VOICE OVER INTERNET PROTOCOL (VOIP)

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

13 January 2004

DISA
FIELD SECURITY OPERATIONS

This page is intentionally left blank.

FORWARD AND ACKNOWLEDGEMENTS

This *Voice Over Internet Protocol (VoIP) Security Technical Implementation Guide* (STIG) is published as a tool to assist in the improvement of the security of Department of Defense (DOD) information systems. The document is meant for use in conjunction with the other applicable STIGs.

This page is intentionally left blank.

TABLE OF CONTENTS

Page

APPENDICES

LIST OF TABLES

1. INTRODUCTION/BACKGROUND

This *VoIP Security Technical Implementation Guide* (STIG) is published as a tool to assist in securing of Department of Defense (DOD) networks and systems supporting VoIP technology. This document is meant for use in conjunction with the Defense Switched Network (DSN), and appropriate Operating System (OS) or network STIGs.

VoIP technology offers the prospect of improved productivity through enhanced voice services for the DOD. However, with these enhanced services, comes an increased risk in exposing government information systems to security vulnerabilities. This document is intended to provide a basic overview of VoIP technologies and to provide guidance for securing the operation of VoIP supported networks and systems. The target audience for this document includes DOD functional managers, information technology personnel, and network and security administrators.

- *(VoIP0010: CAT III) The Information Assurance Officer (IAO) will ensure that VoIP systems are approved by the DAA before they are installed and/or used to store, process, or transmit DOD information.*

- *(VoIP0020: CAT II) The IAO will ensure that VoIP systems are compliant with overall network security architecture and appropriate enclave security requirements.*

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

The directives and standards cited above do not specifically address VoIP supported networks or applications, but assert a level of security that will be maintained over the entire network from terminal device to terminal device. In order to meet the security requirements of these systems, the VoIP supported network must be designed, implemented, 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 and associated support software (e.g., SQL server, IIS web server, etc.).

1.2 Authority

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

Compliance with the applicable STIG is mandatory for systems residing in a DISA facility and for any system directly administered by DISA. The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD

systems operating at the MAC II Sensitive level, containing unclassified but sensitive information

1.3 Scope

The requirements set forth in this document will assist security and DSN support personnel in implementing and meeting the minimum-security requirements addressed in higher-level documents and as required to support final accreditation. This document applies to all VoIP supported networks, systems, and devices residing in, administered, or controlled by the DISA or applicable Military Department (MilDep). This document is not limited to a single OS, hardware platform, or VoIP device.

1.4 Writing Conventions

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

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

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

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*)". If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the PDI (i.e., "[*N/A: CAT III*]"). "**Bold**" font within a policy bullet represents a change of direction that has been implemented within the current release of this document. For example, the policy now states "**should**" vs. previous policy of "**should not**."

1.5 DISA Information Assurance Vulnerability Management (IAVM) Program/Vulnerability Compliance Tracking System (VCTS) Process

DISA developed the Vulnerability Management System (VMS) as a DOD tool to notify commands, agencies, and organizations of new and potential security vulnerabilities. VCTS and the SRRDB have recently been combined into the Vulnerability Management System (VMS).

The VMS meets the DOD mandate to ensure information system vulnerability alert notifications are received and acted on by all System Administrators (SAs) and Web Managers. It provides a mechanism to ensure that new vulnerabilities are corrected within the specified period. It provides the means, via Security Readiness Review Database (SRRDB), for scheduling periodic validations of system status. Users who require access to VMS should contact the DECC-D Chambersburg Help Desk, DSN 570-5690, and commercial (717) 267-5690, e-mail **weblog@chamb.disa.mil**.

Use of VMS is mandated within DISA and available for use throughout DOD. Each DISA site will ensure all information systems and their SAs register with the VMS. A DISA information system is a system that is physically located at a DISA site or managed by DISA personnel. The VMS tracks the site implementation status of all IAVM alerts, bulletins, and technical advisories. The VMS can provide SRR review teams with a list of system specific IAVM notices as well as the applicable fixes and patches. This document includes detailed information on all IAVM notices issued that apply to this technology. Where applicable, these IAVM notices are referenced or included in summary format in this document. (IAVM notices relevant to this document are located in *Appendix J, UNIX IAVA Detection Procedures and Summary*.

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

1.7 Extensions

The local DAA must approve deviations from compliance with the STIG. If compliance cannot be resolved in a timely manner, an extension may be requested via the Vulnerability Management System Extension Process. Justification for an extension may include operational reasons, technical conflicts, and insufficient funding. An extension request will identify a plan and timetable for resolving the finding(s). Any supplemental security countermeasures should also be addressed

Deviations from the standards cannot jeopardize the MAC II controls, must be justified by a true business case for the deviation, and must not adversely affect the security of the site.

1.8 STIG Distribution

In the interest of promoting enhanced security for systems both inside DOD and within the Federal Government's computing environments, DISA encourages any interested DOD activity or party to obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

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

1.9 Document Revisions

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

2. IP TELEPHONY OVERVIEW

IP Telephony is a process that enables the transfer of voice data over a packet switched network as opposed to the traditional circuit switched network. The transmission of voice packets over the Internet Protocol (IP) is known as Voice over IP (VoIP) and 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. This section will present a very high level overview of the technology and predominant protocols used, in order to provide a basic understanding of IP Telephony or VoIP. It is not intended to provide detailed information of all vendor specific, proprietary protocols, or implementations of the VoIP technology.

2.1 VoIP Components

Although 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 supported 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 as it is needed out of the trunk links interconnecting the switches. IP networks are different from circuit switching networks, because they are a packet-based and build-on statistical availability. In short, Quality of Service (QoS) specifies a guaranteed throughput level and Class of Service (CoS) ensures that packets of a specific application are given priority. This guaranteed through put and prioritization is required for real-time VoIP applications to ensure that the voice service is unaffected by other traffic flows. For the purpose of this STIG any IP network supporting VoIP technology will be referred to as a VoIP network.

2.1.2 Call Processor/Controllers

Call processor/controllers employs 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 process/controller can also be known as a softswitch, call agent, call manager, or gatekeeper depending on its specific function in the VoIP supported network or specific vendor solution being implemented. The amount of functionality provided by a call process/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 information transported on the IP network using packet formats to pulse code modulation (PCM) encoded voice on the PSTN side and vice versa. Simply stated, the MG provides 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 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 signal system would provide both the media and signaling gateway functions and interfaces between the VoIP network and PSTN.

2.1.4 Telephony (Subscriber) Terminal

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 must provide voice communications and may offer other optional services such as data or video. The IP phone can also come in the form of an actual hardware device, i.e. a telephone desk set, or in software forms for example 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 forces 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, 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 proprietary H.323 protocol. These proprietary protocols will be addressed in future appendices of this STIG.

2.2.1 H.323 Protocol

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

Terminal - An H.323 terminal is a LAN endpoint that provides duplex 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 brain 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 and trunking 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. In response, the UAS generates a request, which may be sent to a local SIP proxy server for further processing. The UAC and the UAS can be located on the same device such as an IP-phone.

Network Servers - There are three types of SIP network servers—registration server, proxy server, and redirect server.

The *registration server* maintains an inventory of user locations within its domain. When a call is made, it is consulted so incoming calls can be correctly routed.

The *proxy server* handles SIP requests to the next server. For example, if an outbound call is initiated, the proxy server would query DNS for the destination address (URL) of the SIP server and forward the request to that machine. When the destination SIP server receives the request, it forwards the request to the destination address of the user agent being called.

The *redirect server* returns a message to the source about the next server to contact. In the above scenario, assume the destination SIP server wants calls to be forwarded to another domain. Then the SIP server acts as a redirect server by returning the new destination address.

2.2.3 Media Gateway Control Protocol (MGCP)

MGCP complements SIP and H.323. This protocol 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 MG using the H.248 (or Megaco protocol), but will communicate with other MGC via H.323 or SIP. This protocol provides a scalable approach to manage media gateways in a heterogeneous infrastructure.

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.*

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 packetized or non-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).

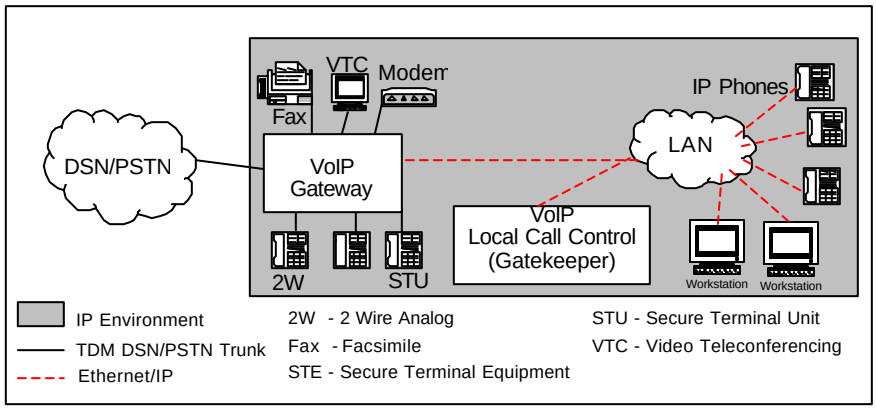

Figure 2.1. Illustration of IP Centric Architecture

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 offer 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.

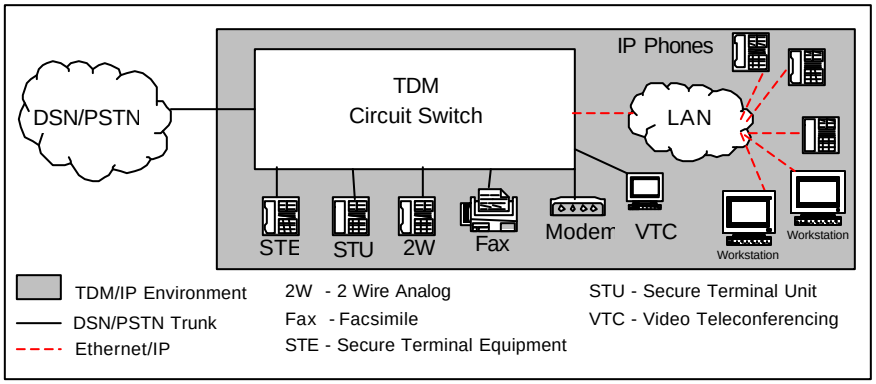

Figure 2.2. Illustration of IP Enabled (Hybrid) Architecture

2.3.3 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 Sniffing

Sniffing can result in disclosure of confidential information, unprotected user credentials, and the potential for identity theft. It also allows sophisticated malicious users to collect information about your VoIP systems that can be used to mount an attack on other systems or data that might not otherwise be vulnerable. IP 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 plugins for packet sniffers, are available on open source web sites, so 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.

2.5 Denial of Service (DoS)

Flooding the network with unnecessary data, or 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 be very effective against the VoIP system considering the Quality of Service necessary for VoIP to be functional.

2.6 Traffic Flow Disruption

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.

This page is intentionally left blank.

3. SECURING THE VOIP ENVIRONMENT

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 a 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.

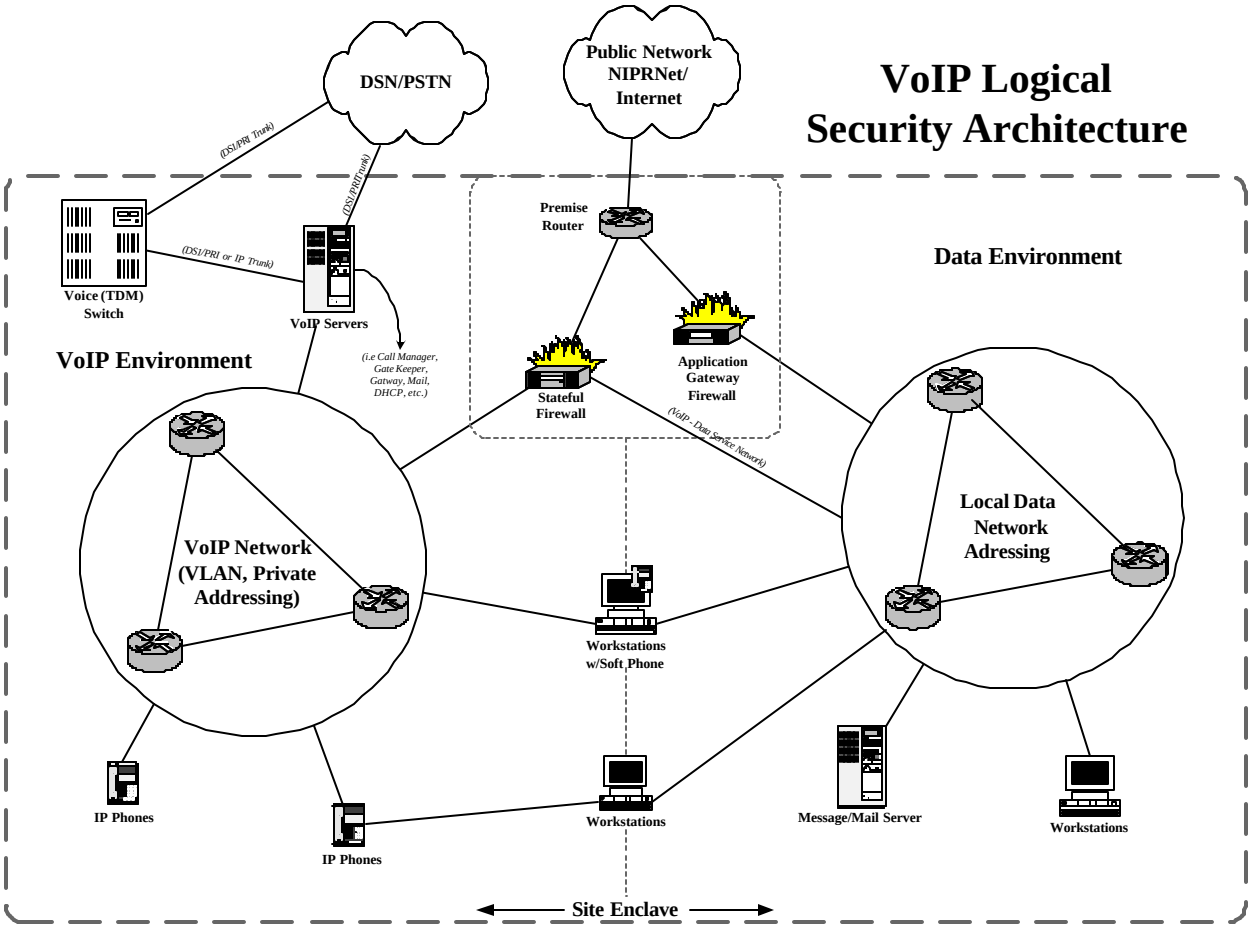

Figure 3.1. VoIP Logical Security Architecture

3.1 Physical Security

The design of the network 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.*

- *(VoIP0060: CAT III) The IAO will ensure that telephony terminals (IP phones) do not display network IP configuration information on their liquid crystal display (LCD) device.*

3.2 Logical Address Segregation

VoIP provides a means of providing telephony over an existing IP network. However, for reasons including QoS, scalability, manageability, and security, deployment of IP telephony devices and IP data devices should be deployed on two logically different IP segments. The combination of data and voice segmentation and a switched infrastructure strongly 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 IP filters will help to ensure the security and aid in protecting the VoIP environment from external threat.

All VoIP components (i.e. Gatekeepers, Call Managers, voice mail systems, IP Subscriber Terminals etc.) should be deployed on their own, separate private IP network or sub-network. Ideally, 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.

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

- *(VoIP0080: CAT II) The IAO will ensure that all VoIP systems and components are deployed using private address space IAW RFC 1918. This check does not apply to VoIP systems residing on the SIPRNet.*

Network connections may be required between the VoIP and data network segments in order to provide services such as voice mail. In this scenario, to aid in protecting the VoIP network segment, NAT should to be implemented at the VoIP/data segment connection point. Although stateful firewalls are used as outlined in the firewall section of this document to protect VoIP traffic call connections, NAT cannot be used at this connection and can only be employed between the data and VoIP segments. 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.

- *(VoIP0090: CAT II) The IAO will ensure that NAT is implemented on the VoIP segment to data segment connections.*

3.3 VLANs

VoIP traffic should be segmented from the traditional data network using Virtual Local Area Networks (VLAN). In a switched network environment, VLANs create a logical segmentation of collision domains that can span multiple physical network segments. The separation of collision domains serves to mitigate the risk that a DOS attack or packet sniffing on the data network will affect the voice network and vice versa. In addition, separating Voice and data traffic into separate collision domains will reduce competition for the network and thus reduce latency (queue/wait time) for transmission services. Since VoIP is very latency sensitive this segmentation approach is the cheapest way to improve performance in an existing network infrastructure.

VLANs can enhance the security of the VoIP environment by segmenting the voice and data for PCs that are connected via VoIP phones. This VLAN segmentation also reduces potential conflicting issues with videophones when all, voice, data, and video come from the same source.

VLAN memberships can be configured on a port-by-port basis. VLAN ports for VoIP can be secured by assigning a phone's MAC address to a single port. VLAN switch ports that are not in use by active voice equipment should be disabled or assigned to a different VLAN. In addition, some VoIP telephones have built-in network ports for the purpose of connecting a workstation. This type of VoIP telephone should support the use of configuring its network port into a separate VLAN and the ability to disable the port from use. Disabling unused VoIP VLAN ports mitigates the risk of rogue network devices being inserted into the VoIP network. To further protect against rogue devices, a VLAN port can be configured to only connect to a single MAC address.

- *(VoIP0100: CAT II) The IAO will ensure that VoIP components reside on a separate VLAN from the data network.*

- *(VoIP0110: CAT III) The IAO will ensure that VoIP VLAN ports that are not in use are disabled.*

- *(VoIP0120: CAT III) If VoIP telephones with built-in data network ports are used, the IAO will ensure that the data port is disabled when not in use, and if it is used the port must be configured on the appropriate data VLAN.*

3.4 IP Hardware Phones and Soft Phones

IP soft phone agents inherently reside in the data segment but require access to the voice segment in order to access call control, place calls, and leave voice messages. However, 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 must reside on the data segment, it is susceptible to any attack against that entire segment and not just the host itself. In contrast, IP hardware phones can reside in the VoIP segment and run proprietary Operating Systems with limited network services enabled and 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.

- *(VoIP0130: CAT III) The IAO will ensure that all Soft Phones utilize a separate dedicated NIC for VoIP VLAN access and the host system is in compliance with the applicable STIG.*

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.

- *(VoIP0140: CAT III) The IAO will ensure DAA approval prior to the use of any IP Soft Phone agent software.*

- *(VoIP0150: CAT III) The IAO will ensure a local policy exists and is being enforced that prohibits the installation and use of IP Soft Phone agent software.*

Many IP hardware phones provide a separate data port for the connection of a PC to the phone so that only a single cable is required to provide data and voice connectivity to the end user's desktop. Additionally, some IP hardware phones are only capable of providing basic layer 2 connectivity, acting like a hub and combining the data and voice network segments. While other IP phones offer enhanced Layer 2 connectivity providing the option to use VLAN technology, to place the phone and the data traffic on two different VLANs. To ensure logical separation of voice and data in order to maintain the security of the VoIP environment, only layer 2 enhanced or VLAN capable phones should be considered for use.

- *(VoIP0160: CAT II) The IAO will ensure that all IP Phones and Soft Phones are:*

  - *VLAN capable and that this function is enabled.*
  - *Assigned to the VoIP VLAN segment.*

Any connections between the voice and data network segments required for phone access to voice mail should be controlled by blocking direct data access to the voice network segment(s) to prohibit compromise from data vulnerabilities and data tunneling within the voice segments. This can be accomplished by placing firewall functions between the VoIP VLAN and the data segments. Further guidance can be found in the following sections of this document.

3.5 Firewall Controls

VoIP systems require many ports to be "opened" in firewalls to avoid a noticeable delivery delay. The protocol used for carrying VoIP traffic through the network uses a wide range of ports (10024 to 65535) to transport packets. VoIP requires four ports per connection, two for signaling and two to transmit/receive user information. Opening a range of ports this large would surely compromise any network. There are two methods that may be used to help overcome this vulnerability; dynamic port mapping and static port mapping.

Dynamic port mapping limits the range of ports that may be used for VoIP traffic. This reduces the number of ports that are opened on the network, but with four ports (1023 and above) 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. 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.

Firewalls, routers, and switches should be implemented in a manner that will compartmentalize the VoIP servers from unauthorized access. This is necessary to limit and control access from the data network to the IP telephony network, firewall controls are to be placed in front of all networks and components supporting VoIP servers. At minimum IP filtering should be implemented between the IP telephony network and the IP data network. This will mitigate possible malicious attacks that may originate from within the data network.

- *(VoIP0170: CAT II) The IAO will ensure that Stateful Firewall filtering is implemented to protect and control access to networks and critical servers supporting the VoIP environment.*

WAN-to-WAN VoIP connections may have application filtering issues when using the H.323 protocol. This problem is encountered when return TCP connections on higher range ports attempt to establish. Therefore, H.323 aware stateful firewalls must be used at WAN-to-WAN VoIP call connection network points.

- *(VoIP0180: CAT II) The IAO will ensure that H.323 aware stateful firewalls are deployed at all WAN-to-WAN connections providing VoIP call connectivity.*

- *(VoIP0190: CAT III) The IAO will ensure that all VoIP security perimeter firewalls that process voice traffic control H.323 call setup and termination (ports 1720, 11000-11999, and 16384-32767).*

- *(VoIP0200: CAT III) The IAO will ensure all VoIP security perimeter firewalls are dedicated to VoIP traffic to reduce transmission latency caused by access control list (ACL) processing.*

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
DNS	UDP 53
NTP	UDP 123
LDAP	TCP 389
H.323RAS	TCP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
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

3.6 VoIP Firewall Management

In order to ensure the security of VoIP perimeter firewalls it is imperative that administrative/management connections and access to the devices be controlled. This can be accomplished by accessing these types of devices locally or by tunneling using the IPSec protocol 51, encapsulated secure payload (ESP).

- *(VoIP0210: CAT 210) The IAO will ensure VoIP perimeter firewall administrative/management traffic is blocked at the perimeter or tunnel/encrypted using VPN technology at the security perimeter (ports 69, 161, 162, 389).*

- *(VoIP0220: CAT 220) 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 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.*

- *(VoIP0250: CAT II) The IAO will ensure that all remote Web access to VoIP security perimeter firewalls is proxied (ports 80, 8080, 443, 8002, and 8003).*

- *(VoIP0260: CAT II) The IAO will ensure that all Web connections to VoIP security perimeter firewalls for administrative/management purposes are encrypted.*

3.7 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.

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 are 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 applicable STIG guidelines (i.e., UNIX, Microsoft NT/Win2K, DSN, etc.).*

3.8 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 WAN-to-WAN VoIP Connections

When WAN-to-WAN VoIP connections are established, call privacy is 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-to-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. If implemented, either method would be transparent to the subscriber community.

- *(VoIP0300: CAT II) The IAO will ensure that all VoIP traffic that is sent over a public IP network (i.e., Internet, NIPRNet) is 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, the voice mail server should be 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. 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.*

- *(VoIP0320: CAT II) The IAO will ensure a stateful firewall is installed between the Voice VLAN and the data network to deny all traffic that is not necessary for voice calls or voice messages to be transferred between the Voice VLAN and the data network if the voice mail platform is connected to the data network.*

- *(VoIP0330: CAT III) The IAO will ensure the server hosting the Voice Mail Service is properly secured by following the applicable STIG (i.e., OS, Database, Web).*

- *(VoIP0340: CAT III) The IAO will ensure the application services (SQL, IIS, Apache, Oracle, etc.) supporting the voice mail service are properly secured according to the appropriate 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, VoIP over 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 VoIP Connection to the Defense Switched Network (DSN)

When a VoIP network is connected to the Defense Switched Network connection approval issues, among others, are of concern. In addition to QoS problems with VoIP technology, one of the greatest security concerns regarding the VoIP technology is the sharing of network infrastructure and resources to provide both voice and data communication, and the priority of service that VoIP can provide to Command and Control (C2) and Special C2 users. With the VoIP terminals connected to the LAN, the task of securing the DSN network poses new challenges to the IAO. As VoIP further develops and standardizes, additional specific security measures will be required and will be outlined in the future new release of this document. Additional DSN security information can be found in the Defense Switched Network (DSN) STIG.

Currently there are ongoing testing efforts to certify the interoperability and security of VoIP technology. However, at this time VoIP has not been certified for use or connection to the DSN. Any VoIP network connected to any DSN switch poses a potential security risk to the DSN and should not be connected until certification by the DISA Joint Interoperability Test Command (JITC) is completed. As of this document, no VoIP solution has been certified by the JITC, and in accordance with Public Law 107-314, no system can connect to the DSN without JITC certification. Finalization of JITC certification is not projected until late 2004.

- *(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.*

Even though all of the above issues have not been resolved with VoIP, the technology is still being deployed within the DSN. Current Joint Staff VoIP policy guidance is contained in the *Interim Voice Over Internet Protocol (VoIP) Policy Message*, December 2002. This message can be found in *Appendix E, Interim Voice Over Internet Protocol (VoIP) Policy Message*, of this document. If VoIP is being used, the following will apply:

- *(VoIP0380: CAT II) The IAO will ensure Voice Over IP is not the primary voice communications system for C2 users.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government 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.

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

Department of Defense Instruction 8500.2, 6 February 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.

Information Technology Laboratory National Institute of Standards and Technology (NIST), "Security Considerations for Voice Over IP Systems" (Draft), October 2003.

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

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. CISCO PLACEHOLDER

This page is intentionally left blank.

APPENDIX C. NORTEL PLACEHOLDER

This page is intentionally left blank.

APPENDIX D. AVAYA PLACEHOLDER

This page is intentionally left blank.

APPENDIX E. INTERIM VOICE OVER INTERNET PROTOCOL POLICY MESSAGE

RATUZYUW RUEOMFA7556 3511542-UUUU--RUEKAMH
ZNR UUUUU ZUI RUEOMCF2496 3511542
R 171649Z DEC 02
FM JOINT STAFF WASHINGTON DC//JSJ6//
TO AIG 915
ZEN/=DOD/OU=JCS/OU=MAIL LISTS/OU=MLMCEB/CN=ML 915 ACTION(N) INFO
RUEKJCS/USMCEB WASHINGTON DC
RUEKJCS/JOINT STAFF WASHINGTON DC//J6/J6B//
ZEN/OU=JCS/OU=MAIL LISTS/OU=MLMCEB/CN=ML 915 INFORMATION(N) BT
UNCLAS
QQQQ
SUBJ: INTERIM VOICE OVER INTERNET PROTOCOL (VOIP) POLICY UNCLAS

UNCLAS
MSGID/GENADMIN/USMCEB//
SUBJ/INTERIM VOICE OVER INTERNET PROTOCOL (VOIP) POLICY//
GENTEXT/REMARKS//
POCS/LT COL BILL MORROW JS/J6T/-/TEL: DSN 312-225-5898 COMM: 703-695-5898/EMAIL: WILLIAM.MORROW@JS.PENTAGON.MIL/
LT COL LINDA MEDLER/ASST MILSEC MCEB/-/TEL: 703-614-7924/EMAIL: LINDA.MEDLER@JS.PENTAGON.MIL/

1. THERE ARE OVER 200 KNOWN TESTBEDS, TRIALS, AND ACTUAL DEPLOYMENTS OF VOIP SOLUTIONS THROUGHOUT DOD. SINCE INDEPENDENT IMPLEMENTATION OF VOIP COULD RESULT IN "STOVE PIPE" SOLUTIONS AND THREATEN NETWORK SECURITY AND INTEROPERABILITY, THE MCEB TASKED AND RECEIVED A COORDINATED OSD/C3I, J6, AND INTEROPERABILITY POLICY AND TESTING PANEL (IPTP) VOIP POLICY RECOMMENDATION BRIEFING ON 24 OCT 02. THE PURPOSE OF THIS MESSAGE IS TO DISSEMINATE THE MCEB APPROVED INTERIM POLICY FOR VOIP.

2. CURRENT VOIP TECHNOLOGY DOES NOT YET MEET THE STANDARDS AS SET FORTH FOR DOD VOICE SYSTEMS IN CJCSI 6215.01B IN THAT IT DOES NOT PROVIDE BOTH ORIGINATION AND RECEPTION OF "ASSURED CONNECTIVITY" OR NONBLOCKING RESPONSIVE SERVICE FOR C2 AND SPECIAL C2 USERS WHO USE DSN FOR BOTH PRECEDENCE AND ROUTINE VOICE, DIAL UP DATA, AND DIAL UP VIDEO SERVICES. FURTHERMORE, NO VOIP SYSTEM HAS BEEN TESTED OR CERTIFIED TO MEET THE STANDARDS FOR NETWORK GRADE OF SERVICE OR THE VOICE QUALITY OF SERVICE.

3. THE INTERIM VOIP POLICY IS AS FOLLOWS:
(A) PERMITS THE CONTINUED LIMITED DEPLOYMENT OF VOIP WHILE PROHIBITING THE USE OF VOIP AS THE ONE AND ONLY VOICE COMM CAPABILITY AVAILABLE FOR C2 USERS.
(B) C2 USERS MUST RETAIN TRADITIONAL DSN OR DRSN CONNECTIVITY UNTIL VOIP TECHNOLOGY CAN MEET THE APPROVED DOD STANDARDS.
(C) IN ADDITION, THE CC/S/A'S MUST RECOGNIZE THAT ALL VOIP IMPLEMENTATIONS WILL ULTIMATELY NEED TO COMPLY WITH AND/OR MIGRATE TO THE DOD STANDARDS FOR ARCHITECTURE, SECURITY, IMPLEMENTATION, AND CONNECTIVITY, AS THEY ARE DEVELOPED SPECIFICALLY FOR VOIP C2 USE.

4. THIS VOIP POLICY WILL BE INCORPORATED IN TO THE NEXT REVISION OF CJCSI 6215.01B AND THE JOINT TECHNICAL ARCHITECTURE (JTA).

5. TO DEFINE DOD'S FUTURE USE OF VOIP, DISA HAS BEEN TASKED BY THE MCEB TO DEVELOP A DOD-LEVEL PLAN OF ACTION TO ADDRESS AND SOLVE THE TECHNOLOGY ISSUES ASSOCIATED WITH MIGRATION TO THE USE OF VOIP. DISA IS ALSO WORKING WITH JITC TO DEVELOP THE DOD STANDARDS FOR BOTH JITC CERTIFICATION AND DSN DAA ACCREDITATION (PER DITSCAP) FOR VOIP. ACCOMPLISHMENT OF THIS DOD-LEVEL PLANNING AND STANDARDIZATION REQUIRES COLLABORATION WITH THE CC/S/A'S TO ENSURE IT MEETS YOUR REQUIREMENTS.

6. POINT OF CONTACT FOR THIS MESSAGE IS LT COL BILL MORROW, JS/J6T, DSN 312-225-5898, COMM: 703-695-5898, EMAIL: WILLIAM.MORROW@JS.PENTAGON.MIL.//

*** NON-IMPORTABLE ATTACHMENT(S) DROPPED FROM MESSAGE ***
ATTACHMENT TYPE: FILE TRANSFER
FILE NAME: WINMAIL.DAT
BT

JOINT STAFF V1 4
ACTION (U,6,8,F)
INFO NMCC:CWO(*) CMAS(*) CMAS(*) J6(1)
USMCEB(1) USTRANSCOMWO(1) JSAMS(1)
JSAMS UNCLAS DMS(*)

SECDEF V2 0
ACTION (U)
INFO CHAIRS(*) CHAIRS TESTBED(*) SECDEF-C(*)
SECDEF-C(*) C3I-DASD-DCIO(*) C2DIR(*) ESC-SMTP(*)
+JCP EMAIL CUSTOMER//CHAIRS//

APPENDIX F. LIST OF ACRONYMS

AIS	Automated Information Systems
ATM	Asynchronous Transmission Mode
C2	Command and Control
CA	Certification Authority
CAT	Category
C&A	Certification and Accreditation
CCB	Configuration Control Board
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
CJCSI	Chairman, Joint Chiefs of Staff Instruction
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 Telephone Integration
CTIM	Computer Telephone Integration Manager
DAA	Designated Approving Authority
DC	Domain Component
DECC	Defense Enterprise Computing Center
DIAM	Defense Intelligence Agency Manual
DISA	Defense Information Systems Agency
DISAC	DISA Circular
DISAI	DISA Instruction
DISN	Defense Information Systems Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DNS	Domain Name System
DOD	Department of Defense
DODD	Department of Defense Directive
DOS	Denial of Service
DRSN	Defense Red Switched Network
DSN	Defense Switched Network
EMS	Element Management System
EO	End Office
EOS	End Office Switch
ES	End System
ESP	Essential Service Protection

FIPS	Federal Information Processing Standard
FM	Fault Management
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Field Security Operations
GOSC	Global Operations and Security Center
GOTS	Government-Off-The-Shelf
GPS	Global Positioning System
GUI	Graphical User Interface
HID	Host Intrusion Detection
HTTP	Hyper Text Transfer Protocol
IAW	In Accordance With
I&A	Identification and Authentication
IAO	Information Assurance Officer
IAM	Information Assurance Manager
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ID	Identification
IETF	Internet Engineering Task Force
INFOSEC	Information Systems Security
IP	Internet Protocol
IPSEC	IP Security
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunications Union
JTAPI	Telephony Application Programming Interface
JITC	Joint Interoperability Test Command
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mission Assurance Category
MAC	Media Access Control
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
MS	Microsoft
MUX	Multiplexer

NAT	Network Address Transalation
NCS	National Communications System
NIPRNet	Non-Classified (But Sensitive) Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSO	Network Security Officer
NTISSP	National Telecommunications and Information Systems Security Policy
NTP	Network Time Protocol
OCONUS	Outside CONUS
OPSEC	Operations Security
OS	Operating System
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
PC	Personal Computer
PCM	Pulse Code Modulation
PDI	Possible Discrepancy Identifier
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QBE	Query by Example
QoS	Quality of Service
RAS	Remote Access Service
RFC	Request For Comment
SA	System Administrator
SCCS	Source Code Control System
SCCP	Signaling Connection Control Part
SDID	Short Description Identifier
SG	Signaling Gateway
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRR	Security Readiness Review
SRRDB	Security Readiness Review Data Base
SS7	Signaling System Seven
SSAA	System Security Authorization Agreement
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
TAPI	Telephony Application Programming Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VCTS	Vulnerability Compliance Tracking System
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network