Committee on National Security Systems

CNSS Instruction No. 5000
April 2007

GUIDELINES FOR VOICE OVER INTERNET PROTOCOL (VoIP) COMPUTER TELEPHONY

Committee on National Security Systems

CNSS Instruction No. 5000

CHAIR

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony," contains guidance for providing on-hook security for telephone systems located in areas where sensitive government information is discussed. Implementation of this instruction does not preclude the application of more stringent requirements and may not satisfy the requirements of other security programs such as TEMPEST, COMSEC (Communications Security), or OPSEC (Operational Security).

2. The National Telecommunications Security (NTS) Working Group (WG), formerly known as the Telecommunications Security Group (TSG), is the primary technical and policy resource in the U.S. Intelligence Community (IC) for all aspects of the Technical Surveillance Countermeasures (TSCM) Program involving telephone systems located in areas where sensitive government information is discussed.

3. TSG Standards will be replaced by and issued as CNSS Instructions (CNSSIs). Director Central Intelligence Directive (DCID) No. 6/9, Reference b., delineated TSG Standards and Information Series compliance by Sensitive Compartmented Information Facilities (SCIFs) for the protection of sensitive information and unclassified telecommunications information processing systems and equipment; SCIF compliance shall now be fulfilled in accordance with the appropriate CNSSIs.

4. CNSS Instruction No. 5000 is effective upon receipt.

5. Copies of this instruction may be obtained by contacting the Secretariat at 410.854.6805 or www.cnss.gov.

6. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

/s/
KEITH B. ALEXANDER
Lieutenant General, U.S. Army

CNSS Secretariat (I922) / National Security Agency
9800 Savage Road - Suite 6716 - Ft Meade MD 20755-6716
Office: (410) 854-6805 / Unclassified FAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL GUIDELINES
FOR
VOICE OVER INTERNET PROTOCOL (VOIP) COMPUTER TELEPHONY

SECTION I – PURPOSE

1. This instruction prescribes the requirements for the secure implementation and use of a VoIP Telephony system in any U.S. Government or government contractor sensitive area where national security systems (NSS) are employed and/or within environments where national security information (NSI) is stored, processed, or transmitted. The requirements established in this standard are necessary in order to achieve on-hook audio security for VoIP telephones and/or systems located in sensitive discussion areas.

SECTION II – SCOPE

2. The provisions of this instruction apply to all unclassified VoIP Telephony Systems that are currently installed, or will be installed, in U.S. Government or U.S. Government sponsored contractor spaces where NSS are employed and/or within environments where classified NSI is stored, processed, transmitted, or when used as a point of isolation in accordance with (IAW) Reference h.

SECTION III – REFERENCES

3. References are listed in ANNEX A.

SECTION IV – DEFINTIONS

4. Definitions in CNSSI No. 4009, Reference f., apply to this policy; additional policy-specific terms are defined in ANNEX B.

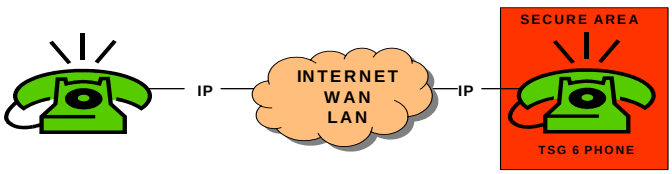
SECTION V – GENERAL OVERVIEW

5. In a VoIP configuration, the telephone instruments are connected via a distributed network to the "telephone switch." The instrument's connection, therefore, is no longer restricted to the "telephone switch" alone, but can be addressed by other devices on the network. Additionally, the VoIP telephone instrument is remarkably different from the conventional telephone attached to a traditional Computerized Telephone System (CTS). A VoIP instrument is essentially a computer with microphone and network connectivity, while many have a built-in web server to permit easier administration of its features. It follows that the administration of the "telephone switch" is no longer limited to a dedicated hardwire connection, but to a distributed network. This substantially reduces the security of the "telephone switch" that previously had sole control over the telephone configuration. Also, note that most traditional CTSs use proprietary protocols whereas most VoIP configurations use open-standard protocols. The use of an open-standard protocol increases the number of individuals who are knowledgeable about system commands, escalating the possibility that someone could compromise the system.

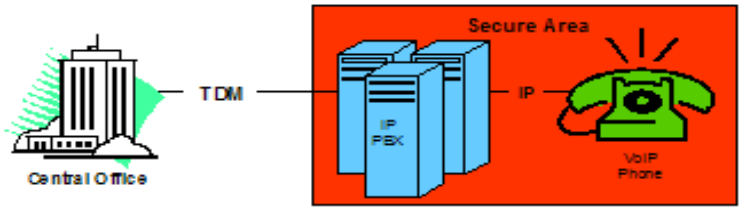
SECTION VI – REQUIREMENTS

6. The requirements of this document cover the above VoIP Telephony Systems but do not specifically address network Certification and Accreditation (C&A) requirements mandated by many organizations. Since VoIP networks may also need to conform to the specific C&A requirements of the individual departments or agencies, contact the appropriate C&A authority for guidance. The security requirements for each of the following configurations are specified in a separate annex, which forms a part of this guideline. General requirements are also discussed in SECTION VII – "Overview of VoIP Telephone System Security." This instruction will be revised to update the applicable sections or annexes as technology changes occur that impact the existing documentation.

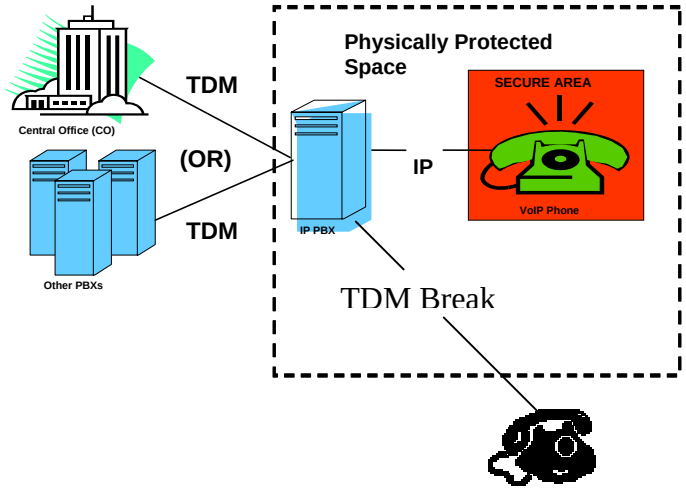
a. Pure VoIP (Annex D). A Pure VoIP, illustrated below, is Internet Protocol-based (IP) for all end-to-end communications and signaling. Reference j. listed instruments provide security in a Pure VoIP System.



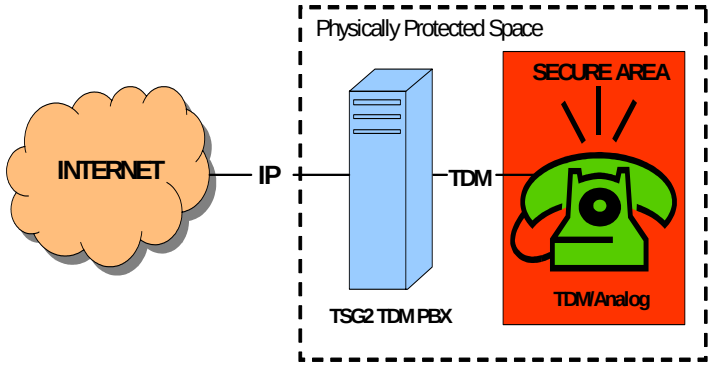
b. Isolated VoIP (Annex E). An Isolated VoIP, illustrated below, uses a mix of traditional Time Division Multiplexing (TDM) and VoIP technologies similar to Hybrid VoIP, but is exclusively for secure area use. The IP Private Branch Exchange (PBX), telephones, and associated wiring must be located in the secure area. Only the TDM trunk lines may be located outside the secure area.



c. Hybrid VoIP (Annex F). A Hybrid VoIP, illustrated below, uses a mix of traditional TDM and VoIP technologies to complete the end-to-end call. However, unlike Isolated VoIP, the IP PBX is not required to be located in the secure area. Rather, it must be located in a Physically Protected Space (PPS). All signal lines must be protected to the same level as the PPS.



d. VoIP Trunk (Annex G). The trunk line is VoIP and the end telephonic device(s) and PBX is TDM as illustrated below. Either the Instrument or the TDM PBX provides security.



SECTION VII – OVERVIEW OF VOIP TELEPHONE SYSTEM SECURITY

7. Unclassified VoIP systems in secure areas shall not pass and/or transmit sensitive audio discussions when they are idle and not in use. Additionally, these systems shall be configured to prevent external control or activation. The concepts of "on-hook" and "off-hook" audio protection, outlined in References h., must be incorporated into VoIP systems.

8. Unclassified VoIP telephone systems and services shall be configured to prevent technical exploitation or penetration. In addition, these systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data. The following specific requirements are applied to unclassified VoIP systems:

a. Provide on-hook audio protection by the use of instrument(s), cited in Reference j., or equivalent system configuration, cited in Reference h.

b. Provide off-hook audio protection by use of a hold feature, modified handset (i.e., Push-To-Talk (PTT)), or equivalent.

c. Provide isolation by use of a properly accredited VoIP computerized network with software and hardware configuration control and control of audit reports (e.g., station message detail reporting, call detail reporting...). System programming will not include the ability to place, or keep, a handset off-hook. Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated.

d. Equipment used for administration of VoIP telephone systems is installed inside an area where access is limited to authorized personnel. When local or remote administration terminals are not or cannot be contained within the controlled area, and safeguarded against unauthorized manipulation, then the use of approved telephone instruments, cited in Reference j., shall be required regardless of the VoIP Network configuration.

9. All unclassified VoIP systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems IAW References a. through d.

10. Unclassified information systems must be safeguarded to prevent manipulation of features and software that could result in the loss/compromise of sensitive audio information or protected data. An unclassified VoIP network may be subjected to C&A.

SECTION VIII – RESPONSIBILITIES

11. Heads of Federal Departments and Agencies shall:

a. Develop, fund, implement, and manage programs necessary to ensure that the goals of this policy are achieved and that plans, programs, and CNSS issuances that implement this policy are fully supported.

b. Incorporate the content of this policy into annual user education, training, and awareness programs.

Encl:

ANNEX A	References
ANNEX B	Definitions
ANNEX C	List of Acronyms
ANNEX D	Pure VoIP Security Requirements
ANNEX E	Isolated VoIP Security Requirements
ANNEX F	Hybrid VoIP Security Requirements
ANNEX G	VoIP Trunk Security Requirements

ANNEX A

REFERENCES

a. Code of Federal Regulations, Title 32 - National Defense, Volume 6, "Part 2004 – Directive on Safeguarding Classified National Security Information," Revised July 2003.

b. Director of Central Intelligence Directive (DCID) No. 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities," November 2002.

c. Director of Central Intelligence Directive (DCID) No. 6/2, "Technical Surveillance Countermeasures," March 1999.

d. Security Policy Board Issuance 6-97, "National Policy on Technical Surveillance Countermeasures," September 1997.

e. National Institute for Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," 25 May 2001.

f. CNSS Instruction No. 4009, "National Information Assurance (IA) Glossary," Revised June 2006.

g. Telephone Security Group (TSG) Standard 1, "Introduction to Telephone Security," March 1990.

h. Telephone Security Group (TSG) Standard 2, "TSG Guidelines for Computerized Telephone Systems," Revised September 1993.

i. Telephone Security Group (TSG) Standard 5, "On-Hook Telephone Audio Security Performance Specifications," March 1990.

j. Telephone Security Group (TSG) Standard 6, "Telephone Security Group Approved Equipment," Revised September 2000.

ANNEX B

DEFINITIONS

Terms used in this policy are defined in Reference f., with the exception of the following, although some additional terms are defined in References g. and h.

a. Disabled: A function or component that is disabled by requirement shall not be re-enabled through any action by a user or the network.

b. Internet Protocol: IP is part of the TCP/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages.

c. Internet Protocol Private Branch Exchange: A private branch exchange that utilizes IP protocols in a packet switched environment. This includes all the computer and IP network resources required for the VoIP implementation.

d. Hybrid VoIP: A VoIP configuration using a mix of traditional Time Division Multiplexing (TDM) and VoIP technologies to complete an end-to-end call.

e. Isolated VoIP: A VoIP configuration that is exclusively for secure area use.

f. Other Network Protocols: Any other networking or management scheme in which data is transmitted or received (e.g., Frame Relay, Asynchronous Transfer Mode).

g. Physically Protected Space: A space within a physically protected perimeter. This area must be locked and access limited to cleared US personnel requiring access to the system.

h. Pure VoIP: A VoIP configuration that is IP-based for all end-to-end communications and signaling.

i. Simple Network Management Protocol (SNMP): A protocol enabling system administrators to monitor and manage a network of connected computers.

j. Transmission Control Protocol/Internet Protocol (TCP/IP): The suite of communications protocols used on the Internet. While TCP and IP are the most commonly used, TCP/IP also includes several other protocols.

k. Time Division Multiplexing (TDM): TDM is, in this instance, indicating a circuit switched link (POTS, T1, ISDN, proprietary digital, etc.). Circuit switched

protocols are generally less vulnerable, something the NTSWG has relied upon as part of the security posture of a telephone system.

l. Voice Over Internet Protocol: A term used to describe the transmission of packetized voice using IP and consists of both signaling and media protocols.

m. Voice over IP Firewalls: A primary function at the Application Layer and protects against vulnerabilities specifically associated with VoIP as well as other telephony concerns. VoIP firewalls can dynamically open and close ports associated with call setup and teardown.

n. VoIP Trunk: A VoIP configuration in which the trunk line is VoIP and the end telephonic device(s) and PBX is TDM.

ANNEX C

List of Acronyms

ACL	Access Control List
C&A	Certification & Accreditation
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMSEC	Communications Security
CTS	Computerized Telephone Systems
DCID	Directive of Central Intelligence Directive
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standards
IA	Information Assurance
IC	Intelligence Community
IAW	In Accordance With
IP	Internet Protocol
IP PBX	Internet Protocol Private Branch Exchange
LAN	Local Area Network
MAC	Media Access Control
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
NTS	National Telecommunications Security
NTSWG	National Telecommunications Security Working Group
OPSEC	Operational Security
OS	Operating System
PBX	Private Branch Exchange
PPS	Physically Protected Spaces
PTT	Push to talk
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing - Circuit switched
TSCM	Technical Surveillance Countermeasures
TSG	Telephone Security Group
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WG	Working Group

ANNEX D

Pure VoIP Security Requirements

1. This annex specifies security requirements for deploying a Pure VoIP voice/data solution. Since the user cannot control the Pure VoIP network, only telephone instruments listed in Reference j. may be used.

2. This document does not address the C&A requirements that many organizations require. Consult with your network accreditation authority for guidance.

3. **Voice Instrument Security.** Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal. The following provisions must be implemented to promote on-hook and off-hook [audio] security in VoIP telephone instruments.

a. Microphone Disconnect. Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of the speakerphone microphone.

b. Identifiable Telephones. Telephones must be easily identifiable as NTSWG approved.

c. Audio Reverse Flow. Speakers used to output audio from a VoIP (telephony) feature must be equipped with amplifier circuits (op-amps or one-way amplifiers) that prevent the reverse flow of audio from the speaker transmit talk path. Side tone circuits are permitted provided they merely feed transmit audio to the local speaker receive circuit.

d. Handset/Headset Disconnect. Handsets/headsets used to process audio for VoIP (telephony) applications must have a means to positively disconnect the microphone and earpiece element from the circuit when not in use. The disconnect must be hardware controlled and must not rely on software controls alone. Compliance may require the use of PTT handsets.

e. Hold/Mute Feature. The VoIP (telephony) application must feature a "hold" function whereby local audio is shunted from the circuit when active. Similarly, when the mute feature is enabled, audio is shunted from the circuit. The "hold" or "mute" feature must be enabled/disabled from the local end only and must not be re-configurable from the distant/calling end of the circuit (i.e., such as a firmware feature). When the hold or mute features are enabled, the audio shunt must be designed to remove the audio path from the transmit circuit so that no digitized audio is present.[2] If these requirements cannot be met, then PTT handsets are required.

f. Telephone Audio Security. For systems in a classified area, the system shall ensure telephony audio security iaw Reference i., On-hook Telephone Audio Security Performance Specifications, telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition. Reference j. listed instruments are required in areas where classified information may be discussed.

g. Unnecessary Telephone Functionality. VoIP telephone instrument functionality shall be limited to typical telephony functions. Unnecessary functionality shall be disabled. Users of VoIP telephones shall not be able to view administrative settings or settings such as IP or Media Access Control (MAC) addresses.

(Note: Such information could enable a user to gain information about the network or potentially spoof a device and gain unauthorized access.)

h. Unnecessary Telephone Services. Services other than those necessary to process VoIP telephone conversations and related VoIP functions (e.g., call setup) shall be disabled. Web services or the ability to browse the web with a VoIP telephone shall be disabled.

i. Speech Processing Software and Telephone Data Ports. Speech to text conversion capability shall not be enabled.

[2] Some VoIP vendors have designed hold and mute features that "flip a bit" to indicate the activation of the feature, but permit the actual transport of audio along the network connection.

ANNEX E

Isolated VoIP Security Requirements

1. This annex specifies security requirements for deploying an Isolated VoIP configuration where the VoIP system is located in a secure area for which it provides exclusive service and the only equipment or wiring outside the secure area are the TDM trunk lines. These requirements apply to a VoIP PBX that exclusively uses TDM trunk lines, whether copper or fiber. Any current or planned IP connectivity outside of the switch must follow the requirements listed in Annex D. No wireless capability is permitted. VoIP networks must be physically separated from other IP networks.

2. This document does not address the C&A requirements that many organizations require. Consult with your network accreditation authority for guidance.

(Note: This install is similar to a traditional installation, cited in Reference h., in that the isolation is provided to the VoIP network by the TDM gateway. Specifically, when a telephone instrument is placed in the on-hook condition it will be disconnected at that point from the outgoing TDM trunks.

3. **Voice Instrument Security**. Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal. The following provisions must be implemented to promote on-hook and off-hook [audio] security in VoIP telephone instruments.

a. Microphone Disconnect. Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of any internal microphones.

b. Telephone Audio Security. VoIP telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition.

c. Telephone Functionality. VoIP telephone instrument functionality shall be limited to telephony related functions.

d. Speech Processing Software and Telephone Data Ports. Speech processing software/ application shall not be enabled for any computerized applications. To ensure data and voice segregation, the data port on the VoIP telephone device shall be disabled.

e. Firmware Upgrades and Configuration File Integrity. A management process must be implemented to ensure that appropriate files are vendor signed and/or

authenticated. The files must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

4. Physical Security.

a. Trunk Line Location. Only the TDM trunk lines may transgress the secure area. The PBX shall be located as close to the demarcation point as practical. All system wiring interconnections will be organized to facilitate technical inspections

b. Program Media Protection. All program media such as tapes or disks must be provided physical protection to prevent unauthorized alterations.

c. Program Master Copy. An up-to-date master copy of the program must be maintained for confirmation and/or reloading of the operating program. This master copy must be verifiable as having been protected against unauthorized alteration. The current program master copy must be maintained in a physically protected storage container, separate from all other program media.

5. **IP PBX Security**. Only the authenticated and authorized VoIP system administrators are permitted to make changes to the system configuration and programming. Authenticated and authorized users are restricted to the use of only VoIP instruments to change preferences (e.g., ring tones, speed dial lists…).

a. Auditing. This function must be configured to monitor successful and failed access attempts to the device, all configuration settings changes (or attempted changes), and any other management control functions. These audit logs shall be enabled by default and the contents reviewed regularly, IAW organizational security policies.

b. Access Control.

1. Access control lists (ACL) shall be configured on the IP PBX to prevent administrative actions being performed from unauthorized devices or users. The system shall be configured such that administrative functions must be performed from an administrative workstation using a dedicated out-of-band management network. Secondary user authentication shall also be implemented (e.g., Authentication, Authorization, and Accounting Server).

2. Privileged account protection, if an out-of-band management network is not possible, an equivalent level of protection shall be provided for administrative usernames and passwords to prevent unauthorized disclosure of privileged accounts. These administrative usernames and passwords shall be protected IAW NIST FIPS 140-2 encryption, Reference e., via a secure protocol such as Secure Shell (SSH) or Secure Socket Layer (SSL).

3. Usernames and passwords, IAW organizational security requirements, shall be required prior to providing access to the administrative functions of the IP PBX. In addition to required authentication, strong passwords shall be used. Such passwords must consist of a minimum combination of three of the four character types (i.e., uppercase, lowercase, numbers, and special characters) and a minimum length of eight characters.

c. Patch Management. A process must be implemented to ensure that the latest available security patches are applied. The patches must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

ANNEX F

Hybrid VoIP Security Requirements

1. This annex specifies security requirements for deploying a Hybrid VoIP voice/data solution. This solution is where the VoIP system uses a VoIP PBX that is located outside of the secure area, but within a PPS that is also controlled by the organization having oversight of the secure area. The VoIP System may only use TDM trunk lines, whether copper or fiber, for connectivity to other phone systems external to the PPS or central office. No wireless capability is permitted.

(Note: This Annex covers hybrid VoIP configurations wherein the VoIP system also provides phone support to areas outside the secure areas. Hybrid VoIPs exclusively for secure area use are defined as Isolated VoIPs and are covered in Annex B of this standard.)

2. This document does not address the C&A requirements that many organizations require. Consult with your network accreditation authority for guidance.

3. VoIP networks must be either physically separated or have logical Virtual Local Area Network (VLAN) separation from other IP networks to ensure isolation between voice and data networks. Physical separation of the networks provides a higher level of security and is the preferred method of isolation. Any IP connectivity from the voice network to other Local Area Networks (LAN), Wide Area Networks (WAN), or Internet negates this solution and requires compliance with Annex A. IP trunking is not allowed in this configuration.

4. Under this solution, the VoIP server may also provide telephone support to areas outside the secure area. In this instance, the VoIP telephones used outside the secure area must meet the security requirements listed below under Voice/Data Network, paragraph 6.c.2. Additionally, these phones require a TDM break located within the PPS. Other methods that provide a similar level of isolation may be approved by the NTSWG.

5. **Voice Instrument Security**. Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal. The following provisions must be implemented to promote on-hook and off-hook [audio] security in VoIP telephone instruments.

a. Microphone Disconnect. Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of any internal microphones.

b. Identifiable Telephones. Telephones must be easily identifiable as meeting the security requirements of this annex.

c. Handset/Headset Disconnect. Handsets/headsets used to process audio for VoIP (telephony) applications must have a means to positively disconnect the microphone and earpiece element from the circuit when not in use. The disconnect must be hardware controlled and must not rely solely on software controls. Compliance may require the use of PTT handsets.

d. Hold/Mute Feature. The VoIP (telephony) application must feature a "hold" function whereby local audio is shunted from the circuit when active. Similarly when the mute feature is enabled, audio is shunted from the circuit. The "hold" or "mute" feature must be enabled/disabled from the local end only and must not be re-configurable from the distant/calling end of the circuit (i.e., such as a firmware feature). When the hold or mute features are enabled, the audio shunt must remove the audio path from the transmit circuit so that no digitized audio is present.[3] If these requirements cannot be met, PTT handsets are required.

e. Telephone Audio Security. VoIP telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition.

f. Unnecessary Telephone Functionality. VoIP telephone instrument functionality shall be limited to typical telephony functions. Unnecessary functionality shall be disabled and administratively protected by use of a password or other approved method. Users of VoIP telephones shall not be able to view administrative settings or settings such as IP or MAC addresses.

(Note: Such information could enable a user to gain information about the network or potentially spoof a device and gain unauthorized access.)

g. Unnecessary Telephone Services. Services other than those necessary to process VoIP telephone conversations and related VoIP functions (e.g., streaming audio, call setup, call breakdown) shall be disabled if not needed. Web services or the ability to browse the web with a VoIP phone shall be disabled.

h. Speech Processing Software and Telephone Data Ports. Speech processing software/ application shall not be enabled for any computerized applications. To ensure data and voice segregation, the data port on the VoIP telephone device shall be disabled.

i. Firmware Upgrades and Configuration File Integrity. A management process must be implemented to ensure that any installation or upgrade of program or data

[3] Some VoIP vendors have designed hold and mute features that "flip a bit" to indicate the activation of the feature, but permit the actual transport of audio along the network connection.

files originate from the vendor. These upgrades must be tested to prevent downtime (or service disruption) that may be caused by compatibility issues or undesired changes to the existing security profile. Data network security is required to ensure that upgrades do not originate from unintended sources outside of the secure area.

6. Voice/Data Network

a. Server Security. The hardening of critical network components (e.g., call processor/controllers, media/signaling gateways) is crucial to a VoIP system's security because of the functionality they provide. Server systems have a relatively large level of exposure due to the functions and services that they typically provide. There are additional security concerns associated with VoIP functionality as vulnerabilities that are inherent in the server operating systems are more readily exposed and will be introduced into the telephony system and must be addressed.

1) Operating System (OS) hardening shall be performed in a manner consistent with approved hardening guidelines such as National Security Agency (NSA) Security Configuration Guides or Defense Information Systems Agency (DISA) Security Technical Implementation Guides. DISA has developed several guides that address operating system, network, and device hardening techniques. This level of hardening shall be performed on all management workstations or devices with similar functionality.

2) Patch Management must be implemented to ensure that the latest available security patches are applied. The patches must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

3) Ethernet Port Security shall be configured on switch devices to reduce the risk of an attacker collecting data (using a network-based H.323/SIP data sniffer) and replacing a legitimate telephony device with a rogue device such as a laptop or palmtop.

b. Network Perimeter Security, whether VoIP or otherwise, plays a key role in the overall security of the network. A combination of both a traditional firewall and a VoIP Application-Layer Firewall shall be applied to perimeters of the secure area and between VLANs.

c. Physical Security

1) PPS must be established to provide positive physical protection for the VoIP system and all of its components and interfaces. This includes all telephones, cables, lines, intermediate patch panels, servers, routers, and switches necessary for the functioning of the system. The PPS must be controlled by the organization having oversight of the secure area.

2) Wiring isolation refers to when only equipment or wiring that is not intended to be isolated by the VoIP system may be located outside of the PPS. However, to ensure data and voice segregation, the data port on all VoIP telephone devices shall be disabled. Additionally, users of all VoIP telephones shall not be able to view administrative settings or settings such as IP or MAC addresses.

3) Program media protection, such as tapes or disks, must be provided physical protection to prevent unauthorized alterations.

4) Program master copy must be up-to-date master and maintained for confirmation and/or reloading of the operating program. This master copy must be verifiable as having been protected against unauthorized alteration. The current program master copy must be maintained in a physically protected storage container, separate from all other program media.

7. **IP PBX Security**. The use of IP, Ethernet, or other LAN connections can provide new methods for performing administration and maintenance of IP PBX's. While such use may result in lower administrative overhead costs, such use may also introduce vulnerabilities not found in traditional telephony implementations. With such use, the IP PBX is potentially susceptible to IP-based network attacks that could permit unauthorized access. To prevent unauthorized access to the IP Enabled PBX's programming, settings, and configurations, the following requirements must be met.

a. Auditing. The auditing function must be configured to monitor successful and failed access attempts to the device, all configuration settings changes (or attempted changes), and any other management control functions. These audit logs shall be enabled by default and their contents reviewed regularly, in accordance with local security policies.

b. Access Control.

1) ACLs shall be configured on the IP PBX to prevent administrative actions being performed from unauthorized devices. The system shall be configured such that administrative functions must be performed from an administrative workstation using a dedicated out-of-band management network. User authentication shall also be implemented (e.g., Authentication, Authorization, and Accounting Server). These connections must be protected with Reference e. approved encryption protocols.

2) Privileged account protection, if an out-of-band management network is not possible, an equivalent level of protection shall be provided for administrative usernames and passwords to prevent unauthorized disclosure of privileged accounts. These administrative usernames and passwords shall be protected IAW

NIST FIPS 140-2 encryption, Reference e., via a secure protocol such as SSH or SSL.

3) Usernames and passwords, IAW organizational security requirements, shall be required prior to providing access to the administrative functions of the IP PBX. In addition to required authentication, strong passwords shall be used. Such passwords must consist of a minimum combination of three of the four character types (i.e., uppercase, lowercase, numbers, and special characters) and a minimum length of eight characters.

ANNEX G

VoIP Trunk Security Requirements

1. This annex specifies security requirements for deploying a VoIP Trunk voice/data solution. This annex does not provide specific implementations needed to satisfy each requirement. This type of VoIP implementation consists of a TDM CTS using VoIP for an external trunk. These requirements apply if the VoIP Trunk cards of the PBX convert IP to TDM. If the trunk cards provide any other support for IP, the system must meet the requirements of the applicable annex in this document.

2. The requirements of this document do not address the C&A requirements that many organizations require. Consult with your network accreditation authority for guidance.

3. Voice Instrument Security may be accomplished by using one of the following two methods.

a. Method #1: Use approved phones or interface devices (Reference j.).
b. Method #2: Use guidelines for securing telephone systems (Reference h.).

4. Private Branch Exchange (PBX) Security must comply with the installation and maintenance requirements detailed in Reference h.