VOICE VIDEO OVER INTERNET PROTOCOL (VVoIP) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 3, Release 11

28 April 2017

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Voice Video over IP (VVoIP) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to voice and video systems. The VVoIP STIG works in conjunction with the Voice Video Services Policy, Network Infrastructure, supporting application, and appropriate operating system (OS) STIGs.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be … configured … consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil.

This documentation is not published for general access to protect the vendors' proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 VVoIP Overview

The primary focus of the VVoIP STIG is to ensure the availability, confidentiality, and integrity of DoD's IP-based Assured Service (AS) telephone communications and the converged networks supporting the communications service. This is done by providing a defense-in-depth strategy for these communications systems via a multi-layered approach for both Controlled Unclassified Information (CUI) and classified communications services. VVoIP implementations replace or augment traditional circuit-switched telephone systems.

A secondary focus of the Voice Video Services Policy STIG is video communications associated with VoIP telephone systems augmenting VoIP capabilities. A video session associated with a voice session on a VoIP telephone system is established and transported using the same protocols as the voice session. Session establishment is the core of the VVoIP system and controlled by the voice video session manager, such as a Local Session Controller (LSC). Security measures applicable to voice sessions are equally applicable to associated video sessions.

2.2 Command and Control (C2)

Telecommunication switches and systems leased, procured, or operated by any component of the DoD must support special Command and Control (C2) user capabilities. These systems provide Multilevel Precedence and Preemption (MLPP) that prioritize calls based on user levels. In the transition from Time Domain Multiplexing (TDM) systems to IP-based systems, MLPP and other Assured Services (AS) functions have been incorporated into DoD VVoIP networks.

- **Special-C2 User**: A special class of user who has access to DoD Unified Capabilities (UC) networks for essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders.
- **C2 User**: A class of user who has a requirement for C2 communications but does not meet the criteria for the class of Special-C2 user. C2 users include any person (regardless of the position in the chain of command) who issues or receives guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime.
- **Non-C2 User**: DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirements to ever originate or receive C2 communications under the definitions for C2 and Special-C2 Users. During a crisis or contingency, they may be denied access to the DSN or DRSN. These users are provided access to the DSN for the economic benefits to the Department of Defense.

2.3 Voice Video Assessment Guidance

To assess Voice Video components and systems, the following resources apply.

2.3.1 Video Services Policy

Policy and architectural guidance for implementing systems on the DoDIN is contained in two documents. The Voice Video Services Policy STIG provides the policy and architectural guidance for VoIP systems (also referred to as UC systems or implementations) used to support the DoD. The Video Services Policy STIG contains the policy and architectural guidance for Video Conference (VC) systems in use within DoD. Some overlap exists between the documents. When VoIP session managers are fielded, the Voice Video Services Policy STIG is applicable. When VC session managers are fielded, the Video Services Policy STIG is applicable.

2.3.2 Network Device Management (NDM)

Network devices usually contain a management component to handle administration of the network device itself. NDM security practices and procedures applicable to the management of all DoD network devices are contained in the NDM SRG. The NDM guidance works with the technical requirements in other SRGs. Vendors of session management products will use the NDM SRG for the management plane and the Voice Video Session Management SRG for the control and data planes of the device.

2.3.3 Voice Video Session Management

Session managers for voice and video systems will rely on the Voice Video Session Management SRG for technical guidance. The protocol suites used for voice and video session management products include Session Initiation Protocol (SIP), H.323, and proprietary protocols such as Skinny Client Control Protocol (SCCP) and Unified Networks IP Stimulus (UNIStim). For DoD, SIP, H.323, SCCP, and UNIStim are associated with VoIP and VC sessions. Currently, most session managers handle multiple protocols.

2.3.4 Voice Video Border Elements

Voice video border elements are products providing services at the border and within enclaves in support of the voice video system. These products often work in parallel with the data firewalls, providing routing and conversion of voice video transmissions. Border elements rely on the Back-to-Back User Agent (B2BUA) function of the enterprise network Session Border Controller (SBC). SBCs perform inspection and proxy functions for specific ports and protocols used by voice and video signaling and media. Gateways enable communication between voice video networks and other networks, such as PSTN or ISDN networks. Border elements will use the guidance in the Application Layer Gateway (ALG) SRG for the technical implementation of these devices and devices with this functionality.

2.3.5 Voice Video Endpoints

Voice video endpoints include VoIP hardware phones, VC desktop terminals, UC and VC soft clients, and VC Coders/Decoders (CODECs) used in conference rooms with multiple cameras, microphones, and displays. The guidance for these devices is contained in the Voice Video Endpoint SRG.

2.4 On-Hook Audio Security

All unclassified voice video endpoints deployed within a Sensitive Compartmented Information Facility (SCIF) must be National Telecommunications Security Working Group (NTSWG) approved devices in accordance with the Committee on National Security Systems Instruction (CNSSI) 5000 and 5001. Compliance with federal standards helps establish a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements. In most common configurations, voice video endpoints can transmit conversations in secure areas over unclassified networks. Voice video endpoint microphones, speakers, and supporting electronics may pick up nearby conversation audio and conduct it over the network connection, even when the endpoint is on-hook, powered or not. The Technical Surveillance Counter-Measures (TSCM) program protects sensitive government information, to include classified information, through the establishment of on-hook audio security standards. Voice video endpoints certified by NTSWG are modified to prevent this behavior, or limit it to within acceptable levels.

3. VVOIP SYSTEM ARCHITECTURE

An understanding of the VVoIP system cybersecurity architecture, as used in the DoD, is required if one is to understand the security guidance provided by this STIG. The purpose of this section is to provide that understanding as well as an understanding of a number of terms used in this STIG that relate to a wide variety of DoD enclaves. The VVoIP cybersecurity architecture will be presented through a number of drawings and explanations. These drawings do not define specific solutions, but they do graphically demonstrate applications of various requirements.

3.1 Enclave Network Types

This STIG refers to LANs, Enclaves, WANs, and intranets. These terms can mean different things to different readers. For the purpose of this document, the following definitions apply:

- **Enclave; Local Enclave**: For the purpose of this document, these are synonymous and refer to a LAN operated by a single organization having a single security policy that is typically within the fence line of a physical BCPS.
- **LAN**: The LAN is the Ethernet and IP network located supporting a physical BCPS that is operated by a single organization having a single security policy. Such a LAN can be small, supporting one building or small site with a few buildings, or it can support a large site with many building segments. The LAN comprises the local enclave. Such a local enclave might also support one or more remote site local enclaves (LAN) not collocated within the fence line of the main BCPS but connected to it via direct dedicated TDM (T1 or DS3) or Optical (Ethernet or OCx) connection. A remote LAN, such as this, is operated as part of main BCPS enclave, or it is considered a subtended enclave.
- **Sub-Enclave**: Security zones created within the local enclave using Virtual LANs (VLANs) and protected at Layer 3 using router Access Control Lists (ACLs). These VLAN security zones provide trusted connectivity for the systems they support and are required for the VVoIP system as well as dedicated VC systems. These are separate from the data VLANs, which are considered untrusted with respect to the VVoIP and VC VLANs.
- **Subtended Enclave; Tenant Enclave**: A local enclave collocated within the fence line or adjoins a larger BCPS that is operated by a different organization with a different security policy than that of the larger BCPS. Such is the case of a tenant of the larger or host BCPS. Typically, this means that a component of one Combatant Command, Service, Agency (CC/S/A) resides on a BCPS owned and operated by another CC/S/A. An example of such a tenant is an Army post residing on a Navy base. If the tenant operates their own local enclave and reaches the WAN through the WAN boundary of the local enclave operated by the larger BCPS, the tenant enclave is subtended to the BCPS enclave. DoD policy requires the tenant enclave to implement enclave-to-enclave boundary protection at its connection to the BCPS enclave. On the other hand, the tenant enclave may only utilize the cable plant of the host BCPS to reach the WAN POP. In this case, the tenant enclave must provide their own primary enclave-to-WAN boundary protection. As such, the tenant enclave is not subtended. A third scenario, not needing any boundary protection, is when the tenant directly uses the local enclave services of the host BCPS.

- **Intranet**: An extended enclave, operated by a single organization such as a CC/S/A, consisting of the interconnection of multiple local enclaves. The interconnections might be via direct connection, dedicated circuit, or VPN tunnels across a WAN. An intranet might be regional, or it might be worldwide.
- **Regional Enclave**: A type of intranet implemented by a CC/S/A to centralize computing services and potentially enclave boundary protection.
- **Wide Area Network (WAN)**: Generally refers to an inter-enclave transport network such as a DISN service (NIPRNet, SIPRNet, etc.) but might also refer to a commercial provider's network that peers with other commercial provider networks to form the Internet.

3.2 Basic Local Data Enclave and Traditional Voice Architecture

Figure 3-1 notionally depicts a basic data enclave, or LAN, connected to the NIPRNet through a WAN boundary that also supports a local De-Militarized Zone (DMZ).

- The LAN is a notional representation of the required or typically used hardware.
- All required boundary hardware is shown.
- The NIPRNet cloud depicts an Internet Access Point (IAP) as it is today (lower) and a future IAP with a DMZ (upper).
- The Public Internet cloud is a notional representation of the collection of networks that it is.
- Included are service provider clouds for Internet Service Providers (ISPs) and those that also are Internet Telephony Service Providers (ITSPs).
- Also included are the peering points and VoIP session border controllers (SBCs) that are used to interconnect the service provider networks to create the Internet.

The voice communications system, in this case, is a separate circuit-switched network centered on a Multi-Function Switch (MFS), End Office (EO), Small End Office (SMEO), and Private Branch Exchange (PBX). Optional direct phone service from the PSTN is also depicted.

Figure 3-1 is the basis for the similar drawings that follow, each of which shows an added feature of the network. The basic data LAN does not change. Figure 3-2 shows the same information as Figure 3-1, but the focus is on the VLANs and subnets required within data enclave architecture itself. The following items should be noted:

- The DMZ for externally accessible servers and VPN access.
- The "server farm" for the internal servers.
- The server management LAN/VLAN dedicated to server management.
- The Network management VLAN and management server/workstation subnet dedicated to managing and monitoring the network elements that comprise the LAN infrastructure.
- The dedicated printer VLAN.

Figure 3-2 will be the basis for additional drawings. However, some of the detail in the clouds on the right will be removed to make room for the voice architecture on the left.

Figure 3-1: Basic Data Enclave with Traditional Voice Communications

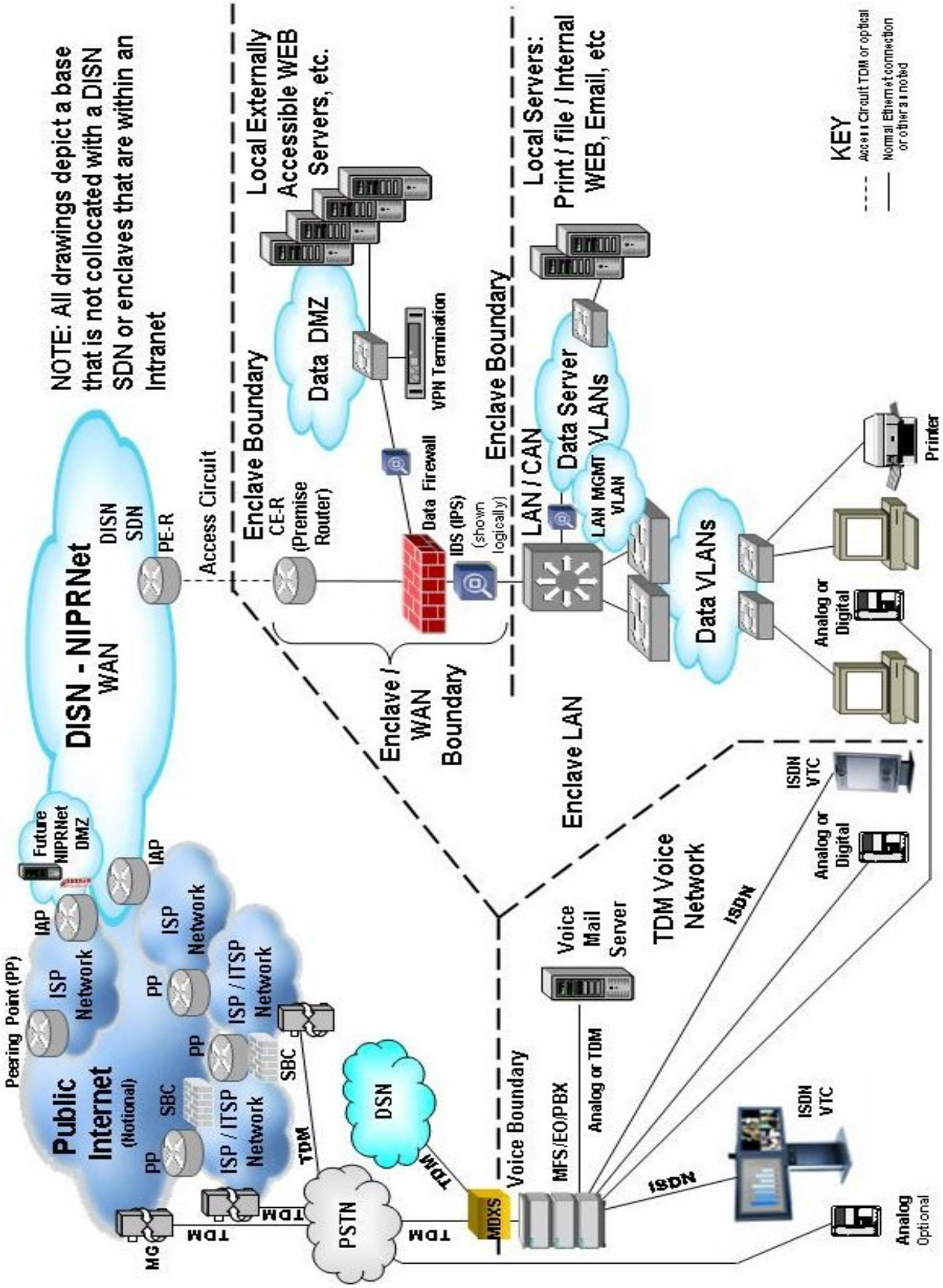
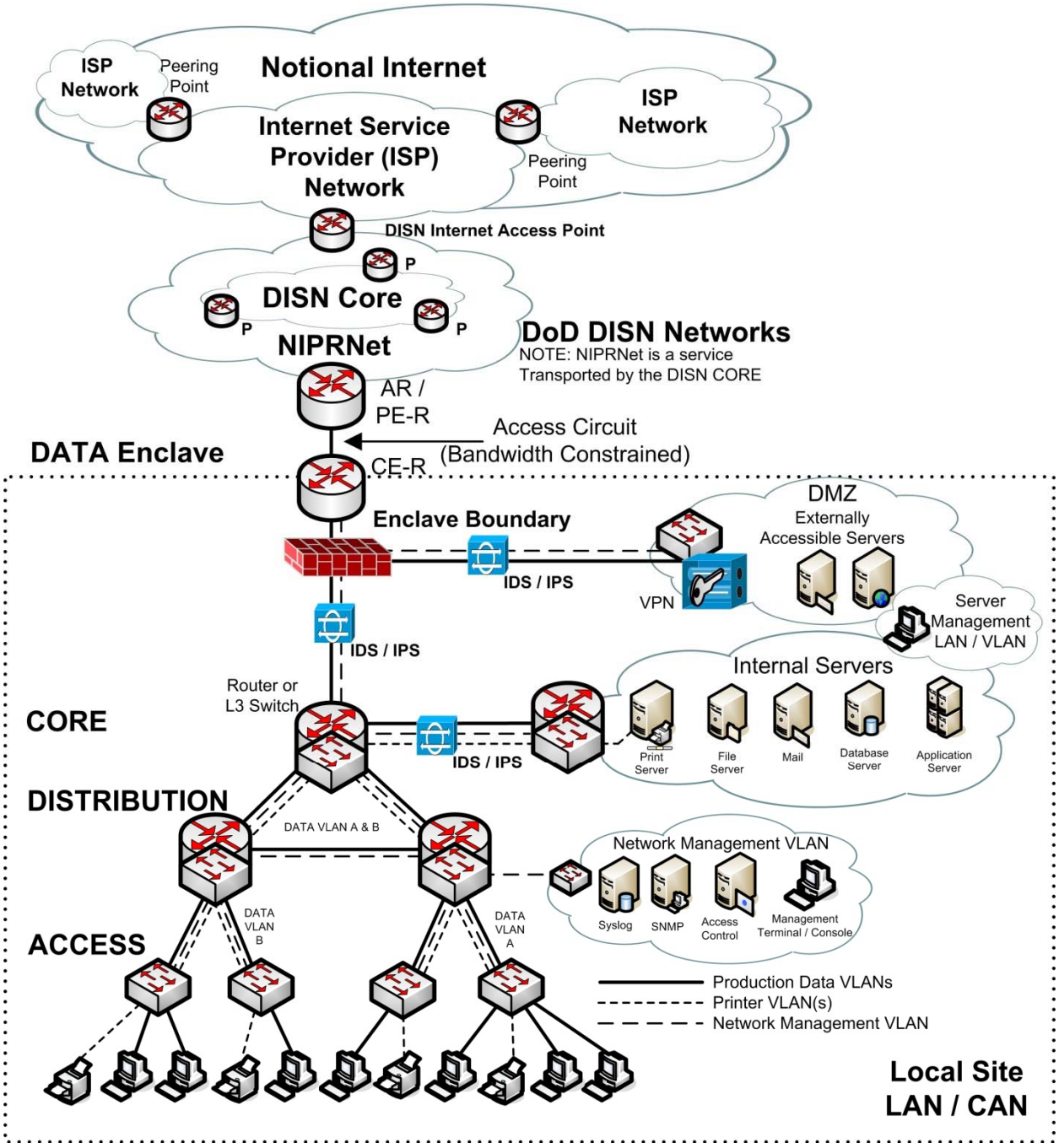


Figure 3-2: Basic Data Enclave Showing Subnets and VLANs



3.3 Adding VoIP Telephones to the Local Enclave LAN

Multiple LANs may connect together to form a Campus Area Network (CAN). An enterprise network may consist of one LAN or CAN, or it may consist of LANs or CANs that are in different geographic locations connected via WAN links. The initial discussion and drawings that follow address adding a VoIP system to a single local LAN/CAN.

When adding a VoIP system with its call controllers, telephone endpoints, and other related devices to a LAN, the VoIP system inherits all of the vulnerabilities that plague our networks and is threatened by them as well as additional vulnerabilities. To protect the VoIP system devices and the communications they enable, we create a closed virtual environment for the system to operate in while sharing the LAN infrastructure with the data environment. This is done by creating a closed set of VLANs and associated subnets in a different address space from the data network. Traffic is controlled within the VLANs with router ACLs. Traffic is blocked or controlled between the data and VoIP VLANs with router or firewall ACLs. In general, the data environment or its users should not be able to access the VoIP environment unless specifically controlled. Additional information can be found in the vulnerability discussions in the requirements surrounding IP addressing, VLANs, and ACLs.

Figure 3-3: Conceptual Virtual VoIP Environment Sharing the LAN

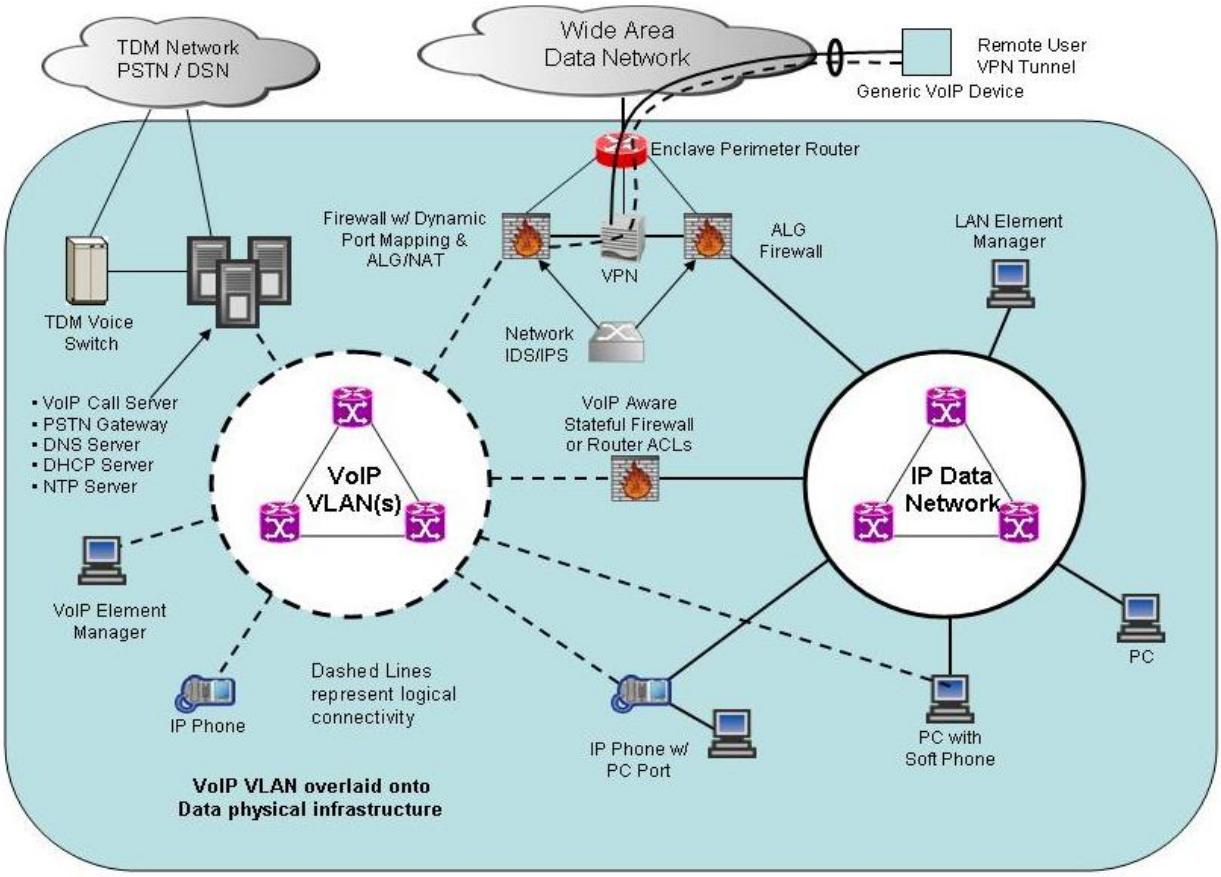


Figure 3-3 provides a graphic representation in its simplest form of the virtual VoIP environment sharing the physical LAN with the data environment it was originally intended to serve. Note the traffic control between the VoIP and data environments represented by the firewall in the middle. Additionally shown is a VoIP-aware firewall at the enclave boundary I, the event the VoIP system access the WAN in that manner. A remote user and generic device is shown connected in a remote access situation. The generic device can be a UC soft client or a hardware-based VoIP phone. The VPN is required to extend the local enclave to the remote device. While remotely

connected VoIP endpoints can reach back through the WAN to their home call controller and register, this leaves the endpoint and its communications unprotected.

Figure 3-4 shows how the virtual environment (shown in Figure 3-3) is overlaid upon the basic data LAN (shown in Figure 3-2). The information from Figure 3-2 has been simplified to focus attention on the VVoIP system. Topics that are not addressed in Figure 3-4 are as follows:

- The remote user VPN tunnel, except to show the VPN concentrator and a note at the firewall.
- UC soft clients (with or without video capabilities) or VC soft clients.
- Unified messaging and/or unified communications.
- Videophones and VC endpoints that integrate with the VoIP system.
- A separate VC system, not integrated with the VoIP system.

There are several things to note in the drawing:

- Addition of the VoIP core equipment and VoIP VLANs.
- Interfaces and ACLs for the VoIP core equipment.
- The ACLs that maintain the closed nature of the VoIP VLANs.
- The phones with the PC jack, and connected PC maintains V/D VLAN separation.
- The LAN/CAN core router/switch and the VoIP core can potentially be the same device.

3.4 VVoIP System and LAN Reliability and COOP

Figure 3-5 is based upon an Air Force Combat Information Transport System (CITS) Program generated example of a possible LAN/CAN involving multiple buildings and types of users (special C2, C2 and non-C2).

Figure 3-5 serves two purposes, the primary of which is to demonstrate how the backup power requirements are applied to a LAN in support of special-C2, C2, and non-C2 users. Per policy, all VVoIP and LAN infrastructure supporting special-C2 users must be supported with 8 hours of backup power. The value changes to 2 hours for C2 users. While policy states that C2R, non-C2, and admin users do not require any backup power support (as noted by “no req” in the drawing), it is best practice to provide some amount so that emergency fire, medical, and police/security calls are supported for some period of time following a failure of primary power anywhere in the LAN/CAN.

The secondary purpose of Figure 3-5 is that it demonstrates the redundancy in the LAN equipment and its uplinks. All network elements (NE) that support in excess of 96 users is required to be internally or externally redundant in support of the uptime required for the level of user(s) the NE supports. Additionally, all connections above the LAN access switch layer must be redundant. These uplinks are also supposed to follow geographically diverse paths. This redundancy and diversity provide a backup path in the event of equipment or cable failure. The geographically diverse paths provide some assurance that both links will not be severed in the event of a cable failure or cut somewhere along the path.

Figure 3-4: Basic Data Enclave VLAN architecture with VoIP

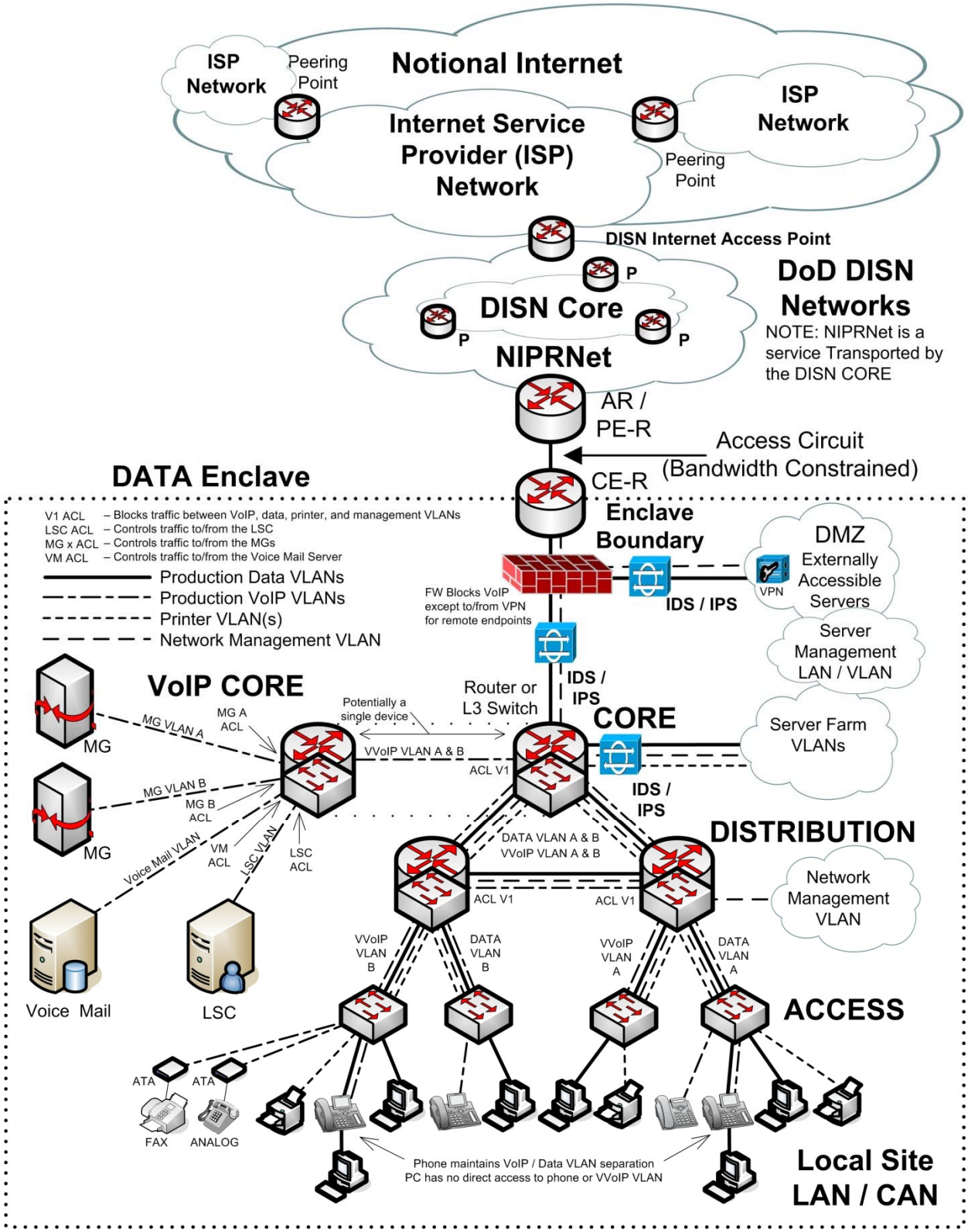
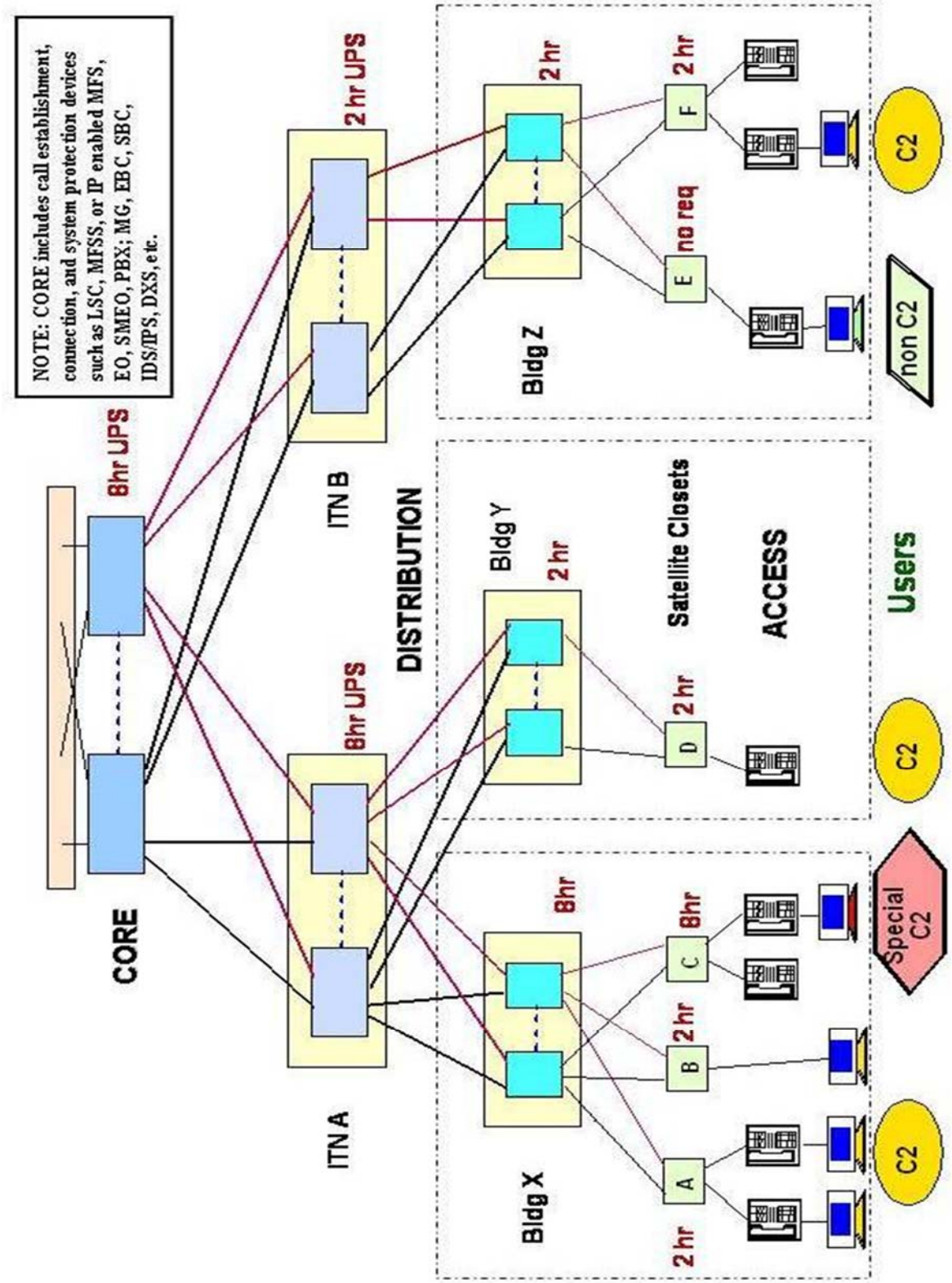


Figure 3-5: VVoIP LAN Redundancy and Backup Power Requirements



3.5 Connecting the Basic Local VoIP System to External Systems

A basic local VVoIP system is wholly contained within a local enclave or LAN/CAN. Calls into and out of the local enclave do not traverse the enclave boundary with the WAN but utilize MGs that interconnect the VoIP portion of the LAN with a traditional circuit-switched telecom network (such as the PSTN or DSN) or switch (such as a local MFS, EO, SMEO, or PBX). When video communications is associated with the VoIP system and endpoints, the associated traffic remains within the LAN. The use of MGs and a TDM network between VoIP systems provides for interoperability between different vendors VoIP products. This also mitigates the vulnerability that VVoIP presents to the enclave when traversing a traditional firewall. The basic local enclave VVoIP cybersecurity architecture primarily consists of VLANs and ACLs.

Figure 3-6 provides a graphic representation of the addition of a VoIP phone system to the LAN/CAN where the VoIP system is subtended to the site's local MFS, EO, SMEO, or PBX via a media gateway. The circuit switch provides the connections outside of the local enterprise LAN.

NOTE: The addition of the VoIP VLANs, which is consistent with current VoIP guidance. With this scenario, the VoIP system may be from a different vendor than the circuit switch.

Figure 3-7 shows the same VoIP system, but this time the site's local MFS, EO, SMEO, or PBX is IP enabled. This means the circuit switch vendor has added an LSC and MG to support VoIP line-side endpoints.

Figure 3-8 shows the same VoIP system, but this time it is directly connected to external circuit-switched TDM networks (DSN and PSTN) via MGs.

In all drawings, note the Data eXfiltration Sensor (DXS) placement that is intended to detect and inhibit or prevent the exfiltration of data from the network using VoIP media protocols as a cover. Additionally, in Figures 3-5 and 3-6, the placement of a Modem Data eXfiltration Sensor (MDXS) is shown. This device detects and may block unauthorized modem traffic using the circuit-switched network.

3.6 DISN IP Voice Services Network/System

The IPVS Network/System is an emerging capability on NIPRNet. This capability supports C2 Assured Service (AS) voice (and associated video) communications for C2 and special-C2 users. The DISN IPVS Network/System is the technological refresh path for the traditional circuit-switched DSN. It is part of the future of the DISN where everything over IP is the goal. The development of, and migration to, the IPVS network or system is also being forced by the technological trends in the telecommunications industry that will ultimately replace circuit-switched telecommunications with VoIP.

The DISN IPVS network consists of interconnected VVoIP systems/enclaves within the various LANs/CANs operated by the various DoD services and agencies. The overall system uses a hierarchical signaling (call control) model, while the media (communications) is peer-to-peer and end-to-end. The signaling used is Assured Service (AS) – Session Initiation Protocol (AS-SIP).

Figure 3-6: Basic VVoIP Enclave/System Subtended to a MFS, EO, SMEO, or PBX

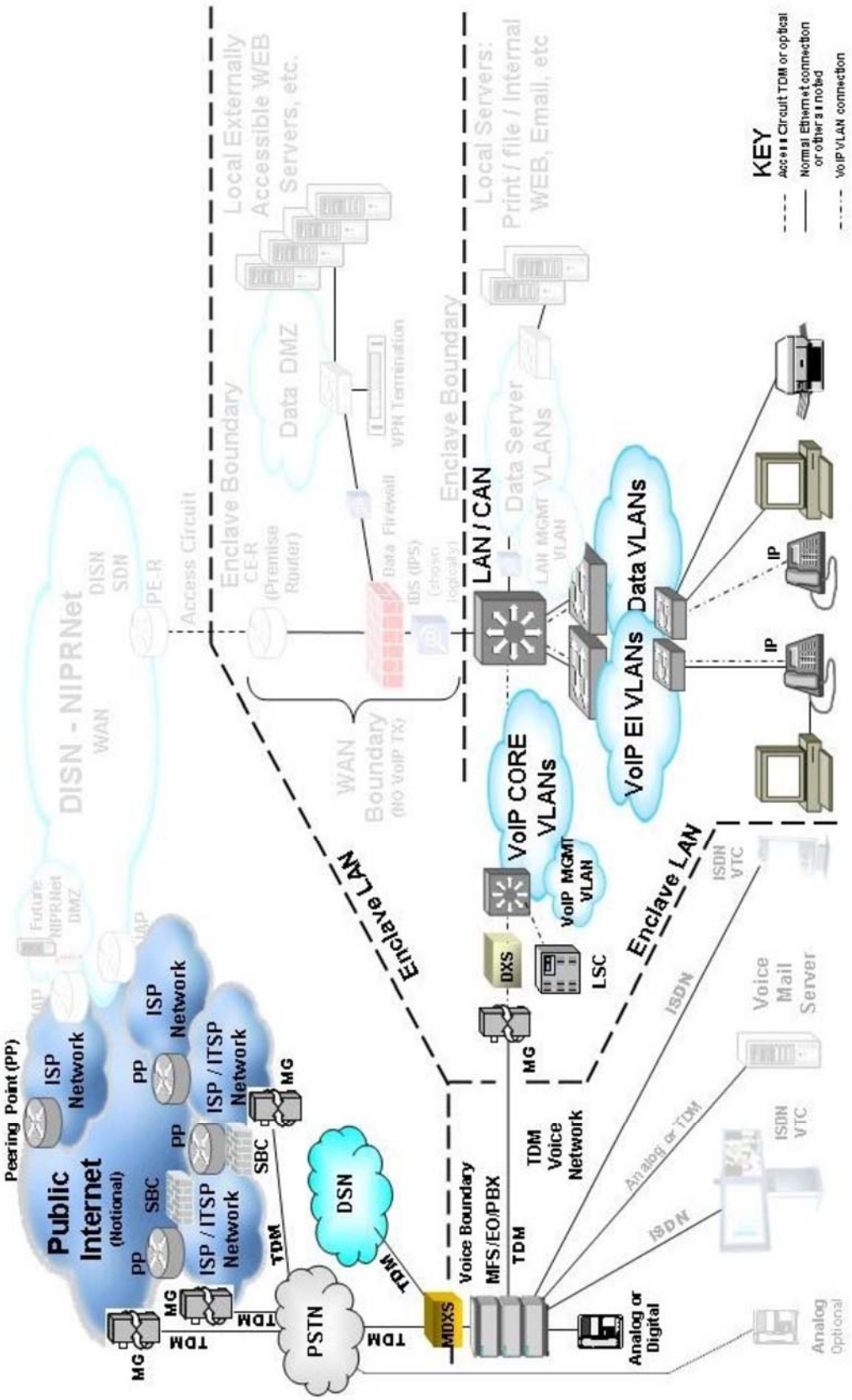


Figure 3-7: Basic VVoIP Enclave Controlled by an IP Enabled MFS, EO, SMEO, or PBX

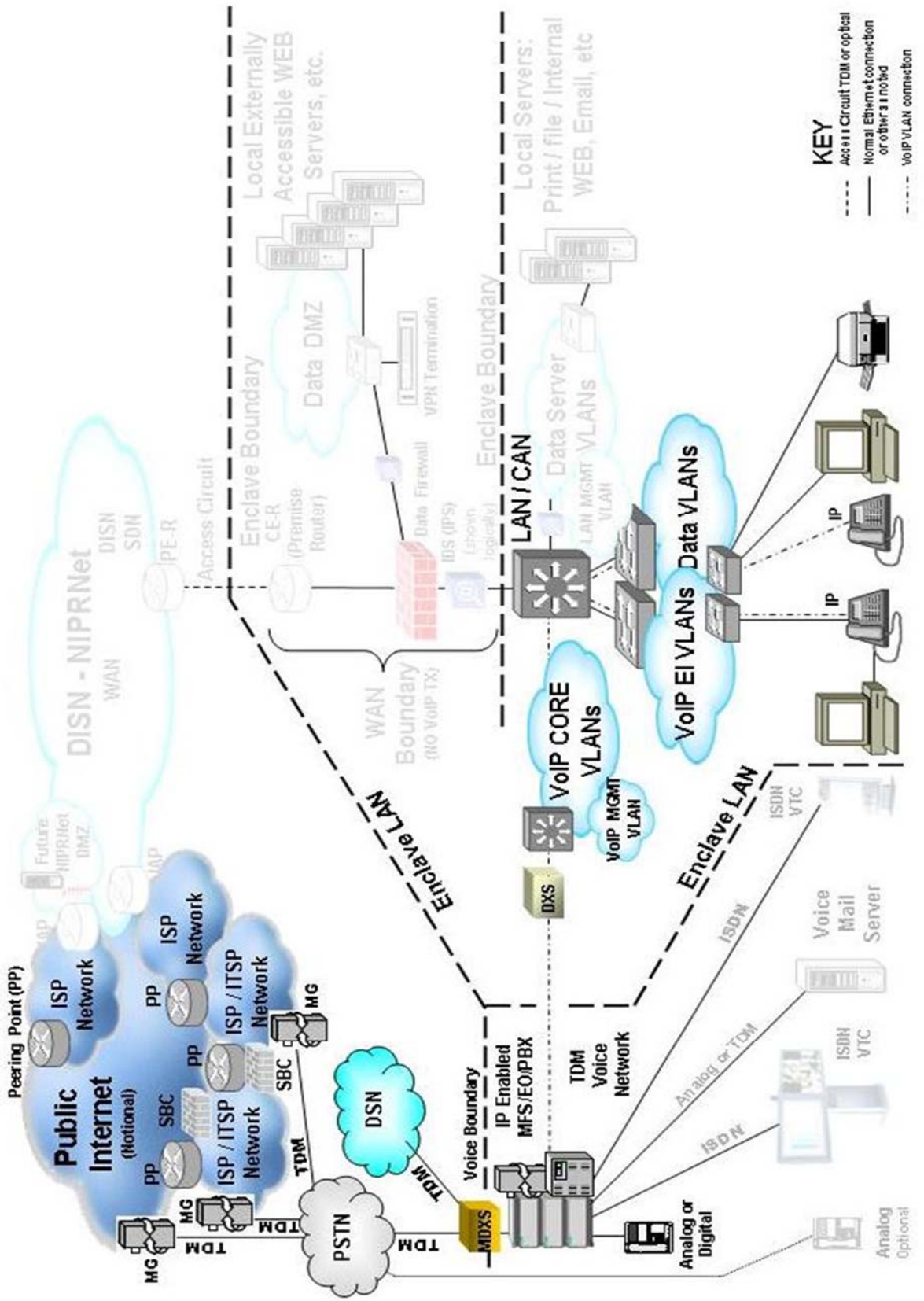
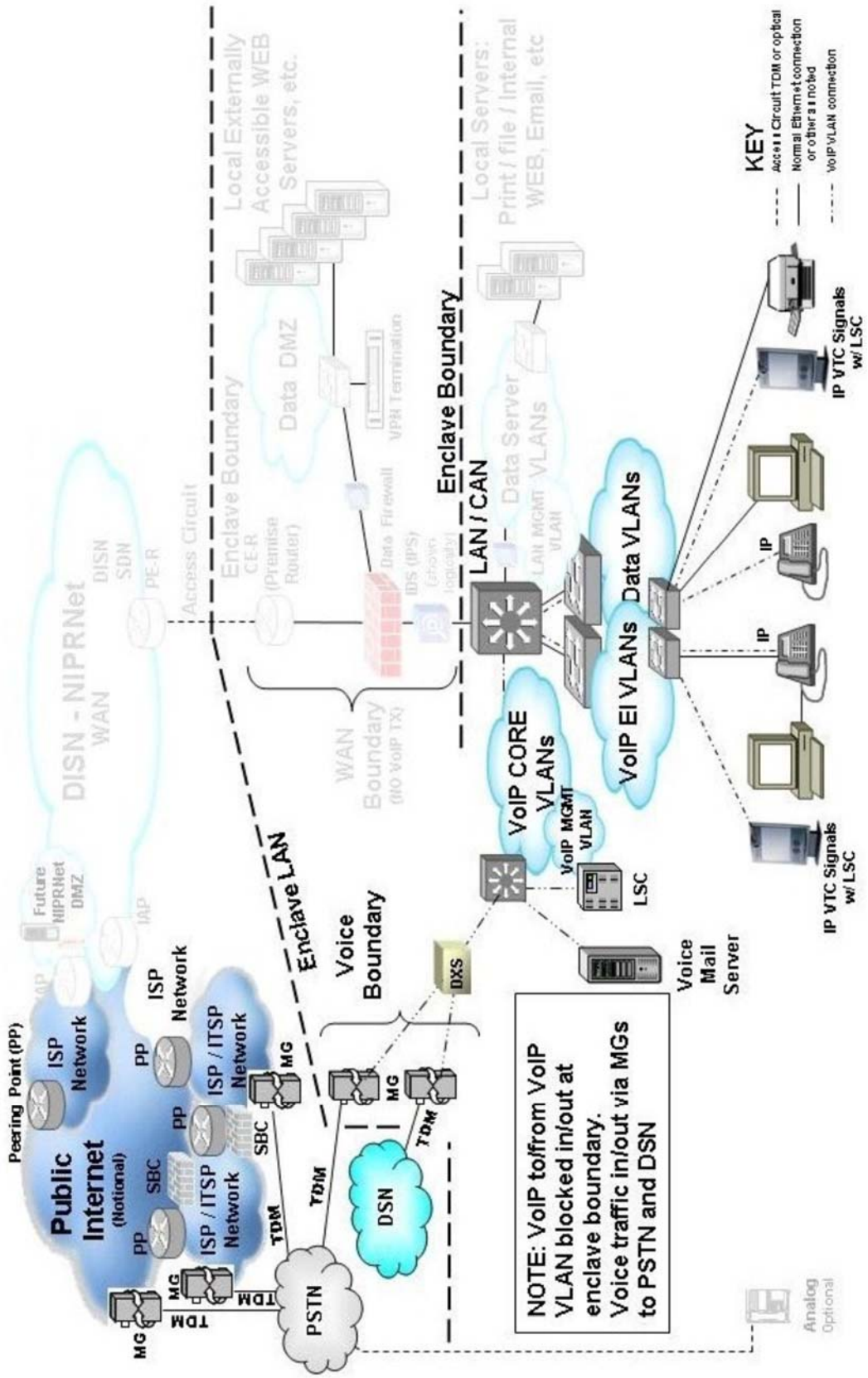


Figure 3-8: Basic VVoIP (Only – No PBX) Enclave



AS-SIP is a DoD extension or specific implementation of the SIP protocol that enables the network/system to provide assured service capabilities, such as pre-emption and priority for command and control (C2) communications. This is similar to the MLPP capabilities of the circuit-switched, TDM-based DSN. AS-SIP is transported in a hop-by-hop manner and protected by Transport Layer Security (TLS) encryption. All signaling appliances except the endpoints are SIP Back-to-Back User Agents (B2BUAs). The media or bearer streams flow directly between communicating endpoints within their respective enclaves and across the WAN. The communications media is also encrypted. The protocol used is Secure Real-time Transport Protocol (SRTP) and Secure Real-time Transport Control Protocol (SRTCP). DISA has worked with the major circuit switch and VoIP system vendors serving the DoD to develop a standardized basis and specification for a DoD implementation of AS-SIP-TLS and SRTP/SRTCP that will foster interoperability among the various vendors' VoIP systems.

LSCs manage signaling within their own enclaves. Signaling between enclaves is managed by a series of Multi-Function Soft Switches (MFSS) and/or Soft Switches (SS) located within their own VoIP system enclaves. LSCs communicate/signal with MFSSs (one primary and one backup) to establish calls across the WAN. MFSSs communicate/signal with other MFSSs and their assigned LSCs to support call establishment. The MFSS/SSs are needed to control/manage the number of active sessions into and out of the enclaves assigned to it so that the AS capability of the network will function properly. The MFSS/SSs perform the LSC function for the VoIP endpoints within their own enclave.

A MFSS provides the circuit-switched MFS function of the TDM-based DSN. An MFSS also provides the local connection to the TDM DSN as well as the TDM PSTN via internal MGs between its VoIP and TDM sides. If one enclave needs to process a call to another enclave, the calling LSC contacts its assigned primary MFSS, which interrogates the destination enclave to determine if there is availability in its budget to receive the call. Based upon this availability, a decision is made to route the call that is also based on the priority of the call. If necessary, the MFSS will instruct the LSC to tear down a lower priority call to receive a higher priority call. This functionality also exists at the calling enclave and is managed by the local LSC. Once the path is cleared for the higher priority call, the call is established.

Figure 3-9 provides a graphic representation of the DISN IPVS network overlaid upon the NIPRNet.

Several things should be noted in the drawing:

- The drawing uses the designation of MOB for most of the enclaves shown, while two have a designation of GRU. MOB stands for Main Operating Base, while GRU stands for Geographically Remote Unit. These are shown to demonstrate the options of how a GRU is subtended to a MOB using a direct connection or a virtual connection via a VPN tunnel.
- A GRU may or may not contain an LSC; however, it must have a backup call control capability to maintain local calling capability within the enclave and to the PSTN in the event the site is cut off from the DISN or the main LSC.

- The various PSTN clouds and DSN clouds represent homogeneous PSTN and DSN networks, respectively. While the PSTN is comprised of multiple operating companies (Local Exchange Carriers (LECs), Competitive Local Exchange Carriers (CLECs), and Inter-Exchange Carriers (IXCs)), the DSN is formed by interconnecting all DoD-owned MFS, EO, and SMEO switches with dedicated trunks. This information is too complicated to depict in this drawing. And it is not to the point.
- Local commercial phone service is required for each site/enclave, MOB or GRU, (where available). This is partially in support of the ability to make local emergency services calls but also serves as a Continuity of Operation Plan (COOP) backup to DISN services.
- Each enclave, MOB, and GRU that supports C2 operations and users must be dual-homed into the DISN cloud. This is shown with a solid primary connection and a dashed backup connection.
- Each VoIP enclave shows a fax machine and a standard analog telephone connected to the PSTN and an Analog Telephone Adapter (ATA). The connections are mutually exclusive and are shown this way to demonstrate the options for serving an analog telephone or fax.
- The MFSS sites are MOBs A, E, and G. These provide a gateway between the IPVS network/system and the traditional DSN.
- MOB site Z in the lower left corner depicts a traditional circuit-switched DSN site having no VoIP. Notice the divide between the data and voice networks. This is shown to demonstrate how such sites are connected into the DSN, PSTN, and NIPRNet.
- MOB site D in the upper right corner depicts a basic VoIP enclave that has not joined the IPVS network directly. Thus the MG connection to the DSN. No VoIP traverses the data enclave boundary.
- DISN IPVS Signaling across the NIPRNet is restricted. LSCs may only signal with their assigned MFSS and its backup. MFSSs may only signal with other MFSSs and the LSCs assigned to them. As such, no DISN IPVS calls (signaling and media) traverse the NIPRNet IAPs except for traffic to/from remotely connected devices that is protected by a properly authenticated VPN tunnel.

3.7 Adding DISN IP Voice Services to the Local VVoIP System

Figure 3-10 notionally depicts the connection of the basic VoIP phone system on the LAN/CAN to the DISN IPVS network/system.

There are several things to note in the drawing:

- The data firewall is required to block traffic through the boundary that is destined for the VVoIP system.
- VVoIP system traffic to/from the NIPRNet must go through the Edge Boundary Controller (EBC) along with the DXS and SIP IPS/ Intrusion Detection System (IDS). The EBC provides some SIP IPS/IDS capability; however, the external device minimally acts as a backup and may provide additional protections.

- The internal network IDS/IPS must be implemented to monitor traffic from both EBC and Data Firewall. This serves as a backup to ensure unauthorized data traffic is not getting through either firewall.
- A local traditional circuit-switched PSTN connection is required for COOP and emergency services calls.
- A connection to the circuit-switched DSN is optional.

Figure 3-9: Notional NIPRNet, DSN, and DISN IP Voice Services (IPVS) Network

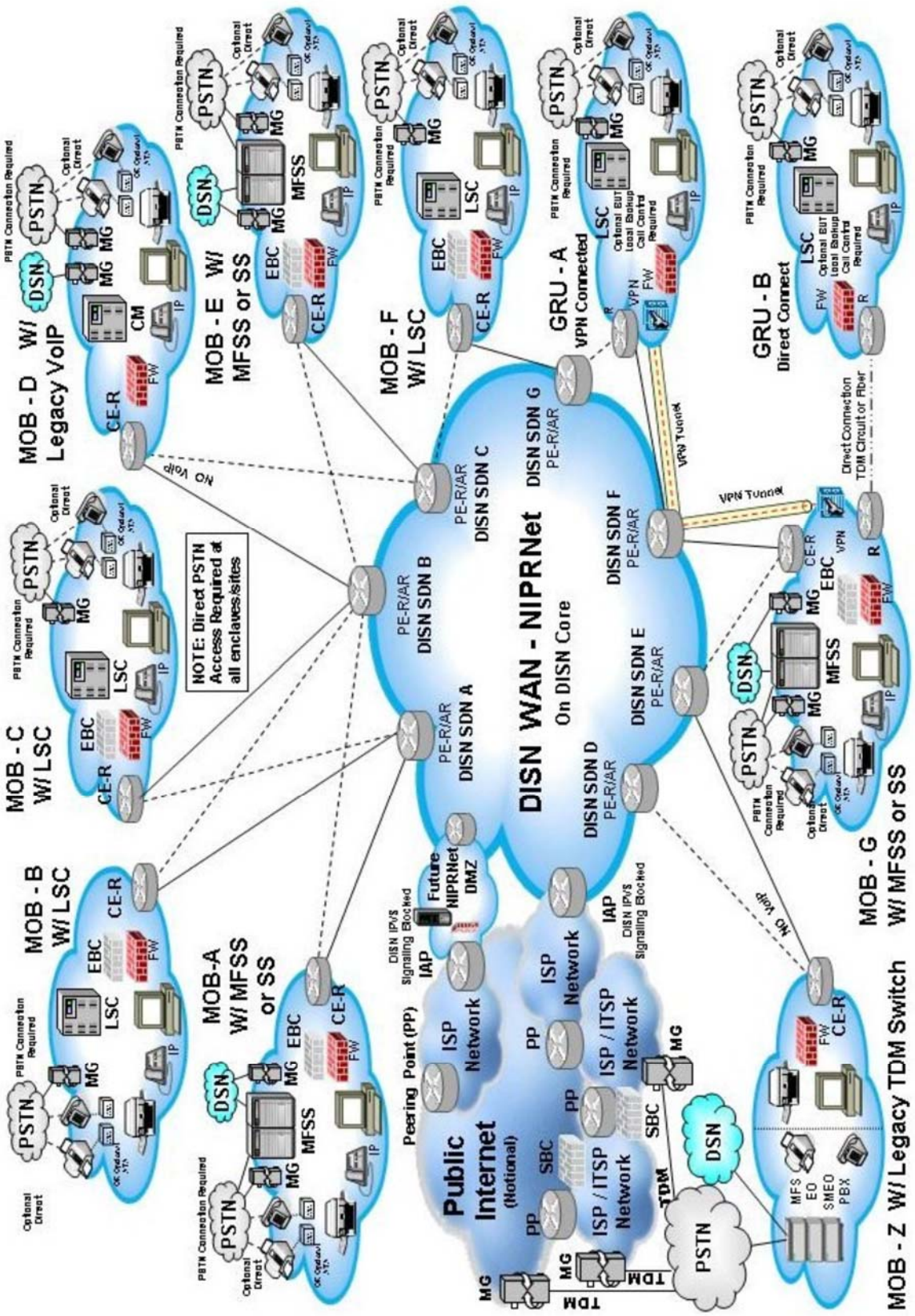
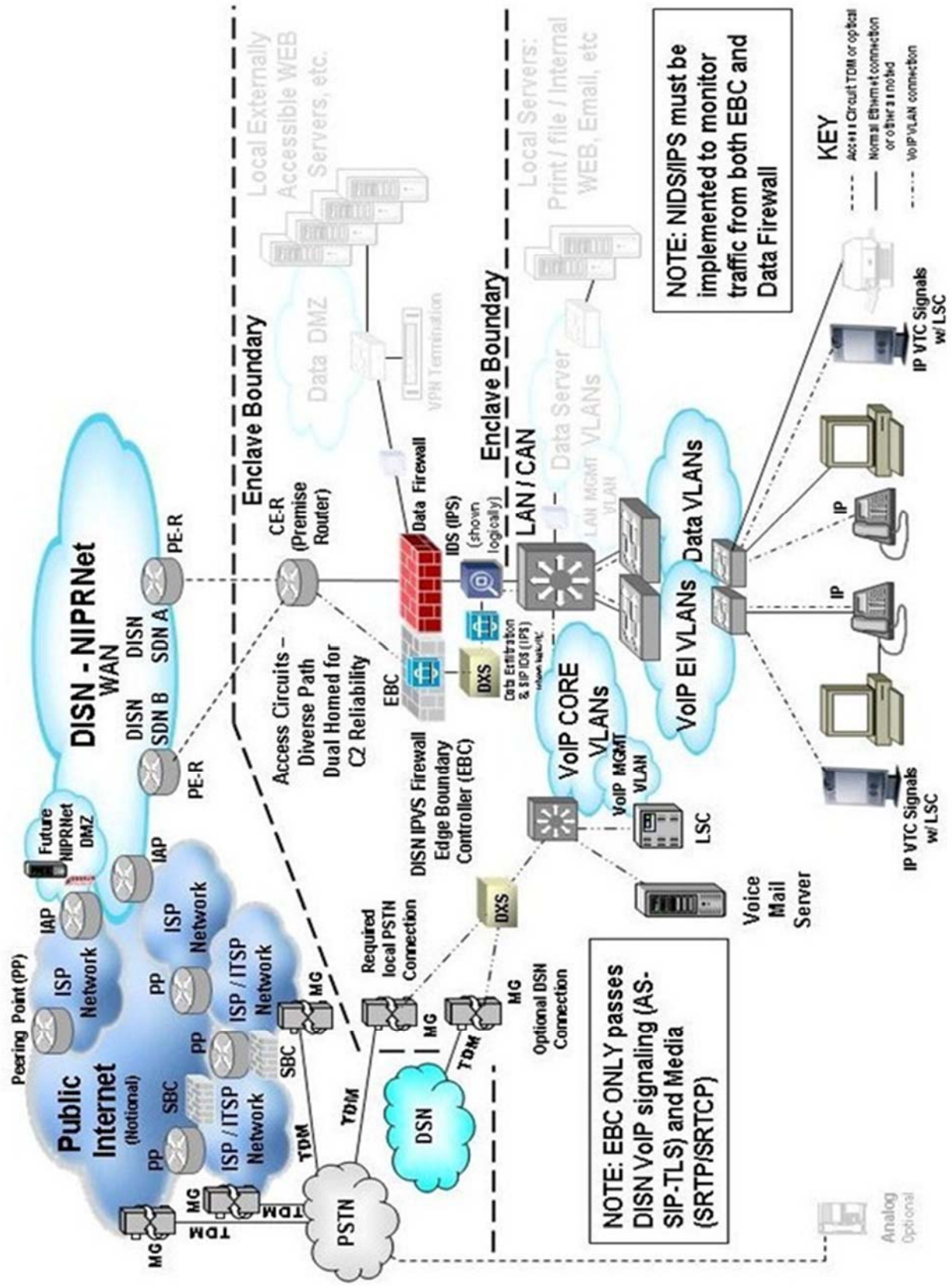


Figure 3-10: VoIP Enclave with DISN IPVS Connectivity



4. APPLICABILITY OF CNSSI 5000/5001

The Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC), provides various forms of policy and guidance for the security and operation of national security systems (NSS) that store, process, or transmit national security information (NSI).

4.1 Definitions for NSS and NSI

National Information Assurance Glossary, (CNSSI 4009) provides the following definitions for NSI, NSS, and sensitive information:

- **National Security Information**: information that has been determined, pursuant to (NSI) Executive Order 12958 (as amended) (Ref b.) or any predecessor order, to require protection against unauthorized disclosure.
- **National Security System**: any information system (including any telecommunications system) used, or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:

  I. Involves intelligence activities;
  II. Involves cryptologic activities related to national security;
  III. Involves command and control of military forces;
  IV. Involves equipment that is an integral part of a weapon or weapon system; or
  V. Subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

  (B). Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 44 U.S. Code Section 3542, Federal Information Security Management Act of 2002.)
- **Sensitive Information**: information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

4.2 Application of NSS and NSI to Systems

Based on the definitions noted above, NSI and NSS refer to classified information and systems processing, storing, or transmitting classified information, respectively. However, a designated NSS may not process, store, or transmit classified information. An example is the DSN that handles unclassified and SBU information. The DSN is an NSS because of its MLPP capabilities that are implemented for the “command and control of military forces”.

4.3 Technical Resource for Telecommunications

The National Telecommunications Security Working Group (NTSWG), formerly known as the Telecommunications Security Group (TSG) and author of TSG Standards 1 through 8, is the primary technical and policy resource in the U.S. Intelligence Community for all aspects of the Technical Surveillance Countermeasures (TSCM) program involving telephone systems located in areas where sensitive government information (classified and controlled) is discussed. TSG Standards will be replaced by and issued as CNSS Instructions (CNSSIs). Director Central Intelligence Directive (DCID), No. 6/9, requires 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 is fulfilled in accordance with the appropriate CNSSIs.

CNSSI No. 5000 supersedes NTSWG Standard 2b entitled "NTSWG Guidelines for VoIP Computer Telephony, dated April 2006". This document complements the TSG standard 2 and NTSWG Standard 2a documents that addressed "Guidelines for Computerized Telephone Systems". CNSSI No. 5001 complements the "Type-Acceptance Program" requirements documents, TSG Standards 3 and 4.

4.4 VoIP Computer Telephony Guidelines

CNSSI No. 5000, entitled "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. The requirements established in this standard are necessary in order to achieve on-hook as an idle state, audio security for VoIP telephones and/or systems located in sensitive discussion areas. 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, Communications Security (COMSEC), or Operational Security (OPSEC).

4.5 VoIP Type-Acceptance Program

CNSSI No. 5001, entitled "Type-Acceptance Program for Voice over Internet Protocol (VoIP) Telephones," specifies the design, construction, connectivity criteria, acceptance procedures, manufacturer's testing requirements, and documentation for VoIP type-accepted telephones. The requirements established in this instruction are intended to ensure that compliant devices cannot pass any audio via VoIP telephones and/or systems located in sensitive discussion areas when in an idle state and not in an active call.

4.6 Scope of VoIP Guidance

The scope section of CNSSI 5001 states: "The provisions of this instruction apply to all VoIP Telephony Systems that currently reside, or will reside, 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 reference b. (Telephone Security Group (TSG) Standard 2, "TSG Guidelines for Computerized Telephone Systems," Revised September 1993.)" The scope section of CNSSI 5000 is the same except for minor wording changes, the most significant of which is the addition of the word "unclassified" in the opening sentence between "all" and "VoIP". Since CNSSI 5001 was published after CNSSI 5000, we will assume the scope of both documents applies to both classified and unclassified VoIP systems.

Furthermore, CNSSI 5000 and 5001 both mention "sensitive government information" and "sensitive discussion areas" While classified information is a form of "sensitive government information" (CNSSI) No. 4009 defines "sensitive information" specifically as unclassified information. Additionally, based on the definition of NSS, any telephone system, classified or unclassified, owned and /or operated by, or for, a DoD component, qualifies as an NSS since it can and most likely will "Involve command and control of military forces".

4.7 Government Telephones Applicability

TSG Standard 1, on the other hand, states that it applies to telephones located in government (or government contractor) sensitive discussion areas. It is concerned with on-hook audio security and does not apply to the interception of telephone conversations (COMSEC). TSG 1 states that it is only valid for telephones located in physically protected spaces (PPS) and provides the following definition: Physically Protected Space (PPS): – The space inside one physically protected perimeter. Separated spaces of equal protection may be considered to be part of the same PPS if the communications links between them are provided sufficient physical protection.

As such, the on-hook audio security requirements specified in CNSSI 5000 and 5001 seem to apply to all VoIP telephone systems, whether classified or unclassified, or whether the endpoints are located in classified or unclassified discussion areas. As noted earlier, best practice dictates the implementation of all communications systems with endpoints that are designed to meet on-hook audio security requirements, whether the environment is unclassified or classified. Doing so will limit or eliminate the ability for an endpoint to allow aural information to be improperly disclosed through a design flaw or its compromise. Unfortunately, (as of this document's publication) there are no VoIP telephones that meet the CNSS 5000 requirements.

4.8 Relationship to the VVoIP STIG

So, how does this discussion relate to the VVoIP STIG? Surely, if this STIG addressed DoD telephone systems or endpoints in general, whether traditional or IP-based, all related TSG and NTSWG Standards, as well as CNSS Instructions, would apply, because these systems and their hardware-based endpoints are the focus of these policies. These policies could spawn the inclusion of many requirements in the STIG related to on-hook or idle-state audio security. Minimally, there could/would be a single requirement to use only TSG/NTSWG/CNSSI-certified products in SCIFs and possibly other areas. Additionally, some of the requirements could also be extended to video security. Certainly, endpoints capable of video communications should meet the audio security requirements along with minimally providing a positive, incontrovertible indicator that the video camera is active along with a positive method to mute or disable it.

As technology moves us away from using discrete hardware-based communications endpoints to a single device having embedded microphones and cameras while supporting a software-based audio and video communications environment, the ability to meet the requirements of CNSSI 5000 and 5001 for the telephony applications is lost unless significant modification of the supporting platform (i.e., PC) were to occur or external devices are required. As such, this situation could lead to a policy whereby a PC supporting a voice or voice video communications application, and particularly those with embedded and cameras, are not permitted anywhere classified discussions could occur, or, particularly, in a SCIF. This is not the direction that DoD is headed since convergence everywhere is the plan.

The information in this section is provided to make the reader aware of issues that are not addressed by this document but possibly should be, and probably will be, in the future. Before this can happen, the applicability of these requirements needs to be fully clarified. Interested parties may obtain copies of the CNSSI and other related documents by contacting the CNSS secretariat at 410.854.6805 or www.cnss.gov. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of the CNSS documents.