, we will use the terms IPT and VoIP interchangeably.

We would like to acknowledge the assistance of members of the National Security Agency (NSA), DSN Program Management Office (PMO), DSN Voice Connection Approval Office (VCAO), Joint Interoperability Test Command (JITC), Information Assurance (IA) Test team, Air Force Warfare Information Center (AFWIC), and other DOD components who have provided valuable comments and input for this STIG.

1.1 Background

VoIP is an emerging technology that is a critical component of network centric warfare. VoIP is associated with potential command center desktop convergence, mobility enhancements, infrastructure reduction, multi-media collaboration, and cost avoidance. Implementing VoIP is a critical step toward DOD's ability to effectively provide all DOD communications traffic (data, voice, video, etc.) on an IP network that is central to effective network centric warfare.

Both data network and circuit-switched telephony vendors are investing in VoIP and are aggressively marketing their approaches. In some cases, DOD Components and Agencies have instituted VoIP pilots, trials and implementations that provide DSN phone numbers and dial tone for access to origination and reception of DSN services. Currently, VoIP is being employed with and without C2 capability at the Base/Post/Camp/Station (BPCS) level on the Local, Campus, or Base Area Network (LAN/CAN/BAN), and at the network edge of the DSN, Non-Classified (But Sensitive) Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet). It is also being employed in the backbones of SIPRNet and NIPRNet with and without C2 features.

CJCSI 6215.01B Enclosure A paragraph 10, defines network security requirements for the DSN. While denial-of-service attacks on the circuit-switched DSN are quite rare, denial-of-service attacks on the DOD's data infrastructure occur frequently. This denial-of-service can include: intrusion, spoofing, snooping, or virus attacks such as the Melissa virus. While these attacks have no effect on today's circuit-switched voice community, they can virtually shut down data networks while other data networks are impacted by the congestion generated by these viruses. During these periods, VoIP customers would lose their data and voice capabilities all together. This could have tragic consequences in a military environment.

Security in a VoIP environment differs from security in a closed, circuit-switched network. Most of the security concerns in the circuit-switched network are focused on the central telephone switch. In a VoIP environment, service is no longer based on a central telephone switch with dedicated physical loops to each instrument, but is provided by functional elements distributed throughout the customer service area. Each of these distributed elements, which include terminals (IP phones), gateways, gatekeepers, and call control agents, present an opportunity for security to be compromised. Also, the switching fabric that used to reside inside the PBX cabinet is now distributed and available for malicious attack and eavesdropping. In short, the breaking out of the functional elements of a contained and proprietary switching system into distributed pieces of equipment operating with open protocols complicates the issues involved in securing IPT.

Security issues can be approached from two perspectives: signal ports and operations ports. Signal ports are those involved with call setup and teardown and the transport of bearer traffic. Operations ports are those involved in administration of the distributed architecture, e.g., Command Line Interface (CLI) on routers, gatekeepers, and gateways. Operations ports are network management ports. As VoIP further develops and standardizes, additional specific security measures will be required and will be outlined in future releases of the IPT & VoIP STIG.

There are ongoing testing efforts to certify the interoperability and security of VoIP technology. Any VoIP network element connected to any DSN switch poses a potential security risk to the entire network and should not be connected until interoperability certified by the DISA JITC and security certified for connection through the DISN Security Accreditation Working Group (DSAWG).

1.2 Scope

The scope of this STIG is the application of security and certain performance requirements pertinent to the infrastructure that supports IPT systems employing VoIP technologies. The focus of this STIG is on securing the technology, and not it's specific application within the DOD. DOD telephony requirements can be found in the *DSN STIG*. IPT is just one network centric application that is considered a real-time networking service. The scope of this STIG may be expanded in the future to include other real-time applications since they have similar requirements. One such application is IP based Video Tele-Conferencing (VTC).

Telecommunications system developers and vendors, in order to minimize "time to market" and system cost, as well as to add flexibility, are employing equipment and software that are general-purpose or multi-purpose in nature. Software applications are then developed that run on this foundation to provide the specific and unique functions that make up the vendor's product. Commonly used hardware "servers" and their associated OSs, as well as general-purpose web server and database programs add all of their well-known vulnerabilities to the product in which they are employed. Additionally, the data network forms a distributed switching network for the IPT/VoIP system. These systems therefore inherit all of the data network vulnerabilities. All of these inherited vulnerabilities must be mitigated and the system secured.

Other DOD STIGs focus on the base technologies that comprise the infrastructure on which IPT/VoIP systems rely. These other STIGs are to be used in conjunction with this STIG.

The following is a partial list of the available STIGs and technology categories:

Telecommunications; DSN
Network Enclave & Network Infrastructure (IP centric)
Network Operations Center (NOC) and Network Management (future)
Enterprise Systems Management (ESM)(future)
Secure Remote Computing (Remote network access for travelers and teleworkers)
OS
    Windows NT, 2000, XP, 2003 Server, Unix (includes Linux)
Applications
    "Large" Applications (server or mainframe based and workstation based)
    Desktop Applications (specifically Microsoft Office and Browsers)
    Database (specifically MS SQL, Oracle, and soon to include DB2)
    Web Server (specifically MS IIS, Netscape, and Apache and other web technology)
Domain Name System (DNS)
Wireless Networks

The target of this STIG is VoIP systems, networks, and other systems/devices that use commercially available IPT/VoIP solutions. This document does not cover every vendor's VoIP solution in use, or being considered for use, within the DOD, however, the guidance in this document is to be applied to the greatest extent possible to all IPT/VoIP systems and networks. Additionally, it is intended that the requirements in this STIG supplement the other OS and network STIGs so that a seamless security infrastructure can be maintained within the DOD enterprise. Guidance in this document is not intended to be all-inclusive, but rather a foundation for Network Administrators, Information Assurance Officers (IAOs), and Information Assurance Managers (IAMs) to use in securing their IPT/VoIP environments.

1.3 Authority

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

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

1.4 Writing Conventions

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

A reference that uses "**will**," indicate 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 makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

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

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

1.5 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.6 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.

Table 1-1. Vulnerability Severity Code Definitions

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.7.1 STIG Distribution to DSN Vendors

The STIGs, associated resources, and tools are produced for the purpose of securing DOD systems and are not intended for use by or distribution to the general public. Distribution is therefore restricted to DOD components or government agencies as well as their supporting contractors and vendors. Vendors in the process of having their products tested and certified for use by the DSN may obtain all related STIGs through their DOD sponsor, the VCAO, or the IATT. Additionally, vendors may contact the FSO Support Desk as noted above. When contacting FSO, the VCAO tracking number for the product or system will be needed to validate the request.

1.8 Document Revisions

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

This page is intentionally left blank.

2. IPT OVERVIEW

IPT/VoIP is a very different technology and uses a unique approach to providing voice services when compared to traditional circuit switched Time Division Multiplexed (TDM) based systems. Examples of these traditional systems are the Public Switched Telephone Network (PSTN) and the DSN. In this document, these will be referred to as the TDM DSN/PSTN.

2.1 VoIP Components

Some of the same component concepts that make up the TDM DSN/PSTN are also found in VoIP environments. VoIP networks must perform all of the tasks that these systems perform in addition to performing data and signaling gateway functions between these systems and IP networks. No matter which vendor solution, protocol, or architecture selected, there are certain VoIP components that must exist for the technology to function properly. Though different vendors may have different names for these components, there are four major components or functions that can be found in any VoIP environment, they are:

- The IP network
- Call processor/controllers
- Media/signaling gateways
- Subscriber terminals

2.1.1 IP Network

A network supporting VoIP technology can be viewed as one logical voice switch in distributed form (rather than a single switch frame) with the IP network providing connectivity to the distributed elements in the network. This IP infrastructure must ensure smooth delivery of voice and signaling packets to the VoIP elements. Due to their dissimilarities, the IP network must treat voice and data traffic differently, primarily because latency in voice transmission is more noticeable to the end user than latency in data transmission. If an IP network is to carry both voice and data traffic, it must be able to prioritize the different traffic types.

Some correlations can be made between VoIP and circuit-switching components; however there are many differences. A circuit-switched environment can be classified as a TDM network that dedicates channels and reserves bandwidth out of the trunk links interconnecting the switches. IP networks are different from circuit-switching networks, because they are packet-based and build on statistical availability of bandwidth. Quality of Service (QoS) is critical to providing acceptable VoIP implementations. The first step in establishing priority throughout the network is the marking of packets, which should be done at the first available point in the network. Some networking switches can mark packets for QoS purposes. QoS specifies a priority throughput level while Class of Service (CoS) ensures that packets of a specific application are marked for and treated with priority handling. This priority throughput and treatment is required for real-time VoIP applications to ensure that the voice service is less affected by other traffic flows. For the purpose of this STIG any IP network supporting IPT and VoIP technology will be referred to as a VoIP network.

2.1.2 Call Processor/Controllers

Call processor/controllers employ system software that sets up and monitors calls, maintains the dial plan, performs phone number translations, authorizes users, coordinates some or all of the call signaling, delivers basic telephony features, and may control the bandwidth utilization on each link. In addition, processor/controllers provide the signaling and control services that coordinate the media gateway functions. A call processor/controller can also be known as a soft-switch, call agent, call manager, or gatekeeper depending on its specific function in the VoIP network or specific vendor implementation. The amount of functionality provided by a call processor/controller is based on the particular VoIP product being deployed.

2.1.3 Media/Signaling Gateways

VoIP Gateways are responsible for interfacing IP network based voice communications with the traditional circuit-switched network. They provide call origination, detection, analog-to-digital conversion of voice, and creation of voice packets. In addition, media gateways may provide optional features, such as voice compression, echo cancellation, silence suppression, and statistics gathering. Gateways can exist in several physical forms including discrete device, a physical board or blade found in a dedicated telecommunications frame, or a common Personal Computer (PC) running VoIP software. The features and services provided by Media and Signaling Gateway's can span a wide spectrum; their functions can be divided into three key types:

- Media Gateway (MG) – The media gateway mediates the different signaling protocols between the IP network and the circuit-switched network. This gateway converts voice transported on the IP network using digital packet formats to analog or digital voice signals on the TDM DSN/PSTN side and vice versa. Simply stated, the MG provides single line or trunking functions that interface between the circuit-switched network(s) and a VoIP network. Typically the MG is used to provide access from a local VoIP system to the TDM DSN/PSTN. Additionally, specialized MGs can be used to interface vendor proprietary digital telephone instruments to the IP network.
- Signaling Gateway (SG) – This gateway type mediates the signaling functions between the IP network and the circuit-switched network. For instance, it may provide correlation between the VoIP signaling protocol on the packet network side and the Signaling System Seven (SS7) signaling on the TDM DSN/PSTN side.
- Media Gateway Controllers (MGC) – The media gateway controller communicates with both the MG and the SG, providing the call setup/teardown and processing functions required. This gateway type would use a dedicated protocol type such as the Media Gateway Control Protocol (MGCP) (discussed later) for inter-gateway communications functions.

One or all of the previously listed gateway functions could be employed at a given site depending on many factors, which includes the network architecture at that site. When implemented, these gateways might be distinct equipment suites, provided and/or administered by different organizations or entities. In addition, gateway functions may be implemented in a consolidated or distributed fashion. For example a VoIP network connected to TDM DSN/PSTN may use a SG controller to directly connect to the SS7 network, in addition to interfacing to internal VoIP network elements. This SG would be dedicated to the message translation and signaling needed to bridge the TDM DSN/PSTN to the VoIP network. In this example, a single system combining MG(s) and SG(s) could provide both the media and signaling gateway functions and interfaces between the VoIP network and traditional phone network.

2.1.4 Telephony (Subscriber) Terminal or Instrument

The IP phone is the user or subscriber's telephone instrument. This device provides real time, two-way communication with another compatible device. The IP phone may also offer other optional services such as data or video. The IP phone can come in the form of an actual hardware device, i.e., a telephone desk set, or in software forms i.e., a soft-agent or soft-phone, which resides on the user's desktop computer.

2.2 VoIP Standards and Protocols

As with any emerging technology, there are various standards that are being proposed as the best way to achieve industry acceptance. There are a variety of VoIP products and implementations providing a wide range of features that can currently be deployed. Two major standards bodies govern multimedia delivery (voice being one type) over packet-based networks.

- International Telecommunications Union (ITU)
- Internet Engineering Task Force (IETF)

There are several standards in place that deal with IPT implementations; however, the two major protocol-dependent approaches defined and under revision for VoIP signaling are: H.323 protocol (ITU-T) and Session Initiation Protocol (SIP)(IETF). Each protocol defines how the VoIP network architecture or technology implementation will look. Both standards facilitate audio, video and data communications and are in agreement with respect to media transfer. However, each standard uses somewhat different terminology and distinct methods for call signaling and call control. More importantly, they are not interoperable. In addition, many vendors use proprietary protocols such as the Nortel and AVAYA proprietary versions of the H.323 protocol, as well as Cisco's sub-set version called Skinny. Vendor specific solutions and their proprietary protocols will be addressed in future addendums to this STIG.

2.2.1 H.323 Protocol

This standard describes a centralized intelligence architecture that utilizes terminals, Gatekeepers, Gateways, and Multipoint Control Units (MCU) to provide multimedia communication over IP networks.

- Terminal - An H.323 terminal is a Local Area Network

- LANE - Local Area Network Endpoint (LANE) that provides two-way real-time communication. Examples of H.323 terminals are an IP-telephone or a PC-based virtual phone. An H.323 terminal can communicate with another terminal, a gatekeeper or an MCU. Terminals are capable of direct call completion with each other or of requesting the service from a gatekeeper.
- Gatekeeper - The gatekeeper provides call management functions within a local area. The local area or zone is made up of terminals, gateways and MCUs, which are all, managed by the gatekeeper. Gatekeepers manage calls, and perform signaling and authorization. The gatekeeper can be considered the coordinator of the H.323 network and is the focal point for all calls within the VoIP network. All terminals must check with the gatekeeper prior to processing a call. The gatekeeper gives permission to the terminal to proceed or signal the call setup on behalf of the terminal. The gatekeeper can also perform some of the functionality of the MGC described earlier in this document.
- Gateway - The gateway is used to connect the circuit-switched network to the IP network. It performs the interoperation functions of the signaling (SG) and media (MG) gateways.
- Multipoint Control Units (MCU) - The H.323 MCU provides conferencing capability. The MCU can be a stand-alone unit or incorporated into another H.323 component such as the gatekeeper.

2.2.2 Session Initiation Protocol (SIP)

Unlike H.323, SIP is not a complete protocol for multimedia communication. Instead, SIP works in harmony with other IP protocols to provide functionality similar to H.323. Contrary to H.323, SIP proscribes an architecture using a distributed intelligence that is composed of two types of entities: user agents, and network servers.

- User Agents (UA) - The user agent consists of two functionalities: User Agent Client (UAC) and User Agent Server (UAS). The UAC is used to initiate calls. The UAS responds to call requests. The UAC and the UAS can be located on the same device such as an IP-phone. SIP calls can be made directly to another UA, or through either the redirect server, or the SIP proxy.
- Network Servers - There are four types of SIP network servers, these are the registration server, location server, proxy server, and redirect server.
  - The registration server, in conjunction with a location server, maintains an inventory of UA locations within its domain. Proxy or redirection servers may consult the registration server so that incoming calls can be routed correctly.
  - The location server stores UA location or address information for multiple registration servers. This function is similar to a DNS server. The user initially reports their location to a registrar, which may be integrated into a proxy or redirect server. This information is in turn stored in the external location server.

- The proxy server handles SIP requests for the source UA. The proxy server intercepts outbound messages from endpoints or other services, contacts the location server to resolve the username into an address and forwards the message to the UA or another SIP server. If a destination SIP server receives the request, it forwards the request to the destination address of the UA being called.
- The redirect server performs the same resolution functionality as the proxy server, but the onus is placed on the end points to perform the actual transmission. That is, redirect servers obtain the actual address of the destination from the location server and return this information to the original sender, which then must send its message directly to this resolved address. The redirect server and the proxy server may be integrated.

2.2.3 Media Gateway Control Protocol (MGCP)

MGCP represents a joint cooperative effort between the ITU and the IETF. MGCP is considered complementary to H.323 and SIP, in that a MGC will control an MG using the H.248 (or Megaco protocol), but will communicate with other MGCs via H.323 or SIP. This protocol provides a scalable approach to manage media gateways in a diverse infrastructure.

2.3 VoIP Architectures

Currently, there are many vendors offering VoIP solutions. The end result to all of these offerings is the same, the transfer of voice traffic over a packet-switched network or non circuit-switched medium. However, the manner in which this end result is achieved can be very different from solution to solution. Some vendor offerings embrace a hybrid or IP enabled design utilizing some of the facilities and services of an existing telephone switch (TDM type), while others are based on a pure IP or IP centric architecture wherein IPT system only trunks into the local TDM DSN/PSTN telephone switch.

2.3.1 IP Centric

An IP Centric VoIP architecture is designed around an IP based core-switching system. These solutions have distributed IP devices that function together to perform the functions of a TDM based circuit-switch (see Figure 2.1). In an IP centric solution, the connectivity to the rest of the switched network (i.e., TDM DSN/PSTN) is accomplished via a dedicated trunk (i.e., a T1/E1, or Integrated Services Digital Network (ISDN)) equivalent; the Primary Rate Interface (PRI)).

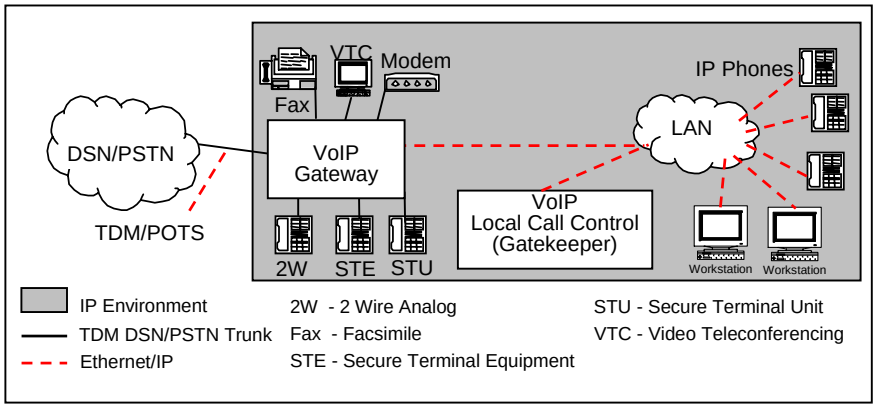

Figure 2-1. Illustration of IP Centric Architecture

2.3.2 IP Enabled

IP enabled architectures are considered hybrid solutions. By design an IP enabled solution incorporates the services and facilities of a traditional TDM based circuit-switch while providing VoIP terminals to the end subscriber. As depicted in Figure 2-2, this solution has a TDM based circuit-switch that provides the core call processing and switching of all calls. In addition, the same TDM switch provides the ability to use either traditional analog / digital telephony instruments or IP phone instruments to provide similar subscriber line functions. The DSN/PSTN interface (T1/E1, PRI, etc) is provided via the TDM based circuit-switch. An integrated Ethernet interface provides connectivity to the IP Local Area Network (LAN) supporting the IP Phones.

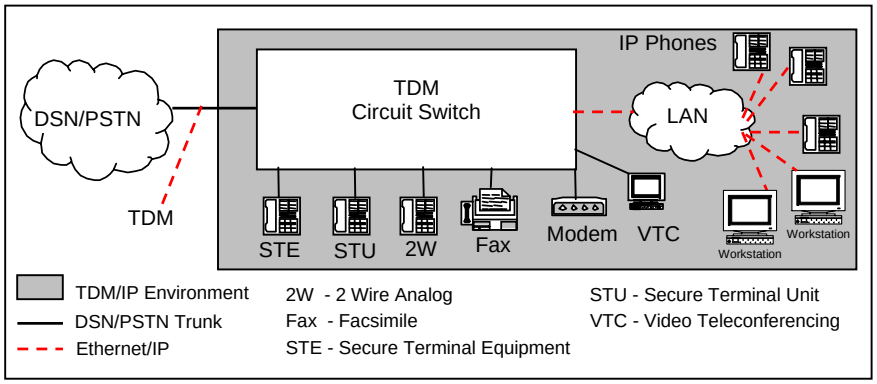

Figure 2-2. Illustration of IP Enabled (Hybrid) Architecture

2.3.3 VoSIP, SVoIP, and SVoSIP

IPT and VoIP are being implemented in new ways to enhance the security of communications within the DOD and to enhance availability and flexibility. New terms are being used for these new implementations. We will discuss these more fully along with their security requirements in subsequent releases of this STIG. The following is a list of the terms and their capabilities.

- Voice over Secure IP (VoSIP)
  - VoIP implemented on a "secured" (typically classified) IP network. VoSIP relies heavily on the security applied to the network primarily for confidentiality outside of the local enclave. Additional security measures as discussed in this STIG are required to secure the VoIP system itself.
  - Security applied at the Network Layer using legacy type 1 link encryption or High Assurance IP Interoperability Specification (HAIPIS)
  - Provides System High security within security domain
  - Provides confidentiality across a black network
  - Provides Traffic Flow Security (TFS) across a black network
  - Confidentiality within a security domain is not supported (not End-to-End)
- Secure Voice over IP (SVoIP)
  - VoIP that provides type 1 encrypted communications end to end.

- Security (encryption for confidentiality) is provided at the Application layer using Secure Communication Interoperability Protocol (SCIP) (formerly known as Future Narrow Band Digital Terminal (FNBDT)) devices. The encryption is typically Type 1; however, SCIP/FNBDT devices can use other crypto methods and libraries such as AES.
- Talker-to-listener security
- Can transition through black PSTN Gateways
- Provides session-unique security levels
- Interoperability with Legacy Secure Voice systems (Secure Telephone Unit (STU) & Secure Terminal Equipment (STE))

o Secure Voice over Secure IP (SVoSIP)
- SVoSIP is the use of SVoIP devices on a VoSIP network.
- Security (confidentiality) provided at both the application and Network layers using HAIPIS + FNBDT
- Confidentiality within HAIPIS domain (End-to-End on top of System High)
- Independent negotiations can permit interoperability with FNBDT only and HAIPIS only systems

2.4 VoIP Environmental Vulnerabilities

Since VoIP, in most environments, likely operates on a converged (voice, data, and video) network, VoIP information is susceptible to the same threats and therefore inherits all the vulnerabilities associated with that data network. This section identifies some of the general network (IP based) threats as they apply to VoIP technology.

2.4.1 Sniffing

Sniffing can result in eavesdropping, disclosure of confidential information or unprotected user credentials, and the potential for identity theft. It allows malicious users to collect information about the network and VoIP system that can be used to mount an attack on it, as well as other systems, and/or data that might not otherwise be vulnerable. VoIP networks differ from circuit-switched networks because the voice information is sent over commonly accessible pathways available to all subscribers connected to the network. Subscribers in a circuit-switched network must modify the network or add an instrument to the network to be able to listen-in on a single call at a time. Subscribers in a VoIP network have access to all calls that are transported by their portion of the network. Any of these calls may be listened to by sniffing the network and sorting out the collected data by address and playing it back. All the tools needed for VoIP sniffing, including H.323 and SIP plug-ins for packet sniffers, are available on open source web sites. Administrators should not assume that special diagnostic equipment is needed to intercept VoIP conversations the way it is for proprietary digital TDM systems. Any signal that is not protected by encryption or other means must be assumed to be accessible to an adversary, possibly without the direct physical access required to compromise a traditional circuit-switched conversation.

2.4.2 Denial of Service (DoS)

DoS attacks can take many forms and be accomplished using various methods. One of these is overloading the network with unnecessary data resulting in taking the network down. The traditional system (separate data and voice networks) allows an organization to still communicate when the data network is unavailable. With the implementation of VoIP in a converged network, a DoS attack against the data network could also be very effective against the VoIP system taking into consideration the QoS necessary for VoIP to be effective. Other methods of creating a DoS for the VoIP network or instruments can include sending malformed packets or spoofed commands to instruments. One example of a spoofed command DoS attack could be the sending of repeated call termination commands to one or more instruments.

2.4.3 Traffic Flow Redirection

Since data packets do not flow over a dedicated connection for the duration of a session, an adversary could manipulate the routing of packets and thus cause delay in certain paths forcing the packets to take a path chosen by the adversary. This results in two noticeable vulnerabilities. The first vulnerability enhances the sniffing vulnerability because an adversary could predict a preferred location to place a sniffing device. The second vulnerability enhances the DoS vulnerability. When this attack is applied to a VoIP network, the QoS may be diminished to a noticeable level, possibly rendering VoIP ineffective.

2.4.4 Additional Vulnerabilities

There are many more vulnerabilities associated with this new technology (VoIP and IPT). We have only touched on a few of them above. System manufacturers and designers have generally focused on developing feature rich systems and have sidestepped security or have tried to apply security as an afterthought. Some of the vulnerabilities that will be discussed in a future release of this STIG are Man in the middle attacks and Audio Interception/Capture

This page is intentionally left blank.

3. SECURING THE VOIP ENVIRONMENT

A future expectation is that long-established security features (i.e., authentication and encryption) will be integrated into VoIP standards. However, today many existing data-centric security technologies can be utilized to enhance security in the VoIP environment. VoIP network security includes voice-packet security, which focuses on application concerns, while IP security focuses on transport or network security. Controlling security at these levels of the VoIP environment may require network re-design and/or re-engineering which will affect the architecture of the network supporting the VoIP environment. Some specific issues need further attention when a VoIP system is deployed. This section addresses these types of concerns and should be taken into consideration where technically feasible in order to deploy VoIP in a secure manner. It is important to remember that securing any network is a continual process that requires staying abreast of the latest vulnerabilities that may exist in network infrastructure components, server operating systems, and applications deployed throughout the enterprise.

The following VoIP Logical Security Architecture diagram (Figure 3-1) depicts a generic site with VoIP technology applied. This diagram can be used as a reference when considering the implementation of security requirements contained in this document.

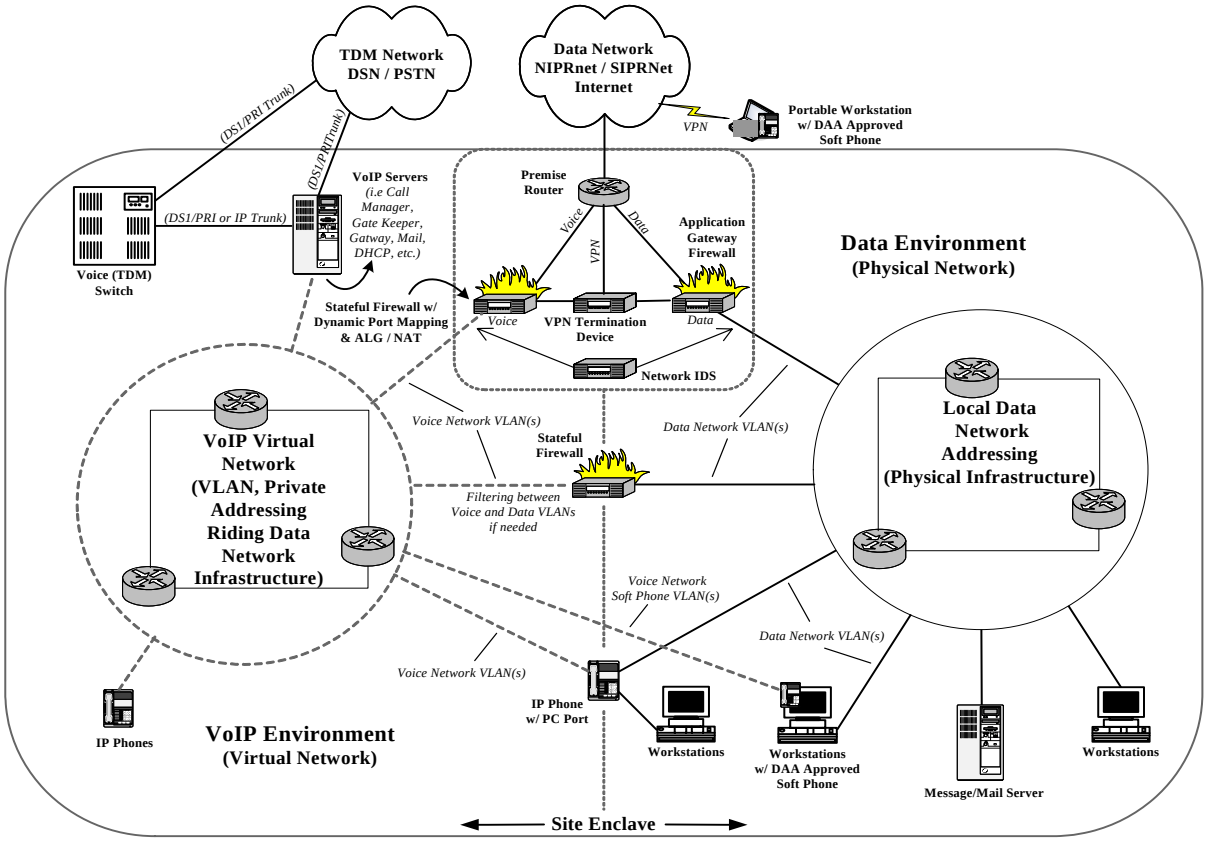

Figure 3-1. VoIP Security Architecture – Logical Diagram

The design of the network supporting the VoIP environment is of great concern. Planning an IPT/VoIP implementation must include the network infrastructure to which the IPT system will be added. Networks need to be robust when it comes to bandwidth, reliability, survivability, and prioritization. Inadequate network design could inherently induce vulnerabilities for DoS situations.

Networks supporting IPT must:

- Possess enough bandwidth capabilities to support the planned voice traffic in addition to the expected data traffic
- Include redundancy of equipment and connections above the access layer to support survivability in the event of a equipment or link failure
- Possess adequate backup power to maintain system operation (including instruments) for a predetermined time period based on the system's mission criticality.
- Employ a consistent network wide QoS / CoS mechanism, to include 802.1P and 802.1Q tagging

Installed networks may have to be upgraded or replaced when adding IPT to the network. Design requirements for networks supporting DOD IPT/VoIP implementations can be found in the DOD Generic Switching Center Requirements (GSCR) document in Appendix 3. This Appendix contains the specifications for a Command and Control Voice Grade LAN (C2VG LAN) required to support DOD IPT. The following requirements apply to the network foundation for IPT systems:

- *(VoIP0020: CAT II) The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is configured to comply with the Network Infrastructure and Enclave STIGs.*

- *(VoIP0025: CAT III) The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is designed and implemented as a DOD C2VG LAN and will possess bandwidth, reliability, survivability, and prioritization capabilities in accordance with the DOD GSCR, Appendix 3.*

- *(VoIP0030: CAT III) The IAO will ensure that VoIP systems / devices are added to site System Security Authorization Agreements (SSAAs).*

- *(VoIP0035: CAT II) The IAO will ensure that VoIP systems are compliant with the DSN STIG. Specific emphasis to be given in the following areas:*

    - *System certification, accreditation, and listing on the DSN APL in accordance with the DODI 8100.3*
    - *Site administrative requirements*
    - *Requirements for management of voice systems and management interfaces.*
    - *This list is not all-inclusive.*

3.1 Protecting VoIP Critical Servers

For the purpose of this document a VoIP critical server is any server directly supporting the VoIP environment. Unlike a regular PC or print server on the network VoIP servers represent mission critical equipment that contain potentially sensitive information that needs to be secured and treated with the same precautions as any other server containing sensitive information. VoIP systems provide powerful management features, which can tag logged calls in many ways to help in future retrieval. Placement of VoIP servers is critical to securing the voice-processing environment. These system components should reside on a separate network segment protected by a VoIP aware firewall. Implementation of this recommendation is discussed at length in the following sections. Dedicating and securing critical VoIP servers is key in securing the IPT environment. Some vendors provide IPT services on their own proprietary OSs while others provide these services on standard UNIX and Microsoft Windows OS based systems. Most known vulnerabilities exist on UNIX and Windows based operating systems. Therefore, the securing of these voice processing and signaling platforms, to include their installed applications, is vital in protecting the VoIP environment from malicious attack. In addition, to minimize possible risk these servers will be dedicated to the IPT applications required for VoIP operations.

- *(VoIP0270: CAT II) The IAO will ensure that VoIP servers are dedicated to only applications required for VoIP operations.*

- *(VoIP0280: CAT III) The IAO will ensure that critical VoIP servers have been secured in compliance with all applicable STIGs (i.e., UNIX, Microsoft NT/Win2K, database, web, etc.).*

3.1.1 Vulnerability Management

Vulnerabilities are discovered every day that apply to general-purpose operating systems and applications used as the basis for IPT systems. The vendors of these general-purpose systems and applications (such as Microsoft and others) routinely provide patches for their products. The DOD IAVM process mandates that the Information Assurance Vulnerability Alerts (IAVAs) for these vulnerabilities be addressed in a specific time frame. Users of IPT systems must be cautioned against applying patches to their systems that are provided by the original vendor of the general-purpose operating systems and applications used in their IPT systems as these may adversely affect the operability of the system. This is partially because IPT and Non-IPT telecommunications system vendors usually customize or use only portions of the general-purpose operating systems and applications. All patches to telecommunications systems and the underlying software must originate with the manufacturer of the telecommunications system.

- *(VoIP0281: CAT II) The IAO will ensure that software patches for critical VoIP servers and other IPT devices originate from the system manufacturer and are applied in accordance with manufacturer's instructions.*

- *(VoIP0282: CAT II) The IAO will ensure that all IAVAs applicable to the general-purpose systems and applications used in VoIP systems are referred to the system manufacturer for approval and patch distribution in order to maintain timely IAVA compliance.*

3.2 Physical Security

The Physical Security of the network components supporting the VoIP environment is of great concern. Routers, Ethernet switches, telephony gateways and servers define VoIP network boundaries and can act as interfaces to other networks. These network devices can provide both the logical and physical connectivity of the entire enterprise network and should be considered a target to be defended against attackers. To prevent unauthorized physical access to these types of devices, measures must be taken to ensure their protection. These precautions include but may not be limited to restricting access to server rooms and network-wiring closets to only trusted authorized personnel.

- *(VoIP0050: CAT II) The IAO will ensure all critical VoIP network and server components are located in physically secured areas. This does not apply to end instruments.*

3.3 Protection of System and Instrument Configuration

Many VoIP telephone instruments have the capability of setting and/or displaying configuration settings in the instrument itself. While this makes it convenient to configure and troubleshoot at the desktop, it presents a vulnerability whereby a user or anybody in the area can obtain information, such as the IP addresses of system components that could be used to facilitate an attack on the system. All access to configuration information and settings must be password protected. Furthermore, the password should authenticate remotely and follow DOD complexity requirements.

- *(VoIP0060: CAT III) The IAO will ensure that IPT terminals (VoIP phones or instruments) cannot be configured at the terminal and do not display network/terminal configuration information on their display without the use of a password.*

- *(VoIP0061: CAT III) The IAO will ensure that the IPT terminal's configuration/configuration-display passwords authenticate remotely to the IPT system controller.*

- *(VoIP0062: CAT II) The IAO will ensure that a policy is in place to ensure that the IPT terminal (VoIP phone or instrument) configuration and display password is managed IAW DOD password policies (e.g., password complexity, expiration, reuse, protection and storage).*

3.4 VoIP Instrument/Terminal Registration

Traditional telephone systems require physical wiring and/or switch configuration changes to add an instrument to the system. This makes it difficult for someone to add unauthorized digital instruments to the system. This, however, could be done easier with older analog systems by tapping an existing analog line. With VoIP, this is no longer the case. Most IPT/VoIP systems employ an automatic means of registering a new instrument on the network with the call management server and then downloading its configuration to the instrument. This presents a vulnerability whereby unauthorized instruments could be added to the system or instruments could be moved without authorization. Such activity can happen anywhere there is an active network port or outlet. This is not only a configuration management problem but it could also allow theft of services or some other malicious attack. It is recognized however, that auto-registration is necessary during large deployments of VoIP terminals, as well as a short time thereafter, to facilitate additions and troubleshooting. This applies to initial system setup and to any subsequent large redeployments or additions. Normal, day to day, moves, adds, and changes will require manual registration. Since, it may be possible for an unauthorized VoIP terminal to easily be added to the system during auto-registration, the registration logs must be compared to the authorized terminal inventory. Alternately the system could have a method of automatically registering only pre-authorized terminals. This feature would support VoIP terminals that are DAA approved for connection from multiple local or remote locations.

- *(VoIP0065: CAT II) The IAO will ensure that auto-registration of VoIP terminals is disabled within 5 days following initial system setup and/or following any subsequent large redeployments or additions.*

- *(VoIP0066: CAT II) The IAO will ensure that an inventory of authorized instruments is documented and maintained.*

- *(VoIP0067: CAT II) The IAO will ensure that the VoIP system only registers authorized terminals. This can be through an automated authorization process during auto-registration or by comparing the registration logs to the documented authorized inventory following any usage of auto-registration.*

- *(VoIP0068: CAT II) The IAO will ensure that manual registration of VoIP terminals is used for normal, day-to-day, troubleshooting and repairs, or moves, adds, and changes.*

3.5 Local Enclave Data and Voice Network Segregation

VoIP networks increasingly represent high-value targets for attacks and represent a greater risk to network security than most other network applications; hence, it is imperative that the voice network and supporting data network(s) be secured as tightly as possible to reduce the impact that an attack can have on either network(s). Segregating voice traffic from data traffic greatly enhances the security and availability of all services. Further subdivision of the voice and data networks can further enhance security.

Achieving the ideal security posture for voice and data would require two physically separate and distinct networks (including cable plant), much as is the case with traditional voice and data technologies. Although this might be considered for the most demanding security environments, it works against the idea of convergence and the associated cost savings expected by having one network (and cable plant).

While cost is not the point of this document, it should be noted that the cost of a converged network capable of supporting highly reliable voice on a data infrastructure might in fact cost as much or more than the older traditionally separate networks. The reasoning behind this statement is that while there can be savings realized in the cable plant, in some cases, (by requiring only one cable for both voice and data) the network equipment and supporting facilities may have to be upgraded to support VoIP. Facility upgrade concerns would include telecom room (old term "closet") size increases, along with increased air conditioning, and power capacity. While these costs can best be addressed in a "green-field" installation, they can still be high.

Logical segregation of VoIP components and data components can be accomplished at both layer 2 using Virtual Local Area Networks (VLANs) and layer 3 using IP addressing.

While these methods, in themselves, are not designed as security mechanisms, they do provide a derived security benefit by easing management of filtering rules and obfuscating or hiding addresses and information that an attacker could use to facilitate an attack. Separation may also prevent an attack on one network from impacting the other. These methods make it harder for an attacker to be successful and help to provide a layered approach to VoIP and network security.

Segregating data from telephony by placing VoIP servers and subscriber terminals on logically separate IP networks and logically separate Ethernet networks while controlling access to these VoIP components through filters will help to ensure security and aid in protecting the VoIP environment from external threats. In addition, further subdivision of those components is necessary to protect the telephony applications running across the infrastructure.

3.5.1 IP Address Segregation

Layer 3 address segregation is the first layer in our layered defense approach to VoIP security. It allows the use of switches, routers, and firewalls with their associated access lists and other processes, to control traffic between the components on the network.

To provide address segregation, best practices dictate that all like components will be placed in like address ranges. Therefore VoIP components (i.e., Gatekeepers, Call Managers, voice mail systems, IP Subscriber Terminals etc.) will be deployed within their own, separate private IP network, logical sub-network, or networks. Where possible, non-routable RFC 1918 "private" IP address space will be used (10.x.x.x, 172.16.x.x, and 192.168.x.x). This sub-network(s) will use a different major address range than is deployed on the local data network(s), (which typically also uses "private" address space), to further separate IPT from the data network. This will help to reduce the chances of voice traffic traversing outside the telephony network segment and vice versa for data traffic. The use of RFC 1918 IP address space has the effect hiding the VoIP components from the WAN, and making them non-routable as a destination across the Internet (or NIPRNet).

Additionally, when using Dynamic Host Configuration Protocol (DHCP) for address assignment, different servers will be used for voice components and data components. That is to say that a DHCP server serving VoIP devices needs to be in the VoIP domain i.e., same address space.

- *(VoIP0070: CAT II) The IAO will ensure that all VoIP systems and components are deployed on their own dedicated IP network(s) or sub-network(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.*

- *(VoIP0080: CAT III) The IAO will ensure that all local VoIP systems and components are deployed using private address space IAW RFC 1918. This is not a finding for DAA approved VoSIP systems residing on secured networks, such as the SIPRNet, where RFC 1918 addressing is not permissible for reasons of accountability or policy.*

- *(VoIP0082: CAT II) The IAO will ensure that when using DHCP for address assignment, different servers are used for voice components and data components. Additionally, the IAO will ensure that these servers will reside in their respective voice or data address space.*

- *(VoIP0085: CAT III) The IAO will ensure that all VoSIP systems and components residing on the SIPRNet utilize address blocks assigned by the DRSN VoSIP PMO.*

3.5.2 Local Network Voice / Data Segregation Using VLANs

An IPT system is built on an IP infrastructure based on layer 2 and layer 3 switches and routers, which comprise the network's access and distribution layers respectively. The layer 2 switches found at the access layer provide high port density for both host and IP phone connectivity as well as layer 2 services such as QoS and VLAN membership. (It should also be mentioned that some access layer switches can also do layer 2 and 3 filtering.) Guidelines and requirements for securing access layer devices including any associated cross-connect hardware can be found in the Network Infrastructure STIG.

Layer 2 network segregation is the second layer in our layered defense approach to VoIP security. Voice traffic must be isolated from data traffic using separate physical LANs or Virtual LANs. The combination of data and voice segregation and segmentation using VLANs along with a switched infrastructure strongly enhances the security posture of the system. This will also help to mitigate call eavesdropping and other attacks.

3.5.2.1 Voice VLAN(s)

VLAN technology has traditionally been an efficient way of grouping users into workgroups to share a specific network address space and broadcast domain regardless of their physical location on the network. Hosts within the same VLAN can communicate with other hosts in the same VLAN using layer-2 switching. In order to communicate with other VLANs, traffic must go through a layer 3 device where it can be filtered and routed. VLANs can offer significant benefits in a multi-service network by providing a convenient way of isolating IPT equipment and traffic from the data equipment and traffic. When VLANs are deployed, excessive broadcast and multicast packets present in the normal data traffic will not disrupt IPT services.

As with data networks, IPT equipment and instruments should be logically grouped using multiple VLANs such that IP Phones share their VLANs only with other IP Phones, gateways with like gateways, and so on. Each type of VoIP device would have mutually exclusive VLANs. This forces layer 3 routing and thereby enables all the filtering capabilities of the layer 3 devices. Additionally, each server type should have its own VLAN. Private server VLANs would prevent a compromised server from attacking another server on the same VLAN at layer two. Since all the devices on any given VLAN would have the same Layer 2 though 4 (at least) characteristics the filtering rules become easier to develop, deploy, and manage. These groupings of IPT devices should be as follows:

- Call processing and voice DHCP servers
- Directory servers
- Message servers and/or servers that might be accessed from both the data network and the VoIP network.
- Gateways – possibly multiple VLANs for multiple types of gateways
- WAN Access firewalls
- VoIP phones with possible subdivision by department or organization
- Data workstations with soft phones.
- VoIP device management

- *(VoIP0100: CAT II) The IAO will ensure that the local network supporting IPT implementations (i.e., the underlying data network) is configured using VLANs, and that at a minimum, one voice VLAN has been configured to segregate voice traffic from data traffic.*

- *(VoIP0101: CAT III) The IAO will ensure that the voice network is subdivided into multiple VLANs to segregate VoIP devices by type and function. At a minimum, this shall include five VLANs containing the following as might be applicable: call control servers, message servers (voice-mail, e-mail, unified), gateways, VoIP phones, and workstations with soft phones.*

- *(VoIP0102: CAT II) The IAO will ensure that servers or devices that are to be accessed from both the voice and data networks (i.e., message servers or workstations with soft phones) reside in their own protected VLANs. Mutually accessible servers may be placed in the DMZ of a dedicated stateful firewall placed between the voice and data networks per voice/data network protection requirements.*

- *(VoIP0103: CAT II) The IAO will ensure that the local network's VLANs are implemented in accordance with the VLAN section of the Network Infrastructure STIG.*

To implement the network segmentation as discussed in the previous section, all IP phones, workstations, and servers providing voice services must be connected to switchports with membership only to one or more "voice" VLAN(s) (i.e., voice VLAN, auxiliary VLAN, VVID, 802.1Q tagged, etc). Additionally, IP phones typically provide a data port or ports so that a PC / workstation, or other Ethernet device, can connect to the phone. The phone then connects to the switchport at the access layer switch. This provides the simplicity of a single physical Ethernet connection for both the IP phone and the attached workstation. With this configuration, it is critical that the data and voice segmentation model is implemented using only IP phones that support 802.1Q VLAN trunking. With a trunk, the voice traffic can be isolated from other data, providing security and QoS capabilities. For IP phones that do not support 802.1Q VLAN trunking both voice and data must be combined over the single VLAN; hence, there is no method to segregate the voice and data traffic at the switch therefore the PC port must be disabled.

- *(VoIP0105: CAT II) The IAO will ensure that IP phones (that do not contain a multi-port switch), and servers providing voice services are connected to switchports with membership only to the voice VLAN(s). Additionally, the IAO will ensure that data workstations (without approved Soft Phones) are connected to switchports with membership only to the data VLAN(s).*

- *(VoIP0110: CAT II) The IAO will ensure that all IP phones containing a multi-port switch for connecting external devices such as a workstation, utilize 802.1Q trunking to separate voice and data traffic or have the data port(s) disabled.*

- *(VoIP0111: CAT II) The IAO will ensure that all access switch ports supporting IP phones that contain a multi-port switch route voice and data traffic to their respective VLANs.*

Guidelines and requirements for segregating management and control plane traffic as well as securing Ethernet access and trunk links can be found in the Network Infrastructure STIG.

Guidelines and requirements for traffic control between VLANs are discussed later in this document.

3.5.2.2 Voice VLAN Access

Eliminating unauthorized access to the network from inside the enclave is vital to keeping the voice infrastructure secure. Unauthorized internal access leads to the possibility of curious insiders or disgruntled employees gaining control of network resources, eavesdropping, or inflicting denial-of-service on the voice network. Simply connecting a workstation, laptop, or IP phone to a wall plate, access point, or another IP phone located in the work area may enable internal access to the local data network and possibly the voice sub-network. Best practice for a VLAN-based network is to place all disabled ports into an unused VLAN; thereby thwarting unauthorized VLAN access using both physical and logical barriers. In addition, unused data ports on IP phones with a multi-port switch capable of connecting another network device must be disabled if not in use.

Once a user or device has connected to the network, services that the client has access to should be based on individual need—and only if that individual or workstation is authorized. This restriction can only be implemented by first determining if the individual, workstation, or IP phone is authorized to connect to the network and then insuring that it is assigned to the appropriate VLAN. Several methods used today for authenticating layer-2 access and VLAN membership are as follows:

- Port security
- Port authentication with 802.1X
- VLAN Management Policy Server (VMPS)

Port Security - Unauthorized relocation of an IP telephone allows unauthorized users to send and receive calls. The use of MAC security will greatly reduce the risk of a user connecting an unauthorized device (maliciously or otherwise) to the voice VLAN and receiving service—or denying service to others. The port security feature provided by most switch vendors can be used to block input to a switchport when the MAC address of the station attempting to access the switchport does not match any of the MAC addresses specified for that switchport—that is, those addresses statically configured or auto-configured (i.e., “learned). You can configure the port to shut down permanently, shut down for a specified time interval, or drop incoming packets from the insecure host if a violation occurs.

When you enable port security on a switchport that has membership to the voice VLAN, you must set the maximum allowed MAC addresses that can be dynamically configured on the switchport to no more than what is necessary for the specific configuration. IP phone configurations with a multi-port switch that enables a PC connection would require two or more allowable MAC addresses. Some IP phones allow for multiple external Ethernet connections. The number of allowable connections must be calculated and each allowable MAC address accounted for.

Port Authentication with 802.1x - Authentication through 802.1x provides the ability to limit network access based on a client profile. A client profile typically contains the client identification and access privileges. 802.1x allows a client to be recognized, authenticated, and granted access privileges from wherever he or she logs-on to the network. However, currently IP phones do not support 802.1x; thus, there is no way to authenticate the phone or the user of an IP phone with this technology. For IP phone configurations with a multi-port switch that enables a PC connection, the downstream PC and its user can be authenticated. However, voice VLAN-tagged packets will always be received and forwarded by a switchport that is configured for 802.1x authentication—regardless of the authorized or unauthorized state of the switchport.

VLAN Management Policy Server (VMPS) - VMPS allows a switch to dynamically assign VLANs to users based on the workstation's MAC address or the user's identity when used with the User Registration Tool. A switch is configured and designated as the VMPS server while the remainder of the switches on the segment act as VMPS clients. When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping. Because of the risks associated with several VMPS vulnerabilities, this technology must not be used for access layer authentication.

Additional guidelines for VLAN access, port security, port authentication, and a discussion on VMPS vulnerabilities can be found in the Network Infrastructure STIG.

- *(VoIP0120: CAT III) The IAO will ensure that all unused ports are disabled and are placed in an unused VLAN.*

- *(VoIP0122: CAT III) The IAO will ensure that all IP phones with a multi-port switch have the data port disabled if a PC is not normally attached.*

- *(VoIP0125: CAT II) The IAO will ensure that port security is configured on all switchports with voice VLAN membership.*

- *(VoIP0127: CAT II) The IAO will ensure that the maximum number of MAC addresses that can be dynamically configured on a given switch port is limited to that which is required (i.e., 1 – 3).*

3.6 IP Soft Phones

The use of Soft Phones is highly discouraged. Exceptions may be made in special situations with DAA approval. Special consideration must be given these situations and additional configuration requirements applied. IP Soft Phone agents inherently reside in a data segment but require access to the voice network in order to access call control, place calls, and leave voice messages. Soft Phones are not as resistant to attack as hardware phones. Soft Phone hosts (desktop PCs) are more vulnerable to attacks due to the greater number of possible entries into the system. These entry mediums include the OS, resident applications, and enabled services all of which could be vulnerable to worms, viruses, etc. In addition, since the Soft Phone resides on a data segment, it is susceptible to any attack against that segment and not just the host itself. In contrast, IP hardware phones can reside in a protected VoIP segment and run proprietary OSs, and with limited network services enabled they are less likely to have vulnerabilities. Because the deployment of Soft Phones provides a conduit for malicious attack against the voice segment, these phones pose great risk to the VoIP environment.

It is recognized that the use of Soft Phones is advantageous under specific circumstances. These might be in support of tactical desktop convergence, or call centers. While such uses as providing convenience for traveling personnel or teleworkers, might be desirable, these pose significantly more risk due to the un-controlled areas and networks from which they may connect. These cases should be given additional scrutiny and avoided if at all possible. The use of Soft Phone agent software must be controlled and used only after DAA approval. The DAA must be made aware of the security risk to the enclave that he/she will be accepting. In addition, any VoIP traffic to and from Soft Phone clients that have been independently installed and configured by an end user for personal use is prohibited within any DOD information system.

- *(VoIP0130: CAT II) The IAO will ensure that written DAA approval is obtained prior to the use of any IP Soft Phone agent software. The IAO will maintain documentation pertaining to such approval for inspection by auditors.*

- *(VoIP0135: CAT III) The IAO will ensure a local IP Soft Phone policy exists and is being enforced that addresses the following:*

    - *Prohibits the installation and use of IP Soft Phone agent software on workstations (fixed or portable) intended for day-to-day use in the users normal workspace.*
    - *Prohibits the use of IP Soft Phone agent software in the users normal workspace, which has been approved and installed on a portable workstation for the purpose of VoIP communications while traveling.*
    - *Prohibits the installation and use of IP Soft Phone agent software clients that are independently configured by end users for personal use or that is provided by commercial IPT service providers.*
    - *Requires prior justification and DAA approval for the use of any IP Soft Phone agent software.*
    - *Requires that the justification and DAA approval of IP Soft Phone agent software use is reviewed annually and approval renewed if justified.*

- *(VoIP0140: CAT II) The IAO will ensure that host systems (i.e., workstations), on which Soft Phones are installed, comply with all applicable STIGs including but not limited to: OS, Application, Desktop Application.*

- *(VoIP0150: CAT III) The IAO will ensure that if/when approved Soft Phones are used in the LAN, the following conditions are met:*

    - *The host computer contains a Network Interface Card (NIC), (commonly called a network adaptor) that is 802.1Q (VLAN tagging) and 802.1P (Priority tagging) capable.*
    - *The host computer, NIC, and IP Soft Phone agent software is configured to use separate 802.1Q VLAN tags for voice and data.*
    - *Alternately, dual NICs may be used where voice traffic is routed to one NIC and data traffic is routed to the other. Each NIC is connected to an access switch port residing in the appropriate VLAN.*
    - *The host computer will be connected to separate voice and data VLANs that have been created expressly for the Soft Phone host(s). That is to say that the LAN should have a voice VLAN and a data VLAN dedicated to hosts with IP Soft Phone agents installed.*

- *(VoIP0160: CAT II) The IAO will ensure that if/when approved Soft Phones are used in remote connectivity situations, the following conditions are met:*

    - *The host computer connects to the "home LAN" through a Virtual Private Network (VPN) connection.*
    - *The VPN is terminated at the enclave boundary in accordance with the Enclave STIG*
    - *The voice and data traffic is routed appropriately to separate voice and data VLANs in the "home LAN"*
    - *The IP Soft Phone agent connects to the Call Manager on the "home LAN" through the VPN using "home LAN" IP addressing.*

- *(VoIP0165: CAT II) The IAO will ensure that, if/when approved Soft Phones are used in a call center situation; the call center network is configured as a separate enclave and secured in accordance with all applicable STIGs.*

3.7 Network Protection And Traffic Control

Networks and the data they transport must be protected from attack and disclosure from internal and external threats. Networks are segmented and boundaries are implemented for this reason. There is however a need for communication between these segments or enclaves. Such communications traffic must be controlled so that the network and data is protected.

Network connections may be required between the voice and data LAN segments or VLANs in order to provide services such as voice mail and other messaging services. The voice and data VLANs can be considered enclaves for the purpose of this discussion. The problem is exacerbated by the use of Soft Phones on workstations. Additionally, there is a need to provide connections between the voice LAN and the Wide Area Network (WAN) to allow calls to be placed to phones external to the enclave or for calls to be placed from outside the enclave to phones that are internal. The following sections will discuss how the required protections should be implemented.

3.7.1 Local Voice to Data Network and VLAN to VLAN Protection

An attacker from the data VLAN can easily overwhelm the voice VLAN if proper protections are not in place. Furthermore, IPT servers are vulnerable to attacks from within the local network as well as from the outside. Filtering of traffic between the data and voice VLANs is imperative to provide security to these servers and to ensure continuous availability of all voice network services.

Firewalls, routers, and switches should be implemented in a manner that will compartmentalize the VoIP network and servers from unauthorized access. Protection must be provided between the various voice VLANs as well as between the voice VLANs and the data VLAN(s). This is necessary to limit and control access from the data network to the voice network and control traffic flow between the voice VLANs. Ideally there should be no traffic flow between the voice VLAN(s) and the data VLAN(s) except in specific situations. These situations might occur when an approved device on the data VLAN needs to access the VoIP servers or when VoIP phones on the VoIP VLAN need to access a device on the data VLAN. Such traffic should be limited, nevertheless. An example of a connection that may be allowed would be between the voice mail server in a voice VLAN and the email server in a data VLAN. The management VLAN may also need access to the voice VLAN and vise versa.

If there is to be any data traffic between the voice and data VLANs, packet filtering must be implemented through an internal firewall or minimally by configuring ACLs in the Layer 3 switches or routers, limiting both ports and addresses that can have access to and from the voice VLAN(s). Such traffic should be limited to traffic sourced from the voice VLAN.

Voice traffic between the voice and data VLANs must be controlled through the use of a stateful inspection firewall. This firewall can be a dedicated internal firewall or can be an additional function of a dedicated enclave boundary VoIP firewall. The requirements for VoIP firewalls are discussed in a later section of this document.

Traffic flow between the various voice VLANs must be controlled through the use of ACLs in a stateful inspection firewall or in the layer 3 switches or routers in the network. These filters will allow the traffic to flow between the VLANs in an approved or planned manner. Anomalous traffic will be blocked. An example of approved traffic flow would be between an IP phone and another IP phone, the call controller, gateway, or supporting directory or message servers. An example of anomalous traffic could be any traffic using ports or protocols that are not used for call control or communications. For reasons discussed in the firewall section below, the use of a stateful firewall would provide better control and thereby better security.

- *(VoIP0090: CAT III) The IAO will ensure that voice or data traffic between the data and voice VLANs is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.*

- *(VoIP0115): CAT II) The IAO will ensure that traffic between all voice VLANs is filtered and controlled by a layer-3 switch/router ACL or a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services.*

- *(VoIP0116): CAT II) The IAO will ensure that traffic between the VLAN containing mutually accessible servers or devices to and from the voice VLAN(s) or the data VLAN(s) is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services. This firewall will block traffic between the voice and data VLANs or fulfill one or more of the traffic control requirements noted above.*

- *(VoIP0095: CAT II) The IAO will ensure that the Data network perimeter (i.e., Data premise router, Data perimeter firewall) is configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and/or fulfill one or more of the traffic control requirements noted above.*

3.7.2 WAN Connectivity and LAN/CAN/BAN -WAN Protection

Connections from a LAN/CAN/BAN based VoIP environment to the WAN for the purpose of establishing connections to other VoIP phones in other VoIP enclaves, remote VoIP call managers, the PSTN, or DSN is referred to as VoIP Trunking.

3.7.2.1 Current Policy

As of this writing off-site VoIP Trunking is not approved for use in unclassified DOD telecommunications systems. The DOD DSN PMO is only certifying VoIP systems at the PBX-1, PBX-2, and SMEO level, as specified in the GSCR, for inclusion on the DSN APL. These systems are specified for use at the BPCS level. No systems are being certified to use VoIP Trunking for off-premise connections. Due to the fact that DOD policy requires that only DSN APL certified systems be deployed, IP trunking is not approved. All trunking connections to DOD VoIP networks must be through media gateways to the TDM DSN/PSTN.

With regard to the VoSIP program, an exception to the above policy has been made by the DISN DAAs via DSAWG approval for the current VoSIP pilot on the SIPRNet.

- *(VoIP0900: CAT II) The IAO will ensure that all calls into and out of the VoIP network enclave are routed via a media gateway to the traditional TDM networks i.e., DSN and/or PSTN. An exception is made for DAA approved remote VoIP instruments and Soft Phones that connect to the VoIP network enclave via a VPN and are therefore part of the VoIP network.*

- *(VoIP0901: CAT III) The IAO will ensure that written DAA approval is obtained prior to the implementation of IP Trunking connections from the VoIP enclave to the WAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors.*

3.7.2.2 IPT/WAN Firewall Requirements and Controls

Perimeter protection is required at any enclave boundary, to protect the internal network, if the enclave is connected to any external network. Typically, this protection takes the form of a firewall, particularly if the enclave is connected to a WAN. The requirements stated previously in this document establish logically separate voice and data networks even though they may operate on the same network infrastructure. Each of these enclaves requires different protection mechanisms, which typically implies separate voice and data firewalls.

Requirements for data enclave firewalls are covered in the Network Infrastructure STIG. Additional requirements for data enclave firewalls were stated in the VLAN to VLAN Protection section above.

The following section of this document contains the requirements for voice enclave perimeter firewalls that protect the IP voice enclave from the WAN in the event that IP voice enclave access to a WAN has been approved. If such approval is not granted, there will be no WAN connection to protect; therefore no perimeter firewall would be required.

Firewalls present operational and QoS problems for VoIP systems, while VoIP presents security issues for the network. VoIP connections present a greater risk to the security posture of the enclave than customary data WAN connections. The reason for this is that VoIP systems may require many ports to be “opened” in firewalls since the protocols used for carrying VoIP traffic through the network (H.323 and SIP) use a wide range of ports (1024 to 65535) to transport packets. VoIP typically requires four ports per connection, two for signaling (call setup and teardown) and two to transmit/receive user information. Opening a range of ports this large for one call would surely compromise any network. Multiple calls would require multiple groups of ports to be opened.

Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call.

To maintain the private addressing scheme on in the VoIP LAN enclave, Network Address Translation (NAT) must be implemented at the VoIP enclave WAN connection point. This provides additional protection in that hackers outside the VoIP network segment will not be able to scan the VoIP segment for vulnerabilities unless NAT is not implemented or is incorrectly configured. NAT also presents a problem when it comes to VoIP call initiation and QoS.

VoIP enclave to WAN connections may have application filtering issues when using the H.323 or SIP protocols due to the number of random ports needed and QoS issues due to embedded internal addresses at Layer 5 and above. Therefore, H.323 and/or SIP aware stateful firewalls must be used at VoIP WAN call connection network points.

Additionally, Dynamic port mapping limits the range of ports that are used for VoIP traffic at any given time. This reduces the number of ports that are opened, but with four ports required per connection, this number could grow to a large number quickly. This configuration option requires stateful firewall brokering of all VoIP calls outside of the local VoIP cluster. Static mapping assigns four ports to each VoIP set. Normally only two ports are required through a firewall for RTP, once the call is set up. This option takes a considerable amount of time to configure in the routers and must be altered every time a VoIP user needs to be added or removed. Without a stateful firewall brokering all connections between the data and voice networks, you would have to open wide UDP port ranges.

The typical solution to the firewall/NAT problem is to use an Application Level Gateway (ALG) or Firewall Control Proxies (FCPs). An ALG with VOIP support is a special firewall. A stateful firewall and ALG can understand H.323 or SIP and dynamically open and close the necessary ports. When NAT is employed, the ALG opens the VoIP packets and reconfigures the header information to correspond to the correct internal IP addresses on the VoIP VLAN, or on the public network for outgoing traffic. Other solutions involving Firewall Control Proxies (FCPs) and Middle Boxes can be used to improve firewall QoS issues. These devices are placed in front of the VoIP firewall and aid in the control of ports opened in the firewall and the application of address translations.

- *(VoIP0180: CAT II) The IAO will ensure that VoIP aware firewalls are deployed at all approved VoIP enclave to WAN connections providing VoIP call connectivity. Such firewalls must employ stateful packet inspection and dynamic port mapping.*

- *(VoIP0190: CAT II) The IAO will ensure that NAT is implemented on approved VoIP enclave to WAN connections.*

- *(VoIP0200: CAT III) The IAO will ensure all VoIP security perimeter firewalls are dedicated to VoIP traffic to reduce transmission latency caused by firewall operations.*

The following Table 3-1 provides ports and services that should be considered in providing firewall filtering for VoIP servers and networks:

SERVICE	***PORT***
SCCP (Cisco Skinny)	TCP 2000-2002
TFTP	UDP 69
MGCP	UDP 2427
Backhaul (MGCP)	TCP 2428
Tapi/Jtapi	TCP 2748
HTTP	TCP 8080/80
SSL	TCP 443
MS Terminal Services	TCP 3389
Transport traffic	16384-32767
SNMP	UDP 161
SNMP trap	UDP 162
DHCP (BOOTP)	TCP & UDP 67 & 68
DNS	UDP 53
NTP	UDP 123
LDAP	TCP 389
H.323Gatekeeper Discovery	UDP 1718
H.323RAS	UDP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
SIP	TCP or UDP 5060 or 5061
RTP & RTCP	UDP 1024-65534
DC Directory	TCP 8404
Echo	echo
echo-reply	echo-reply
MS-SQL	TCP 1433
SMB	TCP 445
ICCS	TCP 8002
CTIM (CTI manager)	TCP 8003
CTI/QBE	TCP 2478
SCCP	TCP 3224
HID agent	TCP 5000

Table 3-1. VoIP Ports and Services

Some VoIP call control servers utilize some commonly used protocols for their operation such as MS-SQL, Network Time Protocol (NTP), MS Terminal Services, and HTTP. These must be blocked from external access. Additionally, see VoIP systems management below.

- *(VoIP0220: CAT II) The IAO will ensure MS-SQL (port 1433) is blocked at the VoIP enclave perimeter.*

- *(VoIP0230: CAT III) The IAO will ensure the Network Time Protocol (NTP) (port 123) is blocked at the enclave perimeter.*

- *(VoIP0240: CAT II) The IAO will ensure Terminal Services or remote desktop protocol (port 3389) is blocked at the enclave perimeter or that these connections are encrypted.*

- *(VoIP0245: CAT II) The IAO will ensure that all remote HTTP access to the VoIP enclave perimeter firewalls is proxied. HTTP access from the VoIP enclave, if required, should route through the data enclave. Additionally HTTPS should be used in place of this if possible.*

3.8 Call Privacy and Confidentiality

When VoIP connections are established, call privacy may be significantly reduced when compared to traditional telephony. This is due to the ease of access to the call data from anywhere on the network. This is not only a problem on the LAN but more so across the WAN. To ensure the same privacy that subscribers expect, such as that provided by the existing PSTN and DSN, encryption must be implemented for all WAN connected calls. This can be accomplished in a number of ways. The best of these is end-to-end encryption, which in turn requires the IP telephone end devices to have greater processing power and the capacity to support encryption. This is not always feasible, as not all VoIP vendors provide encryption capability from the subscriber terminal. Additionally, until VoIP encryption standards are agreed upon and implemented, one vendor's method may not interoperate with others. In lieu of this, however, encryption should be accomplished at the link-level through the incorporation of HAIPIS or VPN technology as applicable. Gateway devices are normally designed to handle heavier processing loads and are also capable of providing link encryption. Either method would be transparent to the subscriber community.

- *(VoIP0300: CAT II) The IAO will ensure that all VoIP traffic that is sent over approved VoIP enclave-to-WAN connections via an IP WAN network (i.e., Internet, NIPRNet,) is encrypted, at a minimum, between enclaves across the WAN.*

NOTE: The inherent site-to-site encryption employed in classified networks, such as the SIPRNet, meets this requirement.

It is highly recommended that end-to-end encryption of the VoIP conversation is employed.

3.9 VoIP Systems Management

Management of VoIP Systems must be done in a secure manner as with any other telecommunications system. Telecommunication system management is discussed at length in the DSN STIG. For the purpose of this version of the VoIP STIG, please refer to the DSN STIG for system management requirements in addition to those noted in the subsections below.

- *(VoIP0295: CAT II) The IAO will ensure that all VoIP systems are managed in accordance with all requirements in the DSN STIG.*

3.9.1 Remote Access Management of VoIP Servers

Logical access to administrative ports by an unauthorized unscrupulous person could result in serious negative impact on the entire VoIP environment. Any remote connection access to critical servers supporting the VoIP environment for administrative or management purposes should be done in a secure manner.

- *(VoIP0290: CAT II) The system administrator will ensure all remote administrative connections (in-band or out-of-band) to critical VoIP servers are encrypted.*

3.9.2 VoIP Firewall Management

In order to ensure the security of VoIP perimeter firewalls it is imperative that administrative/management connections and access to the firewall devices be controlled from the inside interface only. This can be accomplished by accessing these device types locally, by using out-of-band management or by secure in-band management using protocols such as SSH, SNMPv3, Hyper Text Transfer Protocol (HTTPS), or by encrypted VPN tunnel. Dedicate management terminals to the VoIP network if necessary. Additional requirements may be found in the Network infrastructure and Enclave STIGs.

- *(VoIP0210: CAT II) The IAO will ensure VoIP firewall administrative/management traffic is blocked at the perimeter, or is tunneled and encrypted using VPN technology at the enclave perimeter, or is out-of-band.*

3.10 Voice Mail Services

Voice mail services in a VoIP environment are available in several different configurations. For example, a legacy voice mail platform can connect to a VoIP gateway to provide voice mail services for VoIP users. In the same respect, a VoIP based voice mail platform can provide voice mail services to the legacy voice users and the VoIP users. In addition to providing traditional voice mail services, many VoIP voice mail systems are also capable of providing unified mail (integrated voice and electronic mail), or by interacting with existing email messaging systems.

With unified mail, the mail server most likely is logically connected to the data network. The VoIP voice mail platform should be configured to connect to the VoIP Call Processor through a stateful inspection firewall or layer 3 switch as discussed previously. The firewall should be configured to deny all traffic between the Voice VLAN and the data network except the traffic necessary to transfer and receive voice calls and messages between the subscribers phone, the call processor or gateway, and the voice mail platform. This configuration is necessary to mitigate the risk of DoS attacks against the data network and/or the VoIP network. Filtering the traffic will also mitigate the risk of exploiting vulnerabilities on operating systems supporting the VoIP telephony services.

Voice mail services are commonly configured to run on common operating systems, such as, Microsoft Windows NT, Windows 2000, or Sun Solaris. Steps should be taken to ensure that these operating systems are secured in accordance to the appropriate STIG. Application services supporting the voice mail services should also be hardened. For example, MS SQL Server may be used to support subscriber accounts, or MS IIS may be used to allow subscribers to change their voice mail settings using an Internet Browser.

- *(VoIP0310: CAT II) The IAO will ensure text-to-speech is disabled if the voice mail platform is configured to interact with a legacy corporate email system and both systems are not collocated in the same or adjoining VLANs as required under the VLAN section above.*

- *(VoIP0330: CAT II) The IAO will ensure the server hosting the Voice Mail Service is properly secured in accordance with all applicable OS STIGs (i.e., Windows, Unix).*

- *(VoIP0340: CAT II) The IAO will ensure the application services (SQL, IIS, Apache, Oracle, etc.) supporting the voice mail service are properly secured in accordance with all applicable STIGs.*

- *(VoIP0350: CAT II) The IAO will ensure the subscriber can only change their voice mail settings via the phone interface or through a SSL connection. HTTP and Telnet services will be disabled on the voice mail platform.*

3.11 Wireless VoIP

As VoIP technology matures, wireless technology is also fast becoming a reality. A relatively new capability in the wireless realm is VoIP using 802.11 wireless local area networks (WLANs). This new technology elevates many existing VoIP concerns such as QoS, network capacity, provisioning, architecture, and not the least important; security. The success of VoIP over WLAN technology will be the ability of WLAN technology to adequately support and provision QoS capabilities. Many government entities are exploring mobile communication solutions that include wireless VoIP that can meet critical needs for interoperability and flexibility. As of this writing VoIP over WLAN is not approved for use in unclassified DOD telecommunications systems. The DOD is only certifying VoIP systems at the wired LAN level, as specified in the GSCR, for inclusion on the DSN APL. These systems are specified for use at the BPCS level. No VoIP systems are being certified to use WLAN. Due to the fact that DOD policy requires that only DSN APL certified systems be deployed, VoIP over IP WLAN is not approved. If this technology is deployed all the requirements in this document as well as those contained in the Wireless STIG should be applied to the wireless VoIP environment.

- *(VoIP0360: CAT II) The IAO will ensure that if wireless VoIP is used, the requirements contained in the Wireless STIG have been applied to the wireless VoIP environment.*

- *(VoIP0361: CAT II) The IAO will ensure that written DAA approval is obtained prior to the implementation of VoIP over WLAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors.*

3.12 Securing MGCP

The MGCP protocol is the communications protocol used between MGCs and MGs. Typically this communication would occur across an unsecured network (i.e., Internet, NIPRNet). This being the case, all call setup and processing would be transmitted in the clear. To mitigate this security weakness, Request for Comment (RFC) 2705 (MGCP) outlines and recommends the use of IPSEC for encryption and authentication between gateways.

- *(VoIP0040: CAT II) If MGCP is used, the IAO will ensure that IPSEC is enabled and used on each MGC to provide authentication and encryption.*

3.13 VoIP Connection to the DSN

This topic is covered at length in the DSN STIG. Please refer to it for the requirements relating to the use of any telecommunications system in the DOD and connecting that system to the DSN.

- *(VoIP0370: CAT II) The IAO will ensure that no VoIP systems or networks are connected to the DSN switching system without being certified, accredited, and placed on the DSN Approved Products List per DODI 8100.3.*

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense (DOD) Directive 8500.1, 24 October 2002.

Department of Defense Instruction 8500.2, 6 February 2003.

Department of Defense Instruction (DODI) 8100.3, 16 JAN 03.

Department of Defense Voice Network Generic Switching Center Requirements (GSCR) Document, 8 September 2003

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

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

Department of Defense 8510.1-M, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)," 31 July 2000.

CJCSM 6510.10, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND), 15 March 2002.

CJCSI 6215.01b, Policy for Department of Defense Voice Networks, 23 September 2001.

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

Defense Information Systems Agency (DISA) Computer Services Security Handbook, Version 3, 1 December 2000.

Defense Information Systems Agency (DISA) DSN Security Technical Implementation Guide, Version 1, Release 1, 12 March 2003.

Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide, Version 5, Release 2, 17 June 2003.

Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000, Version 43 (to match NSA Guide), Release 1, 26 November 2002.

Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide, Version 4, Release 4, 15 September 2003.

Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) on Enclave Security, Version 1, Release 1, 30 March 2001.

Defense Information Systems Agency (DISA) Web Services Security Technical Implementation Guide (STIG), Version 3, Release 1, dated 22 August 2002.

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 June 1993.

Army Regulation (AR) 380-19, "Information Systems Security," 27 February 1998.

Air Force Instruction 33-111, "Telephone Systems Management," 1 June 2001.

Secretary of the Navy Instruction (SECNAVINST) 5239.3, "Department of the Navy Automated Information Systems (AIS) Security Program," 14 July 1995.

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

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

Memorandum for Secretaries of Military Departments, et al, "Web Site Administration," 7 December 1998.

Generic Requirements for Network Element/Network System (NE/NS) Security, Issue 2, Telcordia Technologies, March 2002.

National Security Telecommunications an Information Systems Security Policy (NSTISSP) 101, "National Policy on Securing Voice Communications," 14 September 1999.

National Institute of Standards and Technology (NIST) Special Publication 800-58 "Voice Over IP Security" (Draft), May 2004

Industry Publications

Avaya Products Security Handbook, November 2002.

Cisco Systems, "IP Telephony Solution Reference Network Design Guide," May 2002.

CISCO Systems, "IP Telephony Security Recommendations," 1992-2001 Cisco Systems Inc.

General Information Sites

http://www.disa.mil	Defense Information Systems Agency (DISA) Web Page
http://www.cert.mil	Joint Task Force Global Network Operations. Emergency Response Team
http://www.specbench.org	The Standard Performance Evaluation Corporation
http://www.ciac.org/ciac	The U.S. Department of Energy's Computer Incident Advisory Capability
http://nsi.org	National Security Institute's Security Resource Net Home Page
http://csrc.nist.gov	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.icsa.net	ICSA.NET Internet Security
http://www.redbooks.ibm.com	"How to" books, written by very experienced IBM professionals from all over the world
http://www.microsoft.com/technet/security/current.asp	Microsoft Security Bulletin and Patch Listings
http://www.nipc.gov	National Infrastructure Protection Center (an FBI program)
http://cisco.com/	Cisco Systems Homepage
http://avaya.com	Avaya Homepage
http://www.iec.org/	International Engineering Consortium

This page is intentionally left blank.

APPENDIX B. ACRONYMS

AAA	Authentication, Authorization, and Accountability
ACD	Automatic Call Director
ADIMSS	Advanced Defense Switched Network Integrated Management Support System
ADM	Add-Drop Multiplexer
AFWIC	Air Force Warfare Information Center
A/NM	Administration and Network Management
AIN	Advanced Intelligent Network
AIS	Automated Information Systems
ALG	Application Level Gateway
ANI	Automatic Number Identification
AO&M/NM	Administration, Operation and Management/Network Management
AORL	Acknowledgement of Risk letter
APL	Approved Products List
ATM	Asynchronous Transmission Mode
BAN	Base Area Network
BPCS	Base/Post/Camp/Station
C2	Command and Control
C2VG	Command and Control Voice Grade (adjective for a LAN)
CA	Certification Authority
CAT	Category
C&A	Certification and Accreditation
CAN	Campus Area Network
CCB	Configuration Control Board
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual
CLI	Command Line Interface
CNSS	Committee on National Security Systems (Formerly NSTISSC)
CM	Configuration Management
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental/Contiguous United States
COS	Class of Service
COTS	Commercial-Off-The-Shelf
CPE	Customer Premise Equipment
CTI	Computer Telephony Interface
CTIM	Computer Telephone Integration Manager
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DC	Domain Component

DECC	Defense Enterprise Computing Center
DIAM	Defense Intelligence Agency Manual
DISA	Defense Information Systems Agency
DoS	Denial of Service
DISAC	DISA Circular
DISAI	DISA Instruction
DISN	Defense Information Systems Network
DISN-C	DISN CONUS
DISN-E	DISN EUR
DISN-P	DISN PAC
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DMS	Defense Messaging System
DNS	Domain Name System
DOD	Department of Defense
DODD	Department of Defense Directive
DRSN	Defense Red Switched Network
DSA	Dial Service Assistant
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
DTSW	Defense Telecommunications System Washington
EAL	Evaluation Assurance Level
ECP	Engineering Change Proposal
EMP	Electromagnetic Pulse
EMS	Element Management System
EN	End Office Node
EO	End Office
EOS	End Office Switch
ES	End System
ESP	Essential Service Protection
EUR	Europe
ESM	Enterprise System Management
FEP	Front End Processor
FCP	Firewall Control Proxies
FIPS	Federal Information Processing Standard
FM	Fault Management
FNBDT	Future Narrow Band Digital Terminal (application layer encryption)(Now SCIP)
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Field Security Operations
FY	Fiscal Year
FTP	File Transfer Protocol
FTS	Federal Telecommunications System

GETS	Government Emergency Telecommunications System
GOSC	Global Operations and Security Center
GOTS	Government-Off-The-Shelf
GPS	Global Positioning System
GSCR	General Switching Center Requirements
GUI	Graphical User Interface
HAIPIS	High Assurance IP Interoperability Specification (for type 1 encryption)
HID	Host Intrusion Detection
HITS	Hawaii Information Transfer System
HTTP	Hyper Text Transfer Protocol
I/O	Input / Output
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAW	In Accordance With
IAVA	Information Assurance Vulnerability Alert
IETF	Internet Engineering Task Force
IAVM	Information Assurance Vulnerability Management
I&A	Identification and Authentication
ID	Identification
IDNX	Integrated Digital Network Exchange
IDS	Intrusion Detection System
IIS	Internet Information Services
INFOSEC	Information Systems Security
IP	Internet Protocol
IPSec	IP Security Protocol
IS	Information System
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part (SS7 protocol)
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
IT	Information Technology
ITU	International Telecommunications Union
JITC	Joint Interoperability Test Command
JWICS	Joint Worldwide Intelligence Communications System
KBPS	Kilobits Per Second
LAN	Local Area Network
LANE	Local Area Network Emulation
LDAP	Lightweight Directory Access Protocol

MAC	Mission Assurance Category
MAC	Media Access Control
MAN	Metropolitan Area Network
MBPS	Megabit Per Second
MCU	Multipoint Control Units
MFS	Multifunction Switch
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MILDEP	Military Department
MLPP	Multi-Level Precedence and Preemption
MPLS	Multiprotocol Label Switching
MMI	Man Machine Interface
MS	Microsoft
MTP	Message Transfer Part (SS7 protocol)
MUX	Multiplexer
MUF	Military Unique Feature(s)
NAT	Network Address Translation
NCS	National Communications System
NID	Network Intrusion Detector
NIDS	Network Intrusion Detector Sensor
NIPRNet	Non-Classified (But Sensitive) Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NM	Network Management
NMC	Network Management Center
NMS	Network Management System
NNM	Network Node Manager
NOC	Network Operations Center
NSA	National Security Agency
NSO	Network Security Officer
NSTISSC	National Security Telecommunications and Information Systems Security Committee (Became the Committee on National Security Systems[CNSS])
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTISSP	National Telecommunications and Information Systems Security Policy
NOC	Network Operations Center
NTP	Network Time Protocol

O&M	Operations and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OCONUS	Outside CONUS
OMAP	Operation and Maintenance Application Part (SS7 protocol)
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OS	Operating System
OMAP	Operation and Maintenance Application Part (SS7 protocol)
PAC	Pacific
PACOM	Pacific Command
PAT	Precedence Access Threshold
PABX	Private Automated Branch Exchange (old term)
PBX	Private Branch Exchange
PBX1	Private Branch Exchange Type 1 (basic, no MLPP MUF)
PBX2	Private Branch Exchange Type 2 (MLPP capable)
PC	Personal Computer
PCM	Pulse Code Modulation
PDI	Potential Discrepancy Item
PIN	Personal Identification Number
PM	Project or Program Manager
PMO	Program Management Office
POA&M	Plan Of Action and Milestones
PPS	Ports, Protocols, and Services
PRI	Primary Rate Interface
PSN	Packet Switched Node
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QBE	Query by Example
QoS	Quality of Service
RAS	Remote Access Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comment
RNOSC	Regional Network Operations and Security Center
RSU	Remote Switching Unit
RTP	Real Time Protocol
SA	System Administrator
SAS	Stand Alone Switch
SCAO	SIPRNet Connection Approval Office
SCCP	Signaling Connection Control Part (SS7 protocol)
SCCS	Source Code Control System
SCIP	Secure Communication Interoperability Protocol (formerly FNBDT)

SCP	Signal Control Point (CCS7 device)
SDID	Short Description Identifier
SG	Signaling Gateway
SIPRNet	Secure Internet Protocol Router Network
SIP	Session Initiation Protocol
SM	Security Manager
SNMP	Simple Network Management Protocol
SMEO	SMall End Office
SMB	Server Message Block
SMU	Switch Multiplex Unit
SOP	Standard Operating Procedure
SQL	Structured Query Language
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SSAA	System Security Authorization Agreement
SS7	Signaling System 7 (protocol suit)
SSL	Secure Socket Layer
SSL	Secure Socket Layer
SSM	Single System Manager
SSP	Signal Service Point (CCS7 device)
STE	Secure Terminal Equipment
STU	Secure Telephone Unit
ST&E	Security Test and Evaluation
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guide
STP	Signaling Transfer Point (CCS7 device)
SWA	South West Asia
SVoIP	Secure Voice over Internet Protocol
SVoSIP	Secure Voice over Secure Internet Protocol
T&S	Timing and Synchronization
TAPI	Telephony Application Programming Interface
TACACS	Terminal Access Controller Access Control System
TAFIM	Technical Architecture Framework for Information Management
TCAP	Transaction Capability Application Part (SS7 protocol)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TNM	Telecommunications Network Management
TOE	Target of Evaluation
TS	Tandem Switch
TSSO	Telephone Systems Security Officer

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UID	User Identification
UNIX	Name of an Operating System
URL	Uniform Resource Locator
UPS	Uninterruptible Power Source
VCAO	Voice Connection Approval Office
VCTS	Vulnerability Compliance Tracking System
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing
VMS	Vulnerability Management System
WAN	Wide Area Network
WLAN	Wireless Local Area Network

This page is intentionally left blank.