DRAFT

IP TELEPHONY & VOICE OVER INTERNET PROTOCOL

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 0

30 December 2004

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

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.
- **Sections 1, 1.2, 1.3: Introduction, Background, Scope, and Purpose**
  - Rewrote section 1 to reflect the current DISA format for section 1 of all STIGS.
  - Removed the Purpose section and included appropriate verbiage in the Introduction.
  - Moved all requirement descriptions and bullets to another sections as appropriate.
- **Section 1: Introduction**
  - Rewrote this section.
  - Removed background from the title.
  - 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.
- **Section 1.2: Scope**
  - Rewrote this section.
- **Section 1.3: Authority**
  - Updated to the current FSO STIG authority verbiage and added verbiage to include the 8100.3. 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 this 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 it's 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 2.2.3: Media Gateway Control Protocol (MGCP)**
  - Rewrote this section for accuracy and clarity. Moved the second paragraph to Section 3.
  - VoIP: 0040, 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
  - 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 sustem 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. was revised for clarity
  - VoIP0280: revised for clarity.
- **Section 3.2: Physical Security**
  - This section was section 3.1. Rewrote for clarity
  - VoIP0060: relocated this PDI to the newly created section 3.2
- **Section 3.3: System Configuration Protection**
  - Added this section. Included VoIP0060 from section 3.1
  - VoIP0060: Rewrote for clarity and generality.
  - VoIP0061: Added this PDI
  - VoIP0062: Added this PDI
- **Section 3.4: VoIP Instrument Registration**
  - Added this section.
  - VoIP0065: Added this PDI
- **Section 3.5: Data and Voice 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.

- **Section 3.5.1: Logical Address Segregation**
  - This section was part of section 3.2
  - 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: Logical Network Segregation Using Virtual Local Area Networks (VLANs)**
  - This section was part of section 3.3. Re-titled.
  - Rewrote the section for clarity
  - VoIP0101: added this PDI relating to VLAN usage in the data network
- **Section 3.5.2.1: Voice VLAN**
  - This section was part of section 3.3
  - VoIP0105: added this PDI
  - VoIP0115: added this PDI
- **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
  - 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: Reassigned this PDI number
  - VoIP0130: Was VoIP0140: rewrote this PDI for clarity regarding DAA approval and adding a requirement for documented evidence
  - VoIP0135: Was VoIP0150: rewrote this PDI for clarity regarding local soft phone policy
  - VoIP0140: added this PDI regarding OS STIG compliance
  - VoIP0150: Was VoIP0130: rewrote this PDI for clarity regarding use of soft phones on a LAN
  - VoIP0160: rewrote this PDI for clarity regarding use of remote soft phones
  - VoIP0165: added this 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 Network VLAN to VLAN Protection**
  - Added this section. Used part of section 3.5
  - VoIP0090: Rewrote this PDI. Eliminated the requirement for NAT between Voice and data VLANs and clarified the requirement for a stateful firewall.
  - VoIP0095: Added this PDI regarding the requirement for the data firewall blocking access to the VoIP VLAN

- **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 Ports
  - 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.
- **Section 3.9.2: VoIP Firewall Management**
  - This section was 3.6. Rewrote for clarity.
  - VoIP0250: rewrote for clarity.
- **Section 3.10: Voice Mail Services**
  - This section was 3.10. Rewrote for clarity.
  - VoIP0320: removed this PDI since it duplicated previous requirements
  - VoIP0330: rewrote for clarity
  - VoIP0340: rewrote for clarity
- **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.
  - VoIP: 0040: 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

- **Appendix B (old): Cisco Placeholder**
  - Deleted this placeholder. Information planned for this section will be placed in an addendum to the STIG
- **Appendix C: Nortel Placeholder**
  - Deleted this placeholder. Information planned for this section will be placed in an addendum to the STIG
- **Appendix D: Avaya Placeholder**
  - Deleted this placeholder. Information planned for this section will be placed in an addendum to the STIG
- **Appendix E: Interim Voice Over Internet Protocol Policy Message**
  - Deleted this message since it is superceded by DSN APL certification efforts.

This page is intentionally left blank.

1. INTRODUCTION

The *IP 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 IP Telephony (IPT). When applied to Department of Defense (DOD) networks and systems, this document must be use 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., SQL server, 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. IP Telephony, 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 IP Telephony 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 NSA, DSN PMO, DSN VCAO, JITC IA Test team, AFWIC, and other DOD components who have provided valuable comments and input for this STIG.

1.1 Background

IP Telephony and Voice Over Internet Protocol (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 switch 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 without C2 capability at the campus level network edge of DSN, NIPRNet and SIPRNet. It is also being employed in the backbones of SIPRNet and NIPRNet 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 virtually shut down some 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 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 making IP telephony secure.

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 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 Joint Interoperability Test Command (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 to the infrastructure that supports IPT systems employing VoIP technologies. The focus of this STIG is on securing the technology, 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 Video Tele-Conferencing (VTC).

The systems that are the focus of this STIG are however not homogeneous unto themselves. 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 Operating Systems (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 used. Additionally, the data network is an integral part of 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 other technologies that make up the infrastructure that IPT/VoIP systems rely on. 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; Defense Switched Network (DSN)
- Network Enclave & Network Infrastructure (IP centric)
- Network Operations Center (NOC) and Network Management (future)
- Enterprise Systems Management (ESM)
- Secure Remote Computing (Remote network access for travelers and teleworkers)
- Operating Systems (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 and Oracle)(soon to include DB2)
  - Web Server (specifically MS IIS, Netscape, and Apache and other web technology)
- Domain Name Services (DNS)
- Wireless Networks

Additionally, this document does not cover in detail every vendor's VoIP solution in use, or being considered for use, within the DOD. However, the contents of this document are to be applied to the greatest extent possible to all VoIP systems and networks. The target is for VoIP systems, networks, and other office systems/devices that use commercially available VoIP solutions. The intent is for the requirements in this STIG to 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 and other STIGs are provided under the authority of DOD Directive 8500.1.

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

Additionally, DOD Instruction 8100.3, which governs the DSN and connected systems, refers to the DODD 8500.1 (IA policy) and DODI 8500.2 (IA implementation), for IA requirements regarding system certification and accreditation. Some requirements in this document are derived directly from the 8100.3

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.

1.7 STIG Distribution

Parties within the DOD and the Federal Government's computing environments can obtain the applicable STIGs 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. Interested users can also subscribe to the “STIG News” which will provide notice when the STIGs and related resources are updated. The NIPRNet URL for the IASE site is http://iase.disa.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a .mil or .gov address.

An additional source for the STIGs is the National Institute of Standards and Technology (NIST) web site. The NIPRNet URL for the NIST site is http://csrc.nist.gov/pcig/cig.html. This site contains copies of any unclassified STIG, as well as checklists, and other related security information. Access to the STIGs on the NIST web server is available to .com addresses.

The STIGs are also available to users that do not originate from a .mil or .gov address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to fso_spt@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.

While vendors are encouraged to use the STIGs to enhance the security of their products in general, they are not authorized to release the STIGs to the general public.

1.8 Document Revisions and Support

Support is available for the application of the STIGs, Checklists, and Tools from FSO Customer Support at fso_spt@disa.mil. It must be noted however; that support is only available to DOD Customers and DOD sponsored vendors. Vendors contacting FSO for support will need to provide the VCAO tracking number for the product or system.

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

2. IP TELEPHONY OVERVIEW

2.1 VoIP Components

Although VoIP is a very different technology and approach to providing voice services, some of the same component concepts that make up the Public Switched Telephone Network (PSTN) are also found in VoIP environments. VoIP networks must perform all of the same tasks that the PSTN does, in addition to performing data and signaling gateway functions to the existing public network. 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 entity) with the IP backbone 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 to VoIP and circuit-switching components; however there are many differences. A circuit switched environment can be classified as a Time Division Multiplexing (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. Quality of Service (QoS) can be critical to acceptable VoIP implementations. Marking packets is the first step in establishing their priority throughout the network and should be done at the first available point. Some networking switches can mark packets for QoS purposes. QoS specifies a priority throughput level and Class of Service (CoS) ensures that packets of a specific application are marked for priority handling. This priority throughput and marking 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, call processor/controllers house the signaling and control services that coordinate the media gateway functions. A call processor/controller can also be known as a softswitch, call agent, call manager, or gatekeeper depending on its specific function in the VoIP network or specific vendor solution being implemented. The amount of functionality provided by a call processor/controller is based on the particular VoIP product used.

2.1.3 Media/Signaling Gateways

VoIP Gateways are responsible for 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 a physical board or blade found in a dedicated telecommunications frame or a common PC running VoIP software. Media and Signaling Gateway's features and services can also span a wide spectrum and their functions can be divided into three key gateway types:

- Media Gateway (MG) – The media gateway mediates the media signals between the IP network and the circuit switched or traditional telephone network (i.e. the PSTN). This gateway converts voice transported on the IP network using packet formats to analog or digital voice signals on the PSTN side and vice versa. Simply stated, the MG provides single line or trunking functions that interface between the telephone network and a VoIP network.
- Signaling Gateway (SG) – This gateway type mediates the signaling functions between the IP network and the switched circuit network. For instance, it may provide correlation between the H.323 signaling on the packet network side and the signaling system seven (SS7) signaling on the PSTN side.
- Media Gateway Controllers (MGC) – The media gateway controller communicates with both the MG and the SG, providing the call setup and processing functions required. This gateway type would use a dedicated protocol type such as the Media Gateway Control Protocol (MGCP) protocol (discussed later) for inter-gateway communications functions.

One or all of the above gateway functions could be employed at a given site depending on many factors to include the network architecture at that site. When implemented, they may be distinct, and may also be 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 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 PSTN to the VoIP network. In this example, a single system combining MG and SG could provide both the media and signaling gateway functions and interfaces between the VoIP network and PSTN.

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 users 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 with 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 IP Telephony implementations; however, there are two major protocol-dependent approaches defined and under revision for VoIP signaling. They are the ITU-T H.323 protocol and the IETF's Session Initiation Protocol (SIP). 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 Cisco Skinny protocol and the Nortel, or AVAYA proprietary versions of the H.323 protocol. 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 LAN endpoint 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 system for multimedia communication. Instead, SIP works in harmony with other IP protocols to provide similar functionality as H.323. Contrary to H.323, the SIP describes architecture with distributed intelligence that is composed of two types of entities: user agents, and network servers.

- User Agents - 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.

NOTE: SIP calls can be made directly to another UA, through the redirect server, or through the SIP proxy.

- Network Servers - There are three types of SIP network servers, these are the registration server, proxy server, and redirect server.
  - The registration server maintains an inventory of UA locations within its domain. When a call is made, proxy or redirection servers so incoming may consult it and calls can be correctly routed.
  - The proxy server handles SIP requests for the source UA. For example, if an outbound call were initiated, the proxy server would query DNS and registration servers for the address of the destination UA or the next SIP server and forward the request to that machine. If a destination SIP server receives the request, it forwards the request to the destination address of the UA being called.
  - The redirect server returns a message to the source about the destination UA or the next server to contact. A SIP server acts as a redirect server by returning the new destination address.

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 Media Gateway Controller (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 heterogeneous 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 and only trunk into the local telephone switch.

2.3.1 Internet Protocol (IP) Centric

This type of 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 or circuit switch (see Figure 2.1). For an IP centric solution, the connectivity to the rest of the switched network (i.e., DSN or PSTN) is accomplished via a dedicated trunk (i.e., a T1/E1 or Integrated Services Digital Network [ISDN]) equivalent to the Primary Rate Interface (PRI).

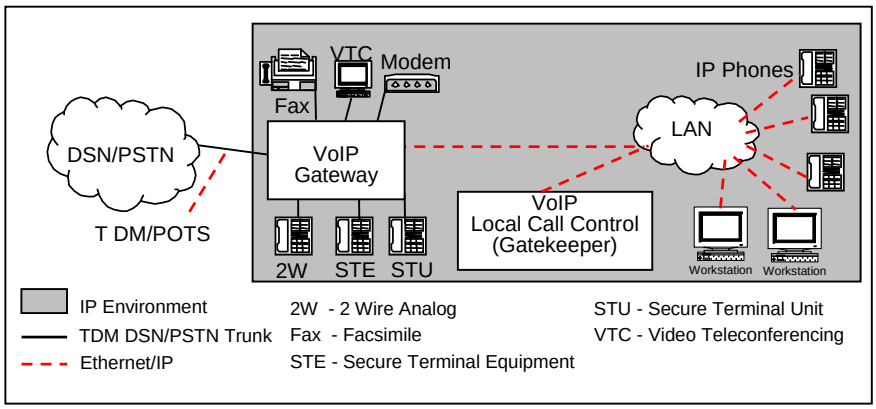

Figure 2.1. Illustration of IP Centric Architecture

2.3.2 Internet Protocol (IP) Enabled

IP enabled architectures are considered hybrid solutions. By design an IP enabled solution incorporates the services and facilities of traditional TDM circuit switches while providing VoIP terminals to the end subscriber. As depicted in Figure 2.2, this solution has a TDM circuit switch that provides the core call processing and switching of all calls. In addition, the same circuit switch offers IP phone instruments to provide subscriber line functions similar to traditional analog or digital telephony instruments. The DSN/PSTN interface (T1/E1, PRI, etc) is provided via the TDM circuit switch and an integrated Ethernet interface provides connectivity to the IP LAN supporting the IP Phones.

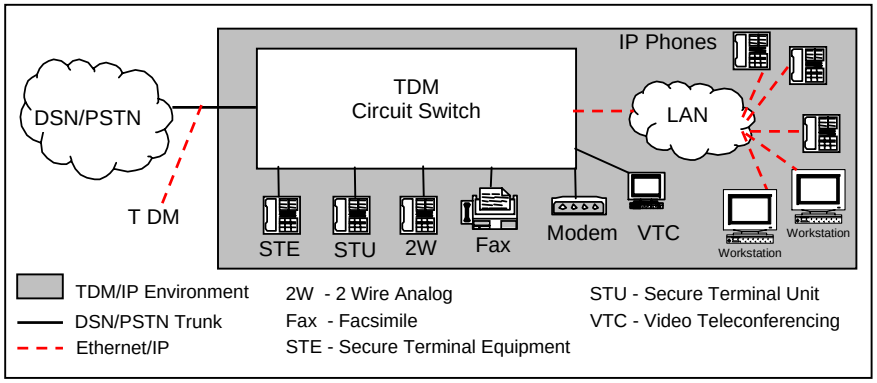

Figure 2.2. Illustration of IP Enabled (Hybrid) Architecture

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 a subsequent release of this STIG. The following is a list of the terms and their capabilities.

- Voice over Secure IP (VoSIP)
  - 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)
  - Security provided at the Application layer using Future Narrow Band Digital Terminal (FNBDT) devices
  - 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))

- Secure Voice over Secure IP (SVoSIP)
  - Security 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 data networks. 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 disclosure of confidential information, unprotected user credentials, and the potential for identity theft. It allows malicious users to collect information about your VoIP system that can be used to mount an attack on it, other systems, or data that might not otherwise be vulnerable. VoIP networks differ from circuit switched networks because information is sent over commonly accessible paths. All the tools needed for 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 needed 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)

Overloading the network with unnecessary data resulting in taking the network down causes a denial of service. The traditional system (separate data and voice networks) allows an organization to still communicate if their data network is unavailable. With the implementation of VoIP in a converged network, a DoS attack could also be very effective against the VoIP system considering the Quality of Service necessary for VoIP to be functional.

2.4.3 Traffic Flow Redirection

Since the data packets do not flow over a dedicated connection for the duration of a session, an adversary could manipulate the routing of packets and 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 Quality of Service (QoS) may be diminished to a noticeable level.

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 ignored 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

3. SECURING THE VOIP ENVIRONMENT

A future expectation is that long-established security features (i.e. authentication and encryption) will integrate with VoIP standards. However, today many existing data-centric security technologies can be integrated to enhance security in the VoIP environment. VoIP network security includes voice-packet security, which focuses on application concerns, and IP security, which 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.

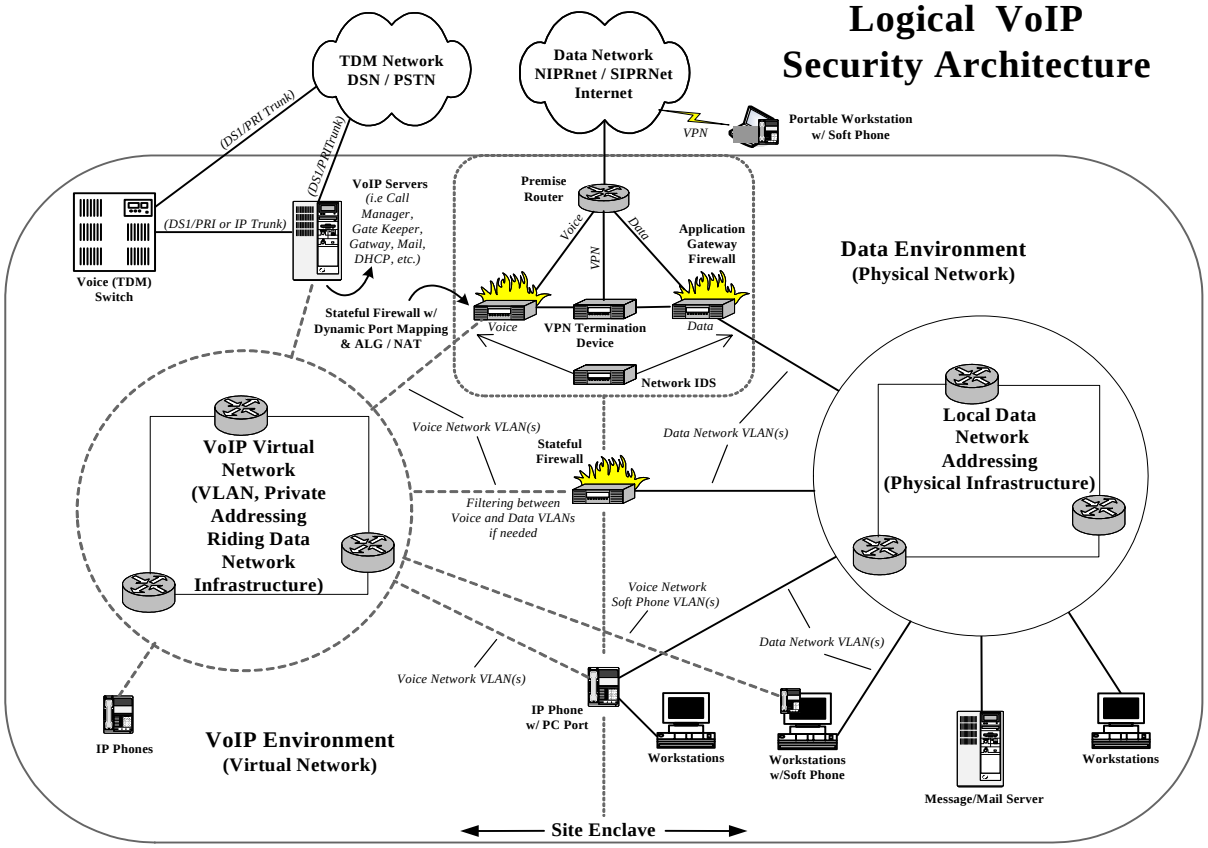

Figure 3.1. VoIP Security Architecture – Logical Diagram

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 denial of service situations.

Networks supporting IPT must:

- possess enough bandwidth capabilities to support the voice traffic
- be redundant above the access layer
- be provided with adequate backup power
- be capable of using QoS, CoS, as well as 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) needed 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 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.*

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 servers 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 IP Telephony environment. Some vendors provide IP Telephony services on their own proprietary systems while others provided these services on standard UNIX and Microsoft Windows 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 IP Telephony 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.).*

3.2 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 physical unauthorized 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 a secured area.*

3.3 Protection of System 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 that could be used in an attack on the system.

- *(VoIP0060: CAT III) The IAO will ensure that IP Telephony terminals (VoIP phones) do not display network configuration information on their display without the use of a password.*
- *(VoIP0061: CAT III) The IAO will ensure that IP Telephony terminals (VoIP phones) cannot be configured at the instrument without the use of a password.*

- *(VoIP0062: CAT III) The IAO will ensure that a policy is in place to ensure that the IP Telephony terminal (VoIP phone) configuration and display password is known by system administrators only and maintained in accordance with customary password changing requirements.*

3.4 VoIP Instrument Registration

Traditional telephone systems require physical wiring and/or configuration changes to add an instrument to the system. This made it difficult for someone to add unauthorized digital instruments to the system. This could be done easier with older analog systems, however, by tapping an existing analog line. This is no longer the case. Most IPT/VoIP systems employ an automatic means of registering a new instrument on the data 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. This is not only a configuration management problem but it could allow theft of services or some other malicious attack. It is recognized however that auto-registration is necessary during initial system setup and a short time thereafter.

- *(VoIP0065: CAT III) The IAO will ensure that the auto-registration feature of a VoIP system is disabled within 5 days following initial system setup and configuration.*

3.5 Data and Voice Segregation

For reasons including QoS, scalability, manageability, and security, deployment of IP telephony devices and IP data devices should be deployed on minimally two logically different IP segments. (See figure 3.1.) Achieving the ideal security posture would require two separate networks, however, this works against the idea of convergence and the associated cost savings. The combination of data and voice segmentation and a switched infrastructure strongly enhances the security posture of the system and mitigates call eavesdropping attacks. In addition, limiting logical access to VoIP components is necessary for protecting telephony applications running across the infrastructure. Logically, segregating data from telephony by placing VoIP servers and subscriber terminals on logically separate IP networks while controlling access to these VoIP components through filters will help to ensure security and aid in protecting the VoIP environment from external threat.

3.5.1 Logical Address Segregation

VoIP components (i.e. Gatekeepers, Call Managers, voice mail systems, IP Subscriber Terminals etc.) should be deployed within their own, separate private IP network or logical sub-network. These subnets should use a different major address range than is deployed on the local data networks. Where possible, non-routable RFC 1918 IP address space should be used (10.x.x.x, 172.16.x.x, and 192.168.x.x), to further separate IP telephony from the data network. This will help to reduce the chances of voice traffic traversing outside the telephony network segment and vice versa. Additionally, when using Dynamic Host Configuration Protocol (DHCP) for address assignment, different servers should be used for voice components and data components.

- *(VoIP0070: CAT II) The IAO will ensure that all VoIP systems and components are deployed on their own dedicated networks or sub-networks that are not shared with the local data network.*
- *(VoIP0080: CAT II) The IAO will ensure that all local VoIP systems and components are deployed using private address space IAW RFC 1918.*

CAVEAT: This finding can be reduced to a CAT IV for VoSIP systems residing on the SIPRNet.

- *(VoIP0082: CAT II) The IAO will ensure that when using DHCP for address assignment, different servers are used for voice components and data components.*
- *(VoIP0085: CAT II) The IAO will ensure that all VoSIP systems and components residing on the SIPRNet utilize separate address blocks from the normal data address blocks to allow for traffic and access control via firewalls and router ACLs.*

3.5.2 Logical Network Segregation Using Virtual Local Area Networks (VLANs)

An IP Telephony system is built on an IP infrastructure based on layer 2 and layer 3 switches and routers—making up 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. Guidelines and requirements for securing access layer devices including any associated cross-connect hardware can be found in the Network Infrastructure STIG.

Voice networks increasingly represent high-value targets for attacks and represent a greater risk to security than any other technology; hence, it is imperative that these networks be secured as tightly as possible to reduce the impact that an attack can have on both the voice network and the data network. Voice traffic must be isolated using a separate VLAN to provide additional QoS, scalability, manageability. Segregating voice traffic from data traffic greatly enhances the security of all voice services. Further subdivision of the voice and data networks can further enhance security.

- *(VoIP0101: CAT II) The IAO will ensure that the network supporting IPT implementations (i.e. the underlying data network) is configured using VLANs in compliance with the Network Infrastructure STIG.*

3.5.2.1 Voice VLAN

VLAN technology has traditionally been an efficient way of grouping users into workgroups to share the same network address space 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 IP telephony equipment from the data traffic. When VLANs are deployed, excessive broadcast and multicast packets present in the normal data traffic will not disrupt IP telephony services. As with data networks, IPT equipment and instruments should be logically grouped using multiple VLANs.

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 so that a PC or workstation can connect to the phone, which then connects to the switchport at the access layer switch. This provides the simplicity of a single 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 tagging. The link mode between the IP Phone and the switch can be an 802.1Q trunk or a single VLAN access link. With a trunk, the voice traffic can be isolated from other data, providing security and QoS capabilities. As an access link, both voice and data must be combined over the single VLAN; hence, there is no method to segregate the traffic at the switch.

An attacker from the data VLAN can easily overwhelm the voice VLAN. Furthermore, IP telephony servers are vulnerable to attacks from within the activity as well as form 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. Packet filtering must be implemented through an internal stateful firewall or by configuring ACLs in the Layer 3 switches, limiting both ports and addresses that can have access to and from the voice VLAN. Examples of connections that would be allowed would be between the voice mail server in a voice VLAN and the email server in a data VLAN. The management VLAN would also need access to the voice VLAN and vise versa.

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

- *(VoIP0100: CAT II) The IAO will ensure that a voice VLAN has been configured to segregate voice traffic from data traffic.*
- *(VoIP0105: CAT II) The IAO will ensure that IP phones, workstations, and servers providing voice services are connected to switchports with membership only to the voice VLAN.*
- *(VoIP0110: CAT III) The IAO will ensure that all IP phones containing a multi-port switch for connecting a PC, support 802.1Q or have the data port disabled.*

- *(VoIP0115): CAT II) The IAO will ensure that all traffic between the voice, data, and management VLANs are filtered and controlled by a layer-3 switch or a firewall.*

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 hackers 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 enables internal access to the private and possibly the voice 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 (malicious 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, the number required would be three—that is, two for the IP phone and one for the connected PC.

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. 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 ports 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 attached.*
- *(VoIP0125: CAT II) The IAO will ensure that port security had been configured on all switchports with voice VLAN membership.*
- *(VoIP0127: CAT III) The IAO will ensure that all the maximum number of MACs 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. 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 number of possible entries into the system. These entry mediums include the Operating System, 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 Operating Systems 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, traveling personnel, teleworkers, or call centers. The use of Soft phone agent software must be controlled and should be used only after the DAA is made aware of the security risk involved and approved their use. 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 systems.

- *(VoIP0130: CAT III) 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.*
- *(VoIP01350: 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 that is provided by commercial IPT service providers.
    - Requires prior approval for the use of any IP Soft Phone agent software.
- *(VoIP0140: CAT III) The IAO will ensure that host systems, on which Soft Phones are installed, comply with the appropriate operating system STIG.*
- *(VoIP0150: CAT III) The IAO will ensure that if/when 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 and data VLAN dedicated to hosts with IP Soft Phone agents installed.
- *(VoIP0160: CAT III) The IAO will ensure that if/when Soft Phones are used in remote connectivity situations, the following conditions are met:*
    - The host computer connects to the “home LAN” through a VPN connection.
    - The VPN is terminated at the enclave boundary in accordance with the Enclave STIG
    - The IP Soft Phone agent connects to the Call Manager on the “home LAN” through the VPN using “home LAN” IP addressing.
    - The voice and data traffic is routed appropriately to separate voice and data VLANs in the “home LAN”
- *(VoIP0165: CAT III) The IAO will ensure that, if/when 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 or 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 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 me implemented.

3.7.1 Local Network VLAN to VLAN Protection

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 voice VLAN and the data VLAN. This is necessary to limit and control access from the data network to the IP telephony network. Ideally there should be no traffic flow between the voice VLAN(s) and the data VLAN(s) except in specific situations. These might be when a soft phone on the data VLAN needs to access the VoIP servers to operate or when VoIP phones on the VoIP VLAN need to access a messaging server on the data VLAN. Traffic should be limited. At minimum IP filtering should be implemented between the IP telephony network and the IP data network. There are several methods for doing this based on the amount and direction of traffic that needs to traverse the boundary. Low volume traffic or access to a specific device such as a messaging server might use an ACL on a layer 3 switch or router. Higher volume traffic, stronger security, or soft phones on the data network (implemented against policy) would require a firewall. This will mitigate possible malicious attacks that may originate from within the data network

- *(VoIP0090: CAT II) The IAO will ensure that network traffic between the data and voice VLANs is restricted to authorized devices using approved ports, protocols, and services as follows:*
    - *Voice VLAN to data VLAN communication to a limited number of servers such as a messaging server require at a minimum a layer 3 ACL on a switch or router. All access from the data VLAN to the voice VLAN will be blocked. A stateful inspection firewall is recommended.*
    - *Data VLAN to Voice VLAN communication for approved IP soft phones is implemented using a VoIP aware stateful inspection firewall with dynamic port mapping.*
- *(VoIP0095: CAT II) The IAO will ensure that the network perimeter (i.e. premise router, perimeter firewall) is configured to block all traffic destined to or sourced from the Voice VLAN IP Address space.*

3.7.2 WAN Connectivity and LAN -WAN Protection

Connections from a LAN based VoIP environment to the WAN for the purpose connections to other VoIP phones in other VoIP enclaves, remote VoIP call managers, the PSTN, or DSN is called VoIP Trunking.

3.7.2.1 Current Policy

As of this writing VoIP Trunking is not approved for use in unclassified DOD telecommunications systems. The DOD is only certifying VoIP systems at the PBX-1 and PBX-2 level, as specified in the GSCR, for inclusion on the DSN APL. These systems are specified for use at the BCPS level. No systems are being certified to use VoIP Trunking. Also, 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 traditional TDM networks, i.e. DSN and 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 enclave is routed via a media gateway to the traditional TDM networks i.e. DSN and/or PSTN. Caveat: An exception is made for approved remote soft phones that connect to the enclave via a VPN and are therefore part of the enclave.*
- *(VoIP0901: CAT II) 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 Firewall Requirements and Controls

Firewalls are required at any enclave boundary to protect the internal network. Firewalls present operational QoS problems for VoIP systems and VoIP presents security issues for the network. The customary firewalls used on data networks present operational and QoS problems for VoIP. 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 not part of a properly originated call.

To maintain the private addressing scheme on in the VoIP LAN enclave, 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 misconfigured. NAT is also a problem when it comes to VoIP 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. 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 on the network, 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 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 allow 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.

- *(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 ALG based 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 3.2 provides ports and services that should be considered in providing firewall filtering for VoIP servers and networks:

SERVICE	***PORT***
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
SNMPtrap	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

Figure 3.2. VoIP Ports and Services

Some VoIP call managers and servers utilize some commonly used protocols for their operation. These must be blocked from external access. Additionally see systems management below.

- *(VoIP0220: CAT II) The IAO will ensure MS-SQL (port 1433) is blocked at the VoIP security perimeter.*
- *(VoIP0230: CAT III) The IAO will ensure the network time protocol (NTP port 123) is blocked at the security perimeter. Clock source is derived from a locally obtained Stratum 1 timing source such as the global positioning system (GPS).*
- *(VoIP0240: CAT II) The IAO will ensure Terminal Services or remote desktop protocol (port 3389) is blocked at the security perimeter or that these connections are encrypted.*

- *(VoIP0245: CAT II) The IAO will ensure that all remote Web acc*ess through *VoIP security perimeter firewalls is proxied. Web access if required from the VoIP enclave should rout through the data enclave.*

3.8 Call Privacy and Confidentiality

When VoIP WAN connections are established, call privacy may be lost today; all DSN trunks are encrypted ensuring the privacy of subscriber calls. To ensure the same privacy as provided by the existing PSTN that subscribers have grown to expect encryption must be implemented for all WAN calls. This can be accomplished in a numbers ways. End-to-end encryption, which requires the IP telephone devices to have a great deal of processing power and the capability of supporting encryption, is not always feasible, as not all VoIP vendors provide encryption capability from the subscriber terminal. However, encryption could be accomplished at the link-level through the incorporation of VPN technology. 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 WAN connections to an IP WAN network (i.e., Internet, NIPRNet, SIPRNet) is encrypted.*

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 types of devices locally, by using out-of-band management or by secure in-band management using protocols such as SSH, SNMPv3, or 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 perimeter firewall administrative/management traffic is blocked at the perimeter, or is tunneled and encrypted using VPN technology at the security perimeter, or is out-of-band.*
- *(VoIP0250: CAT II) The IAO will ensure that all remote Web access* to *VoIP security perimeter firewalls for management purposes is proxied.*
- *(VoIP0260: CAT II) The IAO will ensure that all Web connections to VoIP security perimeter firewalls for administrative/management purposes are encrypted.*

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 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, by interacting with existing email messaging systems.

With unified mail, (combined voice mail and e-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 required above. 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, and 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 III) The IAO will ensure text-to-speech is disabled if the voice mail platform is configured to interact with the corporate email system.*
- *(VoIP0330: CAT III) 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 III) 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 quality-of-service (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. 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 III) 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.*

3.12 Securing MGCP

The MGCP protocol is the communications protocol 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.

- *(VoIP: 0040) CAT II) If MGCP is used, the IAO will ensure that IPSEC is enabled on each MGC to provide authentication and encryption.*

3.13 VoIP Connection to the Defense Switched Network (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 by the JITC.*

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) Defense Switched Network (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	Department of Defense Computer Emergency Response Team (CERT)
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. GLOSSARY OF TERMS

AAA	Authentication, Authorization, and Accountability
ACD	Automatic Call Director
ADIMSS	Advanced Defense Switched Network Integrated Management Support System
ADM	Add-Drop Multiplexer
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
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
CLI	Command Line Interface
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)
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Field Security Operations
FY	Fiscal Year
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 Announcement
IETF	Internet Engineering Task Force
IAVM	Information Assurance Vulnerability Management
I&A	Identification and Authentication
ID	Identification
IDNX	Integrated Digital Network Exchange
INFOSEC	Information Systems Security
IP	Internet Protocol
IPSEC	IP Security
IS	
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
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
MMI	an 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
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
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
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
SCCP	Signaling Connection Control Part (SS7 protocol)
SCCS	Source Code Control System
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
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
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
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