Changes to UCR 2008, Change 1, Section 6.2, Unique Classified Requirements

SECTION	CORRECTION	EFFECTIVE DATE
6.2.2.3 and 6.2.6.10	Revised the requirements for voice quality	18-Month Rule
6.2.6.3	Expanded description of network-Level SS to include Dual Signaling Softswitch	18-month Rule
6.2.6.9	Revised description of White Pages requirement	18-month Rule
6.2.7.2	Revised references to the AS-SIP Requirements	See Change Sheet for Section 5.3.4 for Specific implementation dates
6.2.6.10	Added a new Requirement for Secure Conferencing using NSA Type 1 encryption devices	18-Month Rule

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

6.2 UNIQUE CLASSIFIED UNIFIED CAPABILITIES REQUIREMENTS

6.2.1 Purpose and Scope

The purpose of this section is to describe technical requirements that are unique to providing classified UC. Classified requirements consist of the SBU requirements with modifications as described in this section. This issue of the UCR specifies technical requirements for assured Interoperability and Information Assurance of the following set of UC that will be expanded in the future:

- Voice and Video Services Point to Point
- Voice Conferencing
- Video Conferencing

More specifically, meeting the requirements specified in this section will allow the current best effort, H.323-based single-vendor Voice over Secure Internet Protocol (VoSIP) network to migrate to an AS-SIP-based multivendor AS network, and enable classified UC products to be tested and placed on the UC APL.

The current Classified Voice and Video over IP (CVVoIP) system is a single security level network operating over the Secret ARs of the DISN that includes secure voice capabilities that interfaces to the DRSN at selected locations. The CVVoIP system described for 2010 is not intended to replace the DRSN and its many unique features.

The contents of this section are arranged as follows:

1. Section 6.2.1, Purpose and Scope, provides the purpose of this section and provides a list of major policies that are unique to the multilevel secure voice services provided by the DRSN and to the single security level DISN VVoIP services.

2. Section 6.2.2, General Requirements Overview, provides a summary of the CVVoIP requirements that drive the CVVoIP design.

3. Section 6.2.3, VoSIP Migration to the DISN CVVoIP, addresses the VoSIP migration to a multivendor IP-based, assured, secure CVVoIP system.

4. Section 6.2.4, Classified Unified Capabilities Technical Design Framework, addresses the migration from the VoSIP to CVVoIP and the migration of the current DRSN APL to a UC APL. The approved products for CVVoIP and the APL process are addressed in Section 4.5, Unified Capabilities E2E Networks Description.

5. Section 6.2.5, Technical Design for 2010, addresses the CVVoIP IP technical design for the 2010 timeframe.

6. Section 6.2.6, Modifications to the SBU Assured Services Features to Include CVVoIP-Unique Requirements. This section describes the modifications to the SBU AS requirements as necessary to include CVVoIP-unique requirements. Topics discussed include, voice EI, LSC requirements, network-level SS, MG, SG, EBC, addressing schema, NM, white pages directory service, voice quality, WAN requirements, and the Information Assurance requirements.

7. Section 6.2.7, Classified AS-SIP-Unique Requirements, defines the modifications to the SBU AS-SIP requirements as necessary for classified AS.

8. Section 6.2.8, DRSN Switches and Peripheral Devices, discusses special construction requirements that include PDS cabling, encryption of facilities leaving a secure enclave, and TEMPEST.

6.2.1.1 Policy and Requirements Documents for DRSN and CVVoIP

All the policies identified in Section 3, Policy, apply to CVVoIP. Table 6.2.1-1, Major Policy and Requirements Drivers for DISN CVVoIP Services, lists the major policy and requirements documents that are unique to MLS voice services provided by the DRSN and to single security level DISN CVVoIP services.

6.2.2 General Requirements Overview

A high-level summary of the requirements for CVVoIP are provided by a combination of the documents referenced in Table 6.2.1-1 and a list of key system attributes that have been established in coordination with the Joint Staff over the past decade as the set of required features for an operational C2 communications service offering. These performance attributes have been proven in real world operations stretching from Desert Shield/Desert Storm through Operation Iraqi Freedom.

Table 6.2.1-1. Major Policy and Requirements Drivers for DISN CVVoIP Services

Joint Requirements Oversight Council (JROC), JROC Memorandum (JROCM) 202-02, "Global Information Grid (GIG) Mission Area Initial Capabilities Document (MA ICD)," 22 November 2002. JROCM and date listed refer to the latest JROC approval of the "Global Information Grid (GIG) Capabilities Requirement Document (CRD)." This MA ICD is a cut and paste conversion of the GIG CRD in MA ICD directed by JROCM 095-04 of 14 June 2004.

DoDD 5200.28, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988.

Homeland Security Presidential Directive/HSPD-7, Subject: Critical Infrastructure Identification, Prioritization, and Protection, 17 December 2003.

Homeland Security Presidential Directive 8 (HSPD-8), "National Preparedness," 17 December 2003.

H.R. 45646, Section 804, "Software Acquisition Process Improvement Programs."

DoD 5200.1-R, "Information Security Program Regulation," 14 January 1997.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, "Operation of the Joint Capabilities Integration and Development System," 1 May 2007.

Global Command and Control Systems-Joint (GCCS-J) Single Acquisition Management Plan (SAMP) for Block V, Version 1.0.

"Joint Command and Control (JC2) Capability Technology Development Strategy (TDS)," Draft, Version 3.3.9.

Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," Revised June 2006.

Defense Intelligence Agency (DIA) Memorandum DIA/DTI-4B, 8 October 1992.

"Operational Requirements Document (ORD) for Secure Voice Requirements," J-6A 01665-92, 17 November 1992.

National Security Telecommunications and Information Systems Security (NSTISS) Instruction (NSTISSI) No. 4010, "Keying Material Management (U)," FOUO, 17 June 1993.

National Security Telecommunications and Information Systems Security (NSTISS) Authority Manual (NSTISSAM) No. TEMPEST/2-95, "RED/BLACK Installation Guidelines," FOUO, 12 December 1995.

National Security Telecommunications and Information Systems Security, NSTISSI No. 7003, "Protected Distribution Systems (PDS) (U)," 13 December 1996.

Defense Nuclear Agency/Defense Communications Agency (DNA/DCA), "Classification Guide for Electromagnetic Pulse Testing (EMPT)," Confidential/Restricted Distribution (C/RD), 16 May 1987.

Table 6.2.1-1. Major Policy and Requirements Drivers for DISN CVVoIP Services (cont.)

National Security Telecommunications and Information Systems Security, NSTISSI No. 4002, "Classification Guide for COMSEC Information (U)," SNF, 5 June 1986. Title 5, U.S. Code, Section 552a (Privacy Act), 23 January 2000. Director of Central Intelligence Directive (DCID) 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities," 30 January 1994. DIA Manual (DIAM) 50-4, "Security of Compartmented Computer Operations," 24 June 1980. DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems."

The most demanding set of requirements in all these documents that drive the DISN Classified IP Convergence Migration Strategy involves those associated with:

- Multilevel secure service
- Rapid, high-quality, secure communications and conferencing capabilities for senior leaders and warfighters
- Assured services
- Information Assurance
- E2E interoperability
- NETOPS

These requirements are the most demanding because COTS IP-based technologies are not sufficiently mature that they require GIG E2E system engineering by the Government, development by industry, and test and evaluation by the Government to meet these policies and requirements. In addition, the challenges discussed in the next section prevent the ability to install a common technology base for all services as a "flash cut." Thus, networks based on hybrid technologies will be required for many years.

One of the key C2 functions of the DRSN is to provide rapid, flexible, and secure conferencing. As a result, a number of unique non-COTS MLS operator console features have been developed in response to the COCOMs' command center requirements. These features, which are part of the way those command centers conduct their business, will not be required for the 2010 CVVoIP.

6.2.2.1 Assured Services

The CVVoIP system shall provide the AS features from UCR 2008, Section 4.2.2, Assured Services Features.

The most important consideration for implementing new technology is the affect on mission requirements. Implementing a new technology, such as VoIP, must primarily not degrade the C2 services currently being provided to secure voice users.

6.2.2.2 Multilevel Secure Voice Services

The DRSN provides DoD multilevel secure C2 voice services and is a key component of the DoD global secure voice services. The DRSN supports the secure voice and secure conferencing, requirements of the NCA, components, DoD, and select federal agencies in peacetime, in crises situations, and in wartime. The DRSN is a separate, secure switched network that is considered part of the DISN. The DRSN, the STU-III/STE family of equipment that provides E2E encryption over the DSN, and Condor (the NSA's program to secure wireless communications) are the three subservices that together provide the foundation for the DoD secure voice services. In addition, DRSN provides an interface to the secure service at the Secret-only level, which shall be provided by the CVVoIP system.

6.2.2.3 Secure Voice Quality Requirements

The EI-to-EI voice quality of a telephone connection is subjective and is determined from the complex interaction of multiple switching, speech encoding, voice compression techniques, and transmission parameters. The objective of the DRSN is to provide toll quality, secure voice service on a DRSN-user-to-DRSN-user basis, and to ensure the highest practical voice quality when DRSN users are interfaced to external systems and equipment. For the DRSN subset of CVVoIP, this is defined as receiving a score of at least 90 on the diagnostic rhyme test (DRT) and a score of at least 60 on the diagnostic acceptability measure (DAM). The DRT measures intelligibility, and the DAM measures quality. The E2E voice quality requirements for the IP-based environment of CVVoIP are based on MOS measurements as defined in Section 6.2.6.10, Voice Quality.

6.2.2.4 C2 Requirements

The DRSN provides all C2 features needed for critical applications while providing the rich feature suite of modern administrative telephony systems. Once IP technology matures to the necessary level, the requirements for CVVoIP will encompass the full DRSN requirements. For the near-term, the following requirements will be met by a mix of IP and the current suite of DRSN switches:

- MLS Voice
  - Variable security access level (applicable to DRSN only, CVVoIP is fixed at Secret)
  - Authentication
  - Low probability of misconnect
  - High crosstalk isolation
  - TEMPEST/EMI compliance
- Integrated Red-Black instruments (DRSN only)
  - Instruments located in a Secure Compartmented Facility (SCIF) must be Telecommunications Security Group (TSG)-Approved (DRSN and CVVoIP).
- Secure conferencing
  - Ad hoc conference (three-way CVVoIP and DRSN)
  - Preset conference (CVVoIP and DRSN)
  - Unlimited (DRSN only)
  - Dissimilar devices (DRSN only)
  - Distributed across network (DRSN only)
  - Variable security levels during conference execution (DRSN only)
- Assured connectivity
  - Nonblocking components
  - Transport bandwidth
  - Resilient routing
  - MLPP with override of FLASH OVERRIDE
- High availability
  - Redundant components
  - Redundant transport

  - High-altitude electromagnetic pulse (HEMP) survivability for selected sites

- Real-time operational control

  - C2 consoles giving execution control to operational personnel
  - "Override" capability by operational personnel
  - "Visibility" to operational personnel

- Management

  - Administrative (Provisioning)
  - Utilization (NM)
  - Fault management
  - Real-time health monitoring

- Interoperability

  - Legacy devices (secure voice radios, instruments, and other terminal types (DRSN only))

  - Dissimilar devices (e.g., between MILSTAR and STE terminals (DRSN only))

  - Media conversion

  - Protocol conversion

  - Speakers, recorders

  - Other networks, such as MILSTAR.SECN, DSCS/EPC, Homeland Security, FBI, and Department of State (DRSN only)

6.2.2.5 Key CVVoIP Voice Services Features

The key CVVoIP voice services features and attributes are shown in Table 6.2.2-1, Key CVVoIP Voice Service Features.

Table 6.2.2-1. Key CVVoIP Voice Service Features

FEATURE NAME	FEATURE FUNCTIONAL PURPOSE
Automatic Number Identification (ANI)	Identifies the caller before the call is answered.
Display of Call Security Level	Identifies the classification level of an incoming call.
Directory (White Pages) Service Access	Presents location information and telephone numbers of personnel by using the IP EI display.
Instrument Lock-Out	Requires user login to activate an instrument. Any IP EI must be DISABLED at all times when not under the physical control of the authorized user.
COTS Features	Call forward, call waiting, call hold.

6.2.2.6 General Security Features

The DRSN Red Switches, classified LSCs, and Tier0 SSs must operate with physical security and TEMPEST compliance to allow users within a Red enclave to conduct unencrypted, classified telephone conversations at the level commensurate with the facility, system, and user clearances. As a minimum, DRSN switching nodes must operate at the Top Secret security level. However, VoSIP and CVVoIP users and classified LSCs are only to be configured at the Secret level until an MLS operation for IP-based technology is mature.

Telephone instruments installed outside the Red enclave, but within a limited exclusion area in the same facility may be connected to the switching subsystem through an approved PDS or link encryption between the Red enclave and the "exclusion" area.

All other connectivity into and out of a DRSN or CVVoIP Red enclave must be secured with NSA-approved encryption equipment. In addition, connections to a CVVoIP system (and VoSIP) must be approved or implemented as defined by the SIPRNet Connection Approval Process. The DRSN Red Switches, VoSIP Call Manager, and classified LSCs must interconnect with other Red Switches and/or peripheral devices (to include, but not limited to, Tactical secure voice switches/enclaves, radio interfaces, audio systems, voice announcers, and multimedia and/or secure voice over data capabilities) through encrypted Interswitch Trunks (ISTs) or by means of a PDS. Other secure systems must interconnect to the DRSN using DISA-established interface criteria and encryption devices or a PDS.

6.2.2.7 Special Security Features

The following special security features are currently inherent to the DRSN. The following text is included to aid the reader in understanding the full aspects of the special security features. For CVVoIP, the initial feature set is limited to a fixed call security level of Secret. The Confidential Access Level (CAL) parameter within the AS-SIP requirements is used to convey the call security level.

1. Automatic Number Identification (ANI). During intraswitch and interswitch call processing, DRSN switches exchange classmark information that include the calling and called-station identity and call security access level (SAL) assignments. The ANI information (of the calling party) is displayed on the called party's DRSN user telephone display before the call being answered by the called party. When the called party answers, the ANI information of the called party is displayed on the calling party's DRSN user instrument as well as the security level (i.e., Secret, TS, or TS/SCI) of the established connection being displayed on both the calling and called parties' DRSN user instrument. User ANI identity information is defined in the database of the DRSN switch to which a user is directly connected. All equipment connected to the DRSN must be capable of providing ANI to the DRSN switch to which it is or will be connected. The CVVoIP instruments will be fixed at the Secret level and display the calling telephone number via AS-SIP signaling.

2. Security Access Level. The SAL is a user classmark assigned to each instrument, line key, and trunk, and provides security authentication of the calling and called party. The SALs are assigned to each instrument, line key, and trunk based on the classification and access level authorized for the user. The DISA DRSN Service Manager will develop and publish a standardized set of SALs, which must be implemented at all DRSN nodes. In addition to a standardized set of SALs, the DISA DRSN Service Manager may implement special SALs on a case-by-case basis to meet specific mission requirements. Alteration of SALs and/or implementation of SALs without specific direction and/or approval of the DISA DRSN Service Manager are not permitted and constitute a reportable security infraction.

3. Automatic Security Authentication (ASA). The ASA ensures DRSN calls are set up in accordance with security and access authorization criteria defined for each user and/or DRSN switch interface. The ASA uses a combination of fixed and variable SAL assignments to reconcile and establish, or deny establishment of, connections between users and between users and DRSN switch interfaces based on a highest common denominator scheme. For example, a connection between a user classmarked with a Variable SAL (VSAL) (see paragraph b) of Secret calling a user classmarked with a VSAL of TS will be permitted at the Secret level. As another example, a connection between a user classmarked with a VSAL of Secret calling a user classmarked with a Fixed SAL (FSAL) (see paragraph a) of TS/SCI will NOT be permitted because there is no highest common denominator. This highest common denominator ASA scheme is equivalent to that implemented in the STU-III/STE family of equipment.

    a. Fixed Security Access Level. The FSAL emphasizes call security over call completion. A user selects an FSAL classmarked line when he or she must ensure the call is established at the desired security level. Under FSAL, a call's SAL is "fixed" at the user-selected level and cannot be downgraded as the call progresses through the network. If the called and calling parties and interconnecting trunks are classmarked

with the same SAL (e.g., TS), the Red Switches will establish the call and display the common security level. If a trunk group with a SAL equal to that of the originating station is unavailable for call routing, the originating Red Switch will not complete the call, but instead will route the call to a security code violation recorded announcement. If the called party has a different SAL assignment than the calling party (e.g., the called line is assigned Secret and the calling line is assigned TS/SCI), the call will not be completed, and the originator will be routed to a security code violation recorded announcement. The CVVoIP instruments will be fixed at the Secret level.

b. Variable Security Access Level. The VSAL emphasizes call completion over call security level. With VSAL, a call is established if network resources are available. However, the call may be established at a security level less than that selected by the calling party. The VSAL feature allows calls to be set up when the SAL codes among calling and called stations and trunk groups are unequal. Calls are automatically established at the highest common security level of the users and trunk facilities. The highest common security level, as determined by the switching system, is displayed on the called and calling instruments. Users must read the displayed security level and ensure the security level of conversations does not exceed the displayed security level. The CVVoIP instruments will be fixed at the Secret level.

4. Push-to-Talk Handset. The push-to-talk handset is an integral part of the physical protection afforded classified DRSN voice traffic. Removal of the push-to-talk feature may be justified only by legitimate operational requirements and will be approved on a case-by-case basis of the DAA, through the DISA DRSN Information Systems Security Manager. Before removal, the user must justify the action, develop procedures for maintaining the secure integrity of the instrument, and have written approval in accordance with DRSN security guidelines.

6.2.2.8 Network Security

1. The DRSN Red Switches, VoSIP Call Managers, classified LSCs, and Tier0 SSs must be located in Red enclaves. The DRSN Red Switches at locations that have subscriber terminals authorized to process TS/SCI must be located in SCIFs. The DRSN Red switches, VoSIP Call Manager, and classified LSCs will provide the following:

   a. In-the-clear calling within each Red enclave by means of PDSs and protected ASLANs

   b. Cryptographically protected calling between Red enclaves supported by DRSN Red switches and VoSIP Call Manager and classified LSCs

c. DRSN Red Switches, VoSIP Call Managers, and classified LSCs interface to external cryptographic equipment for all other calling

2. The NSA-approved encryption equipment provides COMSEC to the DRSN and the CVVoIP system. The encryption equipment or PDSs secure all DRSN ISTs and protect links to remote enclaves to include remote locations and quarters. The TSEC/KG-84 family of equipment (including KIV-7) provides Transmission Security (TRANSEC) to ISTs to locations (including quarters) receiving DRSN service via DPA, DTAs, and KG-84 telephone interfaces. The TSEC/KG-81 family of trunk equipment (including KIV-19s, TSEC/KG-81s, TSEC/KG-94s, and TSEC/KG-194s) bulk encrypts the digital streams between geographically separated Red enclaves.

3. The DRSN/VoSIP/CVVoIP instruments and service capability may be installed in senior officer quarters on a case-by-case basis. Such installations constitute the establishment of a Red enclave/limited exclusion area within the quarters and must comply with physical and technical security criteria applicable to the use and storage of COMSEC equipment. Use of DRSN equipment in quarters must comply with DRSN operating and security procedures applicable to a Red enclave office environment.

   a. Any DRSN telephone instrument installed in a quarters must be DISABLED at all times when not under the physical control of the authorized user.

   b. Where the Red signal path (digital or analog) between COMSEC and the DRSN Red equipment (i.e., DRSN instrument and other DRSN terminal equipment) is greater than 3 meters from the COMSEC device, the Red signal path will be routed in an approved PDS.

   c. Before the installation of DRSN service in quarters, the DISA DRSN Service Manager should be contacted for approval and confirmation of current applicable operating and security criteria.

6.2.2.9 Network Interfaces

A key feature of the DRSN is its ability to interface and interoperate with a variety of DoD and commercial networks. The CVVoIP and VoSIP systems interface to the DRSN through a gateway. (See UCR 2008, Section 6.2.6.4, Media Gateway with Signaling Interworking.) The current VoSIP to DRSN interface uses a vendor-unique implementation of a PRI trunk-signaling interface.

As part of the migration toward a multivendor-based CVVoIP environment, gateway signaling between CVVoIP system, the DRSN and VoSIP will be standardized to accommodate AS-SIP

signaling. During a transition period, an SG will allow H.323-based VoSIP to work with the AS-SIP-based CVVoIP system.

6.2.2.10 CVVoIP and VoSIP Connection Approval

All interfaces to the DRSN must be approved in writing on a case-by-case basis by the DISA DRSN Service Manager. Connection to the CVVoIP system and VoSIP must follow the SIPRNet Connection Approval Process. The JITC certification letters documenting a technical interoperability with the DRSN do not constitute connection approval. Such certification letters only serve as a technical basis for requesting approval for connection to the DRSN in support of a Joint Staff-validated mission requirement. The DISA DRSN Service Manager‘s approval for an interface may be in the form of a permanent, conditional, or temporary interface. Use of interfaces not conforming to DRSN interface criteria or as stipulated in the DISA DRSN Service Manager’s approval letter can have adverse technical and security impacts on all DRSN users and constitute an unauthorized use of the DRSN. Any such interfaces can result in the switch supporting such interfaces being denied network-level access to the DRSN infrastructure. All connectivity from a DRSN switch to users outside the Red enclave (i.e., to another building, facility, location, or system) must be provided through an approved interface.

6.2.2.11 DRSN/VoSIP/CVVoIP Network Management

DISA establishes DRSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. The DRSN is under the management control of the Director, DISA SSM, on behalf of USSTRATCOM, and is responsive to the CJCS, the COCOMs, the MILDEPs, and Defense agencies and activities.

1. DISA must possess read-access capabilities and limited/controlled write-access capabilities to all DRSN switch and network-level classified SSs (Tier0 SSs) network-related database tables, Red bandwidth managers, and other network-level infrastructure data.

2. DISA must maintain a CM database of all switch configurations (CONUS and OCONUS) and provide access to agencies, activities, and MILDEPs as authorized by OSD, the Director, DISA, and the Joint Staff.

3. DISA must have the ability to implement network-level database changes and/or network control commands to all DRSN nodal switch and classified network-level SSs (Tier0 LSCs) network-related database tables, Red bandwidth managers, and other network-level infrastructure data. To the maximum extent practical, the DISA DRSN Service Manager must attempt to notify O&M activities before implementing DRSN nodal switch network-level database changes and/or network controls.

4. During emergencies, DISA has the authority to use direct write capabilities to implement switch database revisions required for operation and management of the DRSN.

5. DISA will take necessary action to establish capabilities and procedures necessary to sustain the DRSN and VoSIP/CVVoIP if a failure of the GNSC/TNC occurs and to reconstitute a major DRSN nodal element if a catastrophic failure occurs.

6.2.2.12 Directory (White Pages) Services

The CVVoIP will have a directory services capability for searching "white pages" that allows subscribers to look up specific and applicable user information assigned to other CVVoIP subscribers. This is a FY 2012 Objective requirement and is included for consideration by LSC/SS product development teams. The directory system will be of the same design as described for SBU VVoIP in Section 5.3.2.27, Directory Services ("White Pages"), but for security reasons, the CVVoIP system will not be shared with the SBU system, but implemented as a separate system dedicated to CVVoIP.

6.2.2.13 Conferencing Requirements

The CVVoIP services will not provide the full conferencing features inherent with the DRSN. The CVVoIP conferencing features are currently limited to three-way calling and preset conferencing. Enhancements based on implementing "Meeting Place" servers at selected DISN core nodes are under consideration. Expanded requirements for secure preset and meet-me conferences based on SBU voice subscribers equipped with NSA Type 1 encryption devices are provided in Section 6.2.10, UC Secure Preset Conference.

6.2.2.14 CVVoIP Equipment Certification and Testing Policy

Interoperability and Information Assurance testing of CVVoIP equipment will follow the standard process outlined in UCR 2008, Section 4.5, Unified Capabilities Approved Product List Process.

6.2.3 VoSIP Migration to the DISN CVVoIP

Figure 6.2.3-1 provides an overview of the integrated migration strategy for the VoSIP migration to CVVoIP. The left side of the figure illustrates today's environment. Currently, the DRSN is providing critical Classified voice and conferencing services using TDM/circuit switched technologies. The VoSIP uses the SIPRNet and single-vendor (Cisco®) voice equipment.

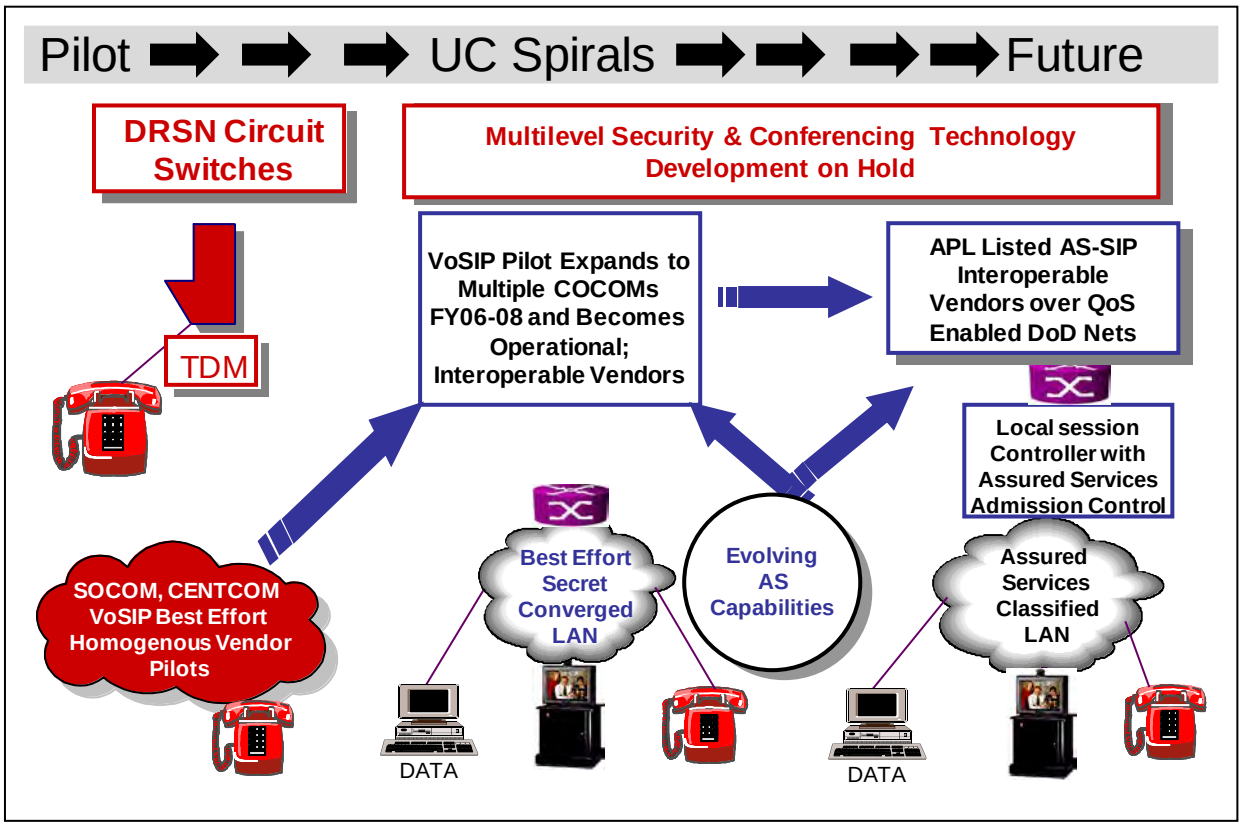

Figure 6.2.3-1. VoSIP Migration to DISN CVVoIP

On the right side of the figure, the target Net-Centric CVVoIP solution is shown. The future target is an all IP solution using the DISN WAN that will provide QoS and Edge solutions, which will provide ASLANs. These ASLANs will have functionality to provide bandwidth allocation for voice and video based on precedence among voice, video, collaboration, time critical messaging, and other service offerings (e.g., e-mail, NCES web portals). The ASAC will provide the required PBAS to replace MLPP on the WAN. The AS-SIP signaling will be used to set up and take down the CVVoIP sessions and will allow multiple vendors to provide systems based on the UC APL. The ASLAN will support fully converged services meeting the performance and security requirement of each service.

The connection between today's systems and the future target is the major migration challenge. The DRSN's unique features of MLS and conferencing require both IP technology development and the expansion of the vendor base for these features to try to create a competitive market. A multivendor MLS market may not be practical, while a multivendor conferencing market must be practical. Investment is essential for this collaborative Government and industry effort. Until this investment is made and the effort succeeds, all nuclear C2 users will continue to get their service via the legacy DRSN. As a result, the CVVoIP requirements will be focused initially on a single security level (Secret). Currently, the VoSIP Pilot is being expanded to include multiple COCOMs and is open to all vendors when they meet the VoSIP Pilot technical requirements and

can provide AS-SIP. A dual-signaling directory/gatekeeper (Tier0 SS) will be deployed to allow users to migrate from the signaling protocol of the pilot to a fully AS-SIP signaling environment. The work (i.e., system design, engineering, assessment, and pilot testing, GSR) on both SBU and CVVoIP will be leveraged to evolve the assured services capabilities to allow CVVoIP products to be placed on the UC APL.

An E2E view of the DRSN/VoSIP IP migration strategy needed to meet the CVVoIP migrations is illustrated in Figure 6.2.3-2, DISN CVVoIP Convergence Migration Strategy Overview.

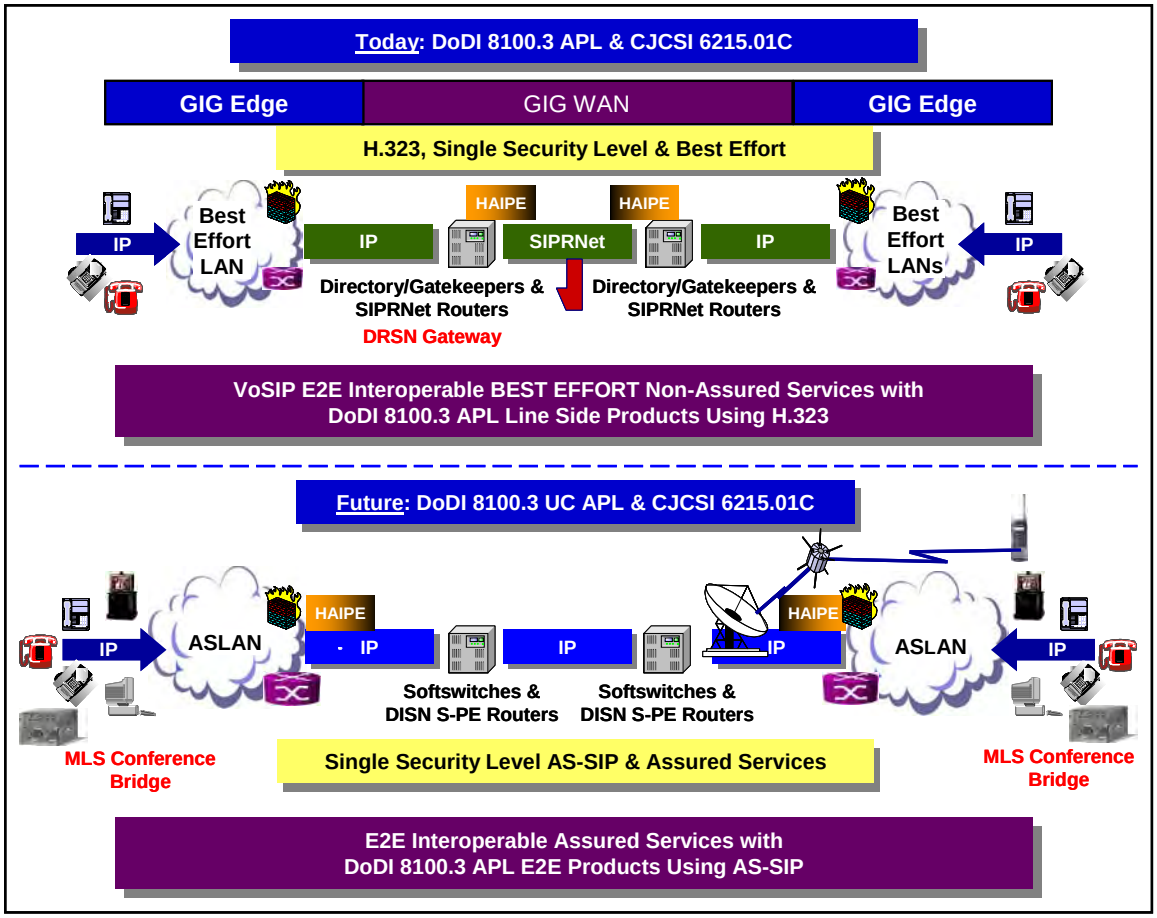

Figure 6.2.3-2. DISN CVVoIP Convergence Migration Strategy Overview

The top of Figure 6.2.3-2 shows the current VoSIP capability, which is a Single Security Level Best Effort service over the SIPRNet, using the H.323 signaling protocol. The DISN Video Services II (DVS II) VTC IP services and data services, ranging from e-mail to web services to C2 applications, are also sharing the same LANs and the SIPRNet backbone as IP converged services. However, the VoSIP Pilot is focused only on voice services. The DRSN circuit-switched services interface the VoSIP services via SGs and MGs. The DRSN provides the critical MLS and conferencing services that IP technologies cannot provide currently. In

addition, the DRSN circuit switches serve as the interface to critical interoperable services to national security networks, allies, and federal and civil agencies.

The bottom of the figure shows the future CVVoIP services, where AS-SIP signaling is used to allow for heterogeneous vendor edge APL solutions and for assured services to be provided E2E as a first step. A gateway to the DRSN provides access to the DRSN for selected users. A future step may be a limited phase-out of the DRSN and the phase-in of the MLS and conferencing features of the DRSN pending a funded successful research, development, testing, and evaluation (RDT&E) program to develop the features in IP-based technologies.

The current Best Effort VoSIP network must be upgraded to migrate from H.323 to AS-SIP, which will provide for assured information delivery E2E under conditions where bandwidth is restricted due to network damage, surge traffic, or Tactical deployments. This migration provides a single level of security over the secret level DISN aggregation routers and is still dependent on the DRSN for MLS and conferencing services.

The progress being made by the NSA with respect to the modifications needed to HAIPE and cross-domain solutions to allow RSVP to achieve its full potential will be monitored closely.

An upgrade to the VoSIP Directory/Gatekeeper to support both H.323 and AS-SIP signaling will be conducted, and the Gatekeeper will be placed on the UC APL. Interoperable classified VVoIP vendors will be tested and placed on the UC APL for CVVoIP products using AS-SIP. Thus in FY 2010, the operational VoSIP services can begin migration to assured services instead of Best Effort enabled by AS-SIP based on available funding by the MILDEPs to upgrade their existing systems as part of their normal scheduled upgrades.

The migration of the DRSN MLS and Conferencing features to IP technologies cannot be described at this time because extensive RDT&E has not begun.

The DRSN circuit-switched network could phase out eventually if:

1. Unified Capabilities migration classified MLS system design, system engineering, UCRs, and test programs are completed. The 2009 System 70 percent design and UCR 2008 must be validated in the DISN VVoIP Spiral deployment of capabilities. This will provide the VVoIP foundation on which the migration to classified UC can be implemented using future versions of the UCR consistent with major policies and requirements for Net Centricity and NETOPS that are continuing to be refined and matured. In addition, the RDT&E program to develop MLS IP technologies must be successfully completed and result in a UCR that both the DIA and NSA approve.

2. The DISN WAN and MILDEP Intranets SLAs for QoS capabilities are available. Assured services requirements capabilities projected to be available during the 2010 time frame

include: assured service SLAs (e.g., nonblocking GOS, voice and video quality, packet loss, jitter, latency, availability, DSCPs from the GIG QoS Working Group, PHB determined by supporting network based on VVoIP SLAs).

3. The UC APL assured services solutions are available. All IP solutions necessary to replace the circuit-switched services are on the APL.

4. Deployment is completed for dual-signaling H.323/AS-SIP SSs, which allow for secure interoperability among multiple vendors and mixed technologies.

5. The "UC Master Plan" is approved.

    a. The DoD plans and programs to fund, purchase, and install hybrid MFSSs and, ultimately, migrate to pure SSs for SBU voice and video.

    b. The DoD components plan and program to fund, purchase, and install VVoIP Edge systems from the APL.

    c. The DoD Tactical community plans and programs to fund, purchase, and install VVoIP APL Edge systems or obtain a Joint Staff-approved ISP.

6. The "UC Master Plan" is executed. Detailed joint transition and cutover planning unique to each theater and country will be required.

6.2.4 Classified Unified Capabilities Technical Design Framework

Initially, the classified UC technical design will be focused on VVoIP. The CVVoIP technical design will transform in each of the three target timeframes: 2009, 2012, and 2016. Due to funding and technology maturity, in all three timeframes, CVVoIP will be provided by three types of designs: 1) FY 2009 Hybrid with DRSN and VoSIP Pilot design, 2) FY 2010 Hybrid with DRSN and CVVoIP converged at the Edge, and 3) Post-FY 2016 goal design of IP E2E. Figure 6.2.4-1, CVVoIP FY 2009 Hybrid Design, illustrates the FY 2009 Hybrid with DRSN and VoSIP Pilot designs. The top of the figure illustrates that the current VoSIP Pilot design, which uses H.323 signaling, is a single security level with Best Effort over the SIPRNet. This design cannot provide precedence and preemption to support bandwidth on demand based on mission priorities consistent with SA.

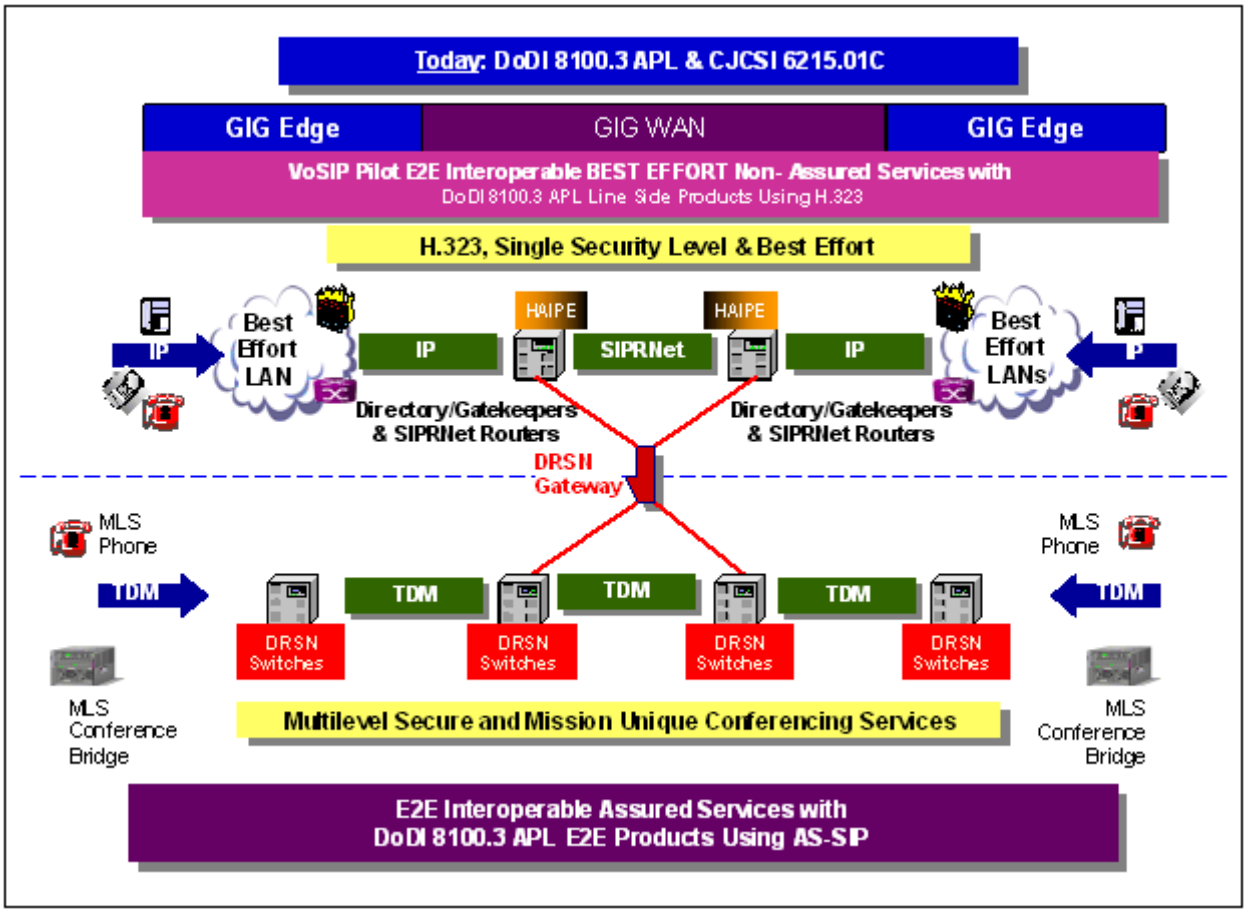

Figure 6.2.4-1. CVVoIP FY 2009 Hybrid Design

Figure 6.2.4-2, DISN CVVoIP FY 2009 Design Overview, illustrates the FY 2009 design, which is the first major step in the VoSIP migration to allow for IP-converged operations at the Edge and for precedence and preemption to support bandwidth on demand based on mission priorities consistent with SA. This is achieved by using the SBU VVoIP APL solutions with augmented AS-SIP signaling. In addition, this design extends assured services to the Tactical community through the DISA Teleport program and because of collaboration with the Tactical programs in the development of their ISP and TISPs. The implementation of these designs is dependent on the continued updating of policy to address the potential phase-out of the DRSN with an all IP-based system (e.g., CVVoIP).

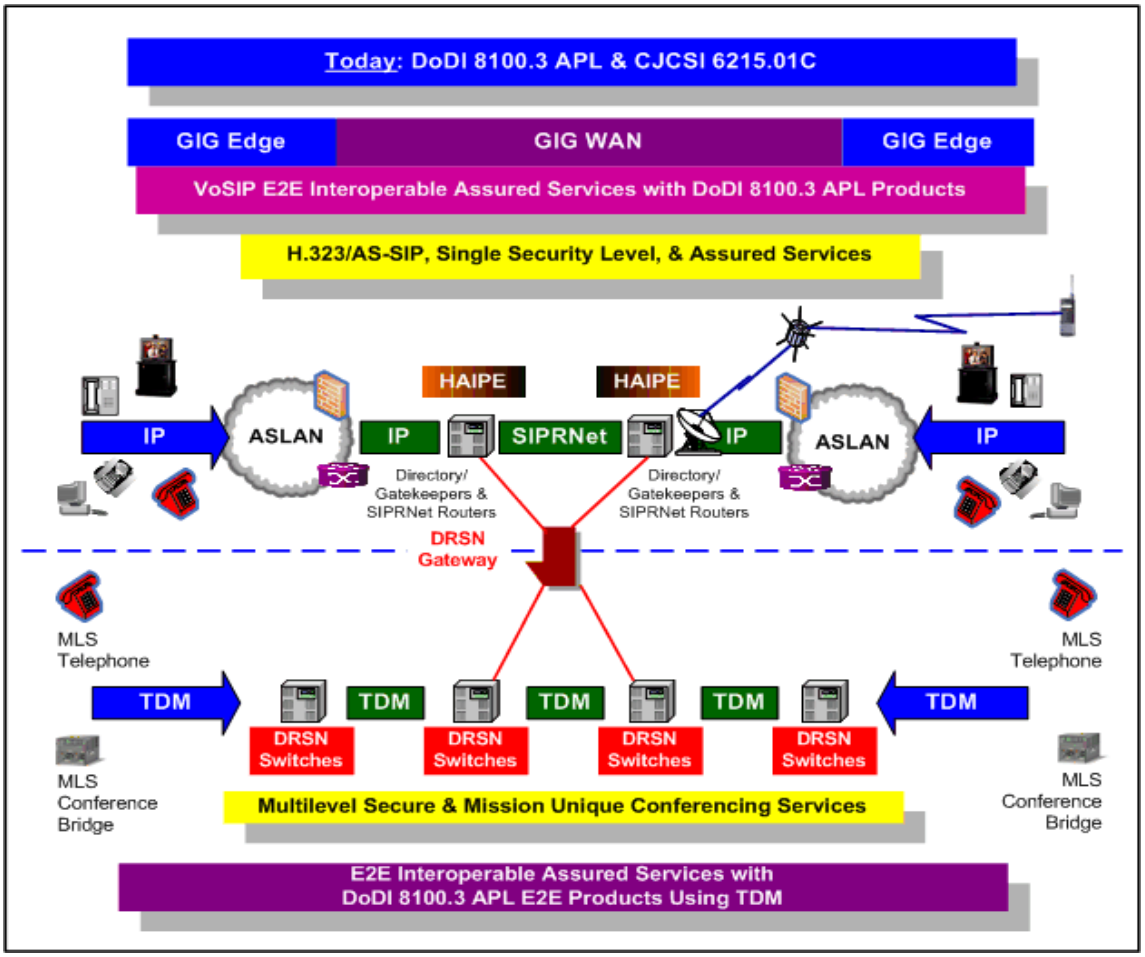

Figure 6.2.4-2. DISN CVVoIP FY 2009 Design Overview

Figure 6.2.4-3, Three-Tier Design of the VoSIP Associated with the CVVoIP FY 2009 Design, illustrates the three-tier design of the VoSIP associated with the CVVoIP FY 2009 design, as it migrates from a Best Effort voice service based on H.323 signaling to an assured services CVVoIP based on AS-SIP signaling.

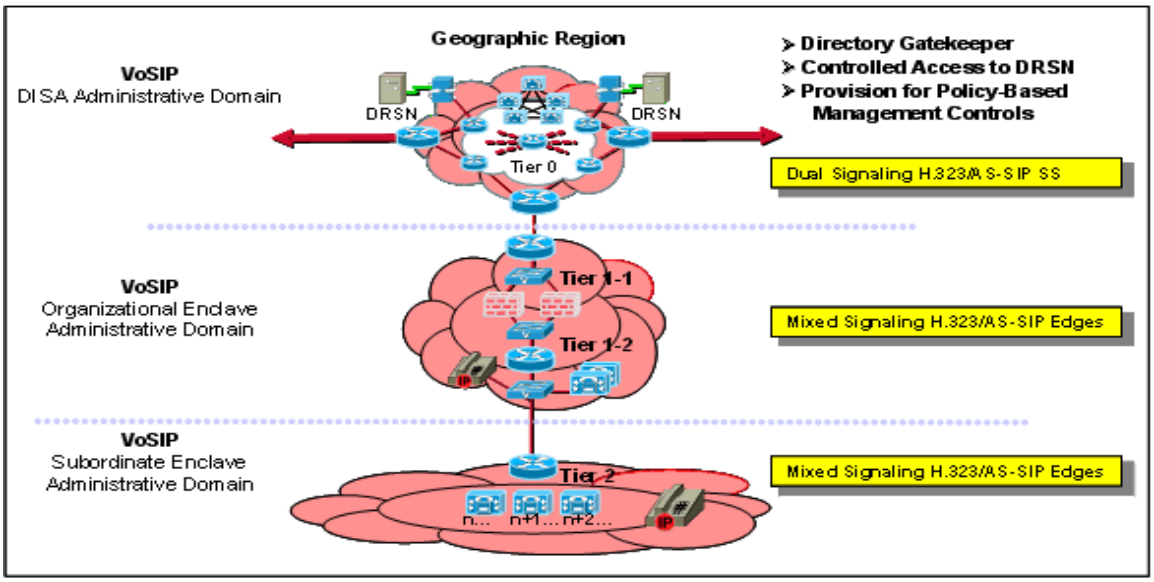

Figure 6.2.4-3. Three-Tier Design of the VoSIP Associated with the CVVoIP FY 2009 Design

6.2.5 Technical Design for 2009

Figure 6.2.5-1, Overview of CVVoIP Assured Services Design for FY 2009, illustrates the CVVoIP technical design for assured classified services at a single security level in the 2009 timeframe. The red text illustrates the significant changes introduced to achieve E2E CVVoIP with assured service. The design is similar to the one that will be used by the SBU VVoIP with the following significant differences:

1. The Secret Provider Edge (S-PE)/Secret Customer Edge (S-CE)/Secret Aggregation (S-A) Routers versus the Unclassified Provider Edge (U-PE)/Unclassified Customer Edge (U-CE)/Unclassified Aggregation (U-A) Routers will be used.

2. HAIPE will be used with the S-PE Router.

There may be variations in the version of AS-SIP that will be used.

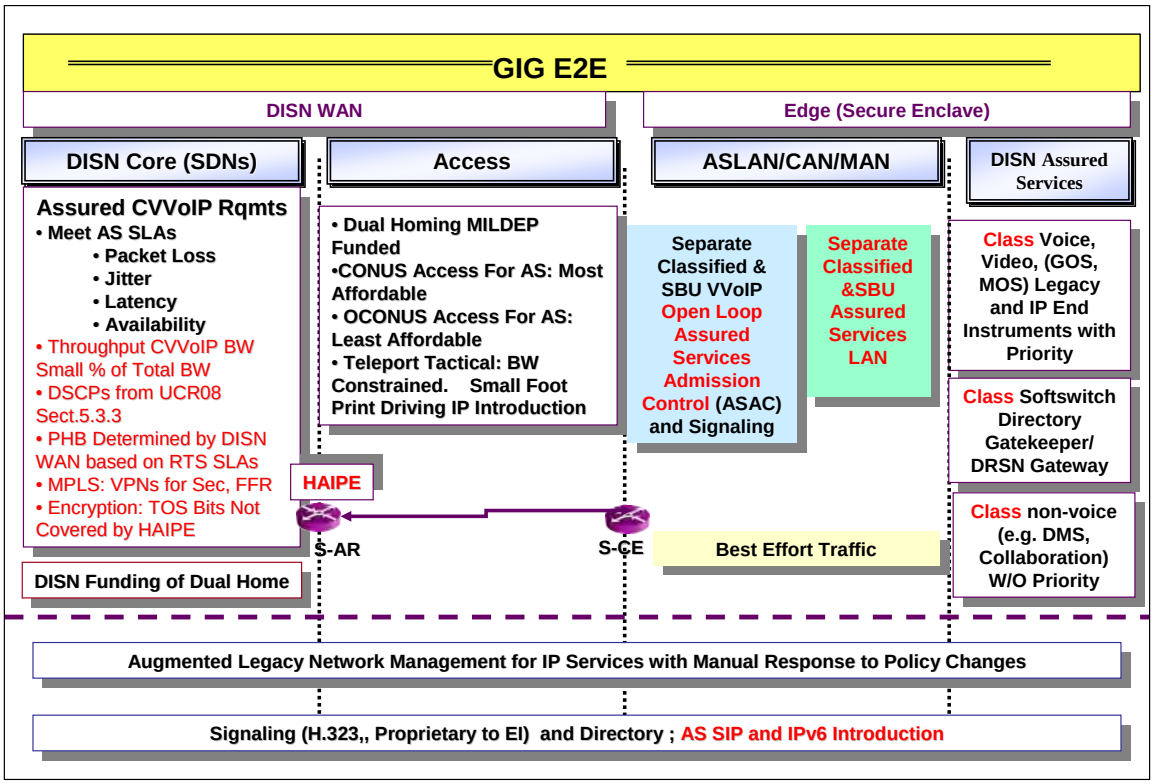

Figure 6.2.5-1. Overview of CVVoIP Assured Services Design for FY 2009

The classified SS, called a directory/gatekeeper in the current VoSIP system, is pure IP without a TDM signaling capability, and provides a unique interface to the DRSN.

Both networks depend on the robustness of the DISN WAN and its ability to meet SLAs for CVVoIP as illustrated by the list in the DISN Core portion of the chart.

In this timeframe, TDM-based classified video service for services will be H.320 (KIV-7 encrypted) over the legacy DSN switches for users who have not yet migrated to IP. Single security level IP-based secure video over SIPRNet is available from secure enclaves. Multilevel secure video will be provided by ISDN and KIVs that allow unencrypted signaling, and then transition to an encrypted bearer mode. This is because no MLS IP encryptors are available to support IP video services. The DVS II hubs will interoperate with the legacy ISDN H.320 services as well as with IP video H.323 users. Users will be encouraged to convert to IP video services when AS-SIP with the full H.323 feature set is available some time in 2009. Nevertheless, until NSA develops an IP replacement for the KIV, multilevel secure services will have to be over the DSN ISDN circuit-switched services.

6.2.5.1 FY 2009 Signaling Design

The signaling design for this timeframe has to provide both backward and forward technology capabilities. Thus, CAS and PRI in the DRSN has to interoperate with H.323 signaling in the VoSIP Pilot to be followed by H.323 and AS-SIP interoperating in CVVoIP until all IP services are via AS-SIP. Once that is achieved, the DRSN interoperability must be maintained until its features can be replicated with IP technologies.

The hybrid CVVoIP signaling design for FY 2009 is depicted in Figure 6.2.5-2, DISN CVVoIP FY 2009 Signaling Design.

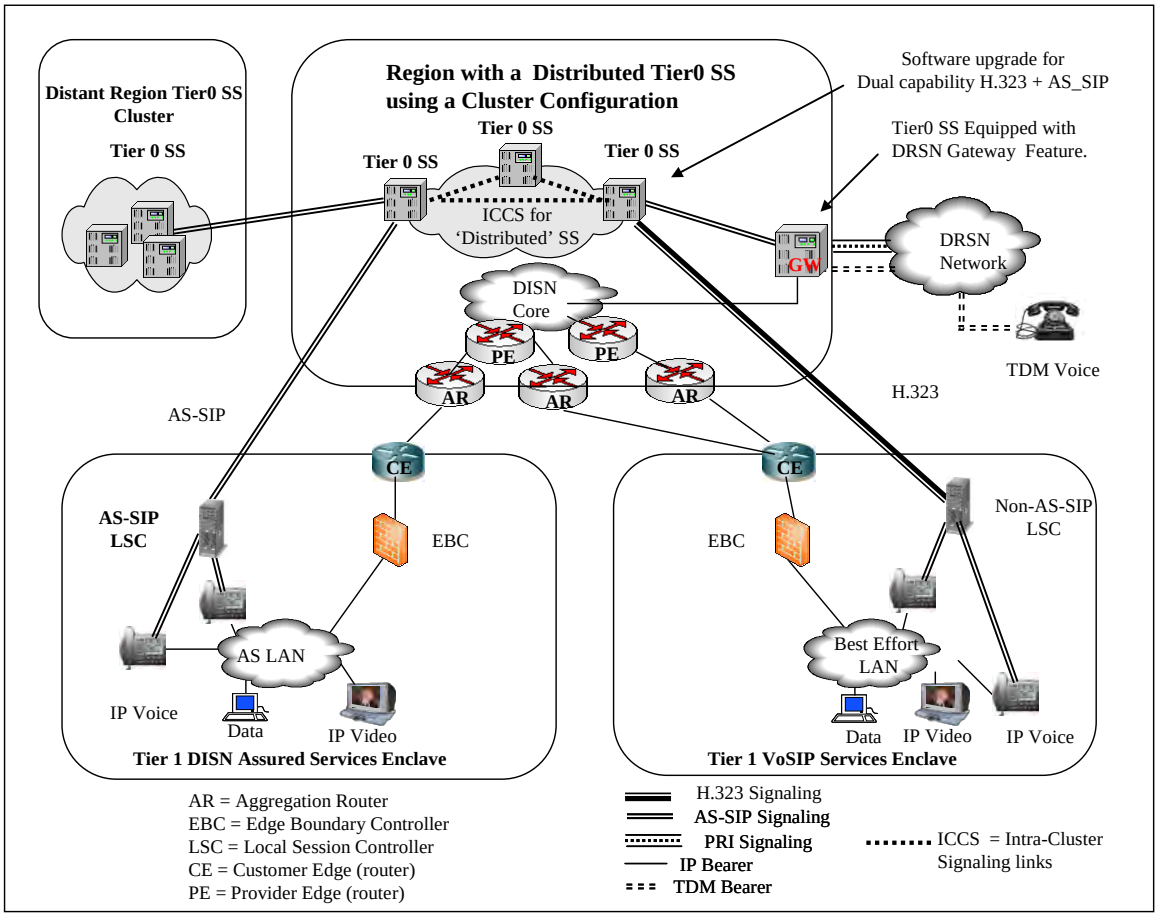

Figure 6.2.5-2. DISN CVVoIP FY 2009 Signaling Design

The signaling design is constructed as a two-tier hierarchy consisting of a "local" level and a "backbone" level. At the local level, LSCs are located in secure enclaves and represent the level of the signaling hierarchy closest to the EIs. The local level is based on a multivendor assortment of LSCs. The backbone, or Tier0 signaling, level is of a robust, homogeneous design based on current vendor-unique geographic cluster arrangements of Tier0 SS used in VoSIP. The CVVoIP assured services signaling backbone will be based on the Tier0 SS cluster concept,

with AS-SIP as the CVVoIP signaling method, but during the transition period from VoSIP to CVVoIP there will be segments using H.323 signaling also. Signaling interoperability between H.323 and AS-SIP will be achieved by an APL product called a Dual Signaling Softswitch (DSSS). (See Section 6.2.6.3, Network-Level SSs.)

The backbone Tier0 SSs represent the upper level of the signaling hierarchy and provide inter-enclave as well as inter-geographical area signaling forwarding. Some of the LSCs as well as a few, select Tier0 SSs provide "Managed Services" to a limited set of EIs and, therefore, a Tier0 SS may also have an LSC function associated with it.

Every LSC is assigned to a primary Tier0 SS and to at least one secondary Tier0 SS for automatic failover.

A Tier0 geographic cluster typically consists of at least three Tier0 SSs. The clustered SSs are connected over proprietary Intra-Cluster Communication Signaling (ICCS) links, and they automatically update each other's databases, as required, in response to configuration changes within the geographic region controlled by the cluster, and as such, can be viewed as a distributed SS. This feature provides an extremely robust Tier0 signaling design enabling automatic nonservice interrupting failover in case a Tier0 SS goes down. The distance between the clustered SSs must be planned so that the maximum round-trip time (RTT) between the clustered SSs does not exceed 40 ms. Based on a propagation delay of 6 microseconds per kilometer without any other network delays being considered, this translates to a maximum theoretical transmission distance of approximately 1860 miles.

To simplify the signaling path description below, the term Tier0 SS from here on refers to a geographic clustered Tier0 SS. Note that during a transition period, H.323 and AS-SIP will coexist at certain locations with interoperability provided by the DSSS. All session signaling messages received by an LSC from a local EI and intended for a destination outside the secure service enclave is sent by the LSC in the form of an AS-SIP message to its assigned Tier0 SS. The Tier0 SS then forwards the AS-SIP message to the distant end by either forwarding the message directly to the distant-end LSC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end LSC. Similarly, all session signaling messages sent from a remote location and intended for IP EIs associated with a given LSC will be routed to the Tier0 SS assigned to the destination LSC and the Tier0 SS will forward the AS-SIP signaling messages to the destination LSC.

The basic AS-SIP message flow between an originating LSC assigned to one backbone geographic cluster Tier0 SS and a destination LSC assigned to another backbone geographic cluster Tier0 SS is:

Originating LSC --- Tier0 SS 1 ---------- Tier0 SS 2 --- Destination LSC

The basic AS-SIP message flow between an originating LSC and a destination LSC assigned to the same Tier0 SS is:

Originating LSC --- Tier0 SS --- Destination LSC

The access link between the CE Router and the AR is resource constrained and the LSC has primary responsibility for ensuring that the telephony traffic across the access link does not exceed a provisioned threshold call count and that the video traffic across the access link does not exceed a provisioned threshold bandwidth.

The Tier0 SS is responsible for implementing a Policing function to protect the access links (and to protect the classified network itself) where the Tier0 SS intervenes by blocking session requests or preempting session requests and active sessions when the Tier0 SS determines that the LSC has exceeded its provisioned threshold for voice traffic or video traffic.

6.2.6 Modifications to the SBU Assured Services Requirements to Include CVVoIP-Unique Requirements

Section 5.3.2, Assured Services Requirements, addresses the functions, methods, protocols, and associated technical parameters for the EI, LSC, MFSS, EBC, and NM components of the DISN VVoIP System. Section 5.3.4, AS-SIP Requirements, provides the complete requirements for AS-SIP, including both the SBU and unique classified requirements.

This section addresses the AS requirements that are unique to the CVVoIP services.

In general, the majority of the SBU requirements are applicable and common to both the SBU and classified VVoIP services. The following modifications and additions to the SBU requirements are caused by unique CVVoIP requirements.

6.2.6.1 Voice End Instrument

1. Voice EI requirement: Section 5.3.2.6.1, Voice Instrument, defines a CAC-enabled instrument as a Conditional requirement. For classified instruments, this is **Required**.

2. New exclusive requirement for classified instrument: Display CAL (security level) of the call.

3. New exclusive requirement for classified: Telephone browser or menu capability to access system-wide white pages directory. (Objective: FY 2012 requirement)

6.2.6.2 Classified LSC Requirements

6.2.6.2.1 SBU LSC Requirements Not Applicable to Classified LSC

The following LSC requirements defined in Section 5.3.2.7, Local Session Controller, do not apply to the classified LSC:

1. MG, SG for SS7 (the classified LSCs do not interface to external networks)

2. Public safety features (e.g., PSAB, E911 access)

6.2.6.2.2 Classified LSC Unique Requirements

The following requirements are unique to classified LSCs:

- Located in secure enclave
- PDS cabling per DRSN requirements
- DHCP not allowed, strict control of EI assignments
- Use the classified version of AS-SIP signaling

6.2.6.3 Network-Level SS

Section 5.3.2.8, Network-Level Softswitches, describes the network-level SSs used in the SBU network (e.g., the MFSS and WAN SS). The CVVoIP system uses a unique backbone SS referred to as a Tier0 SS. During the VoSIP to CVVoIP transition period, the Tier0 SS will be augmented to provide a dual-signaling capability to provide interoperability between H.323 and AS-SIP-based LSCs. When augmented, the Tier0 SS will become an APL product referred to as a DSSS. Figure 6.2.6-1, DSSS Reference Model, provides the functional reference model for the DSSS.

1. **[Required: Tier0 SS, DSSS]** Needs to handle both H.323 Directory/Gatekeeper functionality and AS-SIP. As well as interworking between the two signaling methods. (This is a transitional requirement until VoSIP becomes all AS-SIP-based e.g., CVVoIP.)

2. **[Required: Tier0 SS, DSSS]** Managed Services. Managed Services is the term used to describe the situation where a limited number of subscribers are served on a remote basis from either an LSC or the LSC function of a Tier0 SS. The subscribers are located in a remote secure enclave and provided secure (encrypted) access to the LSC.

3. **[Required: Tier0 SS, DSSS]** Numbering plan/addressing compatibility with VoSIP, DRSN, Tactical Global Block Numbering Plan (GBNP), SIPRNet IP addressing schema.

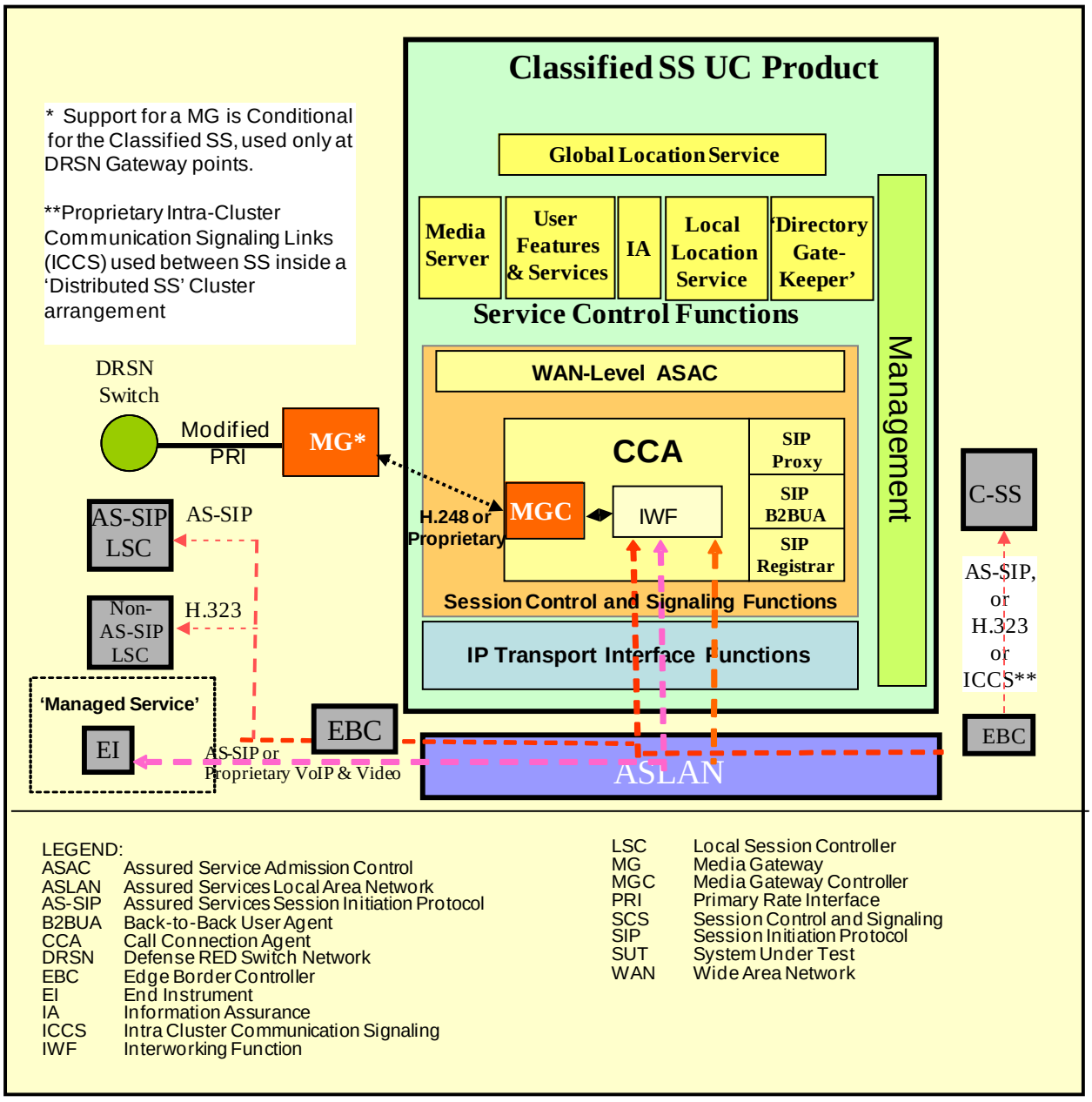

Figure 6.2.6-1. DSSS Reference Model

4. **[Conditional: Tier0 SS, DSSS]** No MFSS TDM capabilities except as noted for the MG function at selected locations.

5. **[Not Required: Tier0 SS, DSSS]** Public safety features (e.g., PSAB, E911 access).

6.2.6.4 Media Gateway with Signaling Interworking

The only MG used in the FY 2008 CVVoIP system is a unique interface between the classified Tier0 SS and a DRSN switching system. This MG performs the following two functions:

- Media conversion
- Signaling conversion

The DRSN "trunk side" uses a modified version of a vendor-unique PRI trunk. The MG performs media conversion between the IP-bearer stream and T1-based media stream. (T1 format is ESF, B8ZS.) In addition, this MG also acts as an "SG" in that it converts the current H.323-based signaling to the DRSN interface trunk signaling (a vendor variant of PRI with two data elements modified to carry the SAL level of the call and precedence level).

For FY 2009, all interfaces to external non-CVVoIP and non-DRSN networks are through DRSN interfaces (e.g., STU-III/R protected access, or encrypted access using KG-xx, KIV-7).

1. **[Required: MG]** Tier0 SS: AS-SIP signaling to DRSN-unique signaling conversion

2. Objective FY 2012 Requirement: AS-SIP signaling and MG via encrypted access to nonsecure (unclassified) networks (such as the DSN, PSTN).

6.2.6.5 Signaling Gateway

Section 5.3.2.13, Signaling Gateway Requirements, defines the SG as an SG exclusively for translating between AS-SIP and SS7 signaling. Since the CVVoIP system does not interface with any SS7-based network, this requirement does not apply to the CVVoIP system.

6.2.6.6 Edge Boundary Controller

All requirements for the EBC specified in Section 5.3.2, Assured Services Requirements, apply to the CVVoIP system.

The following requirement is an additional EBC requirement for the CVVoIP system:

- The EBC must be dedicated to CVVoIP services and not shared with SBU services.

6.2.6.7 Addressing Schema for LSC

The following are all additional requirements unique to the classified LSCs:

1. **[Required: LSC]** DRSN and VoSIP numbering plan capability
2. **[Required: LSC]** Interoperability with Tactical GBNP
3. **[Required: LSC]** SIPRNet IP addressing schema

6.2.6.8 Network Management

All requirements specified in Section 5.3.2.17, Management of Network Appliances, for NM apply to the classified LSC, EBC, and Tier0SS.

The following unique features are required for classified:

1. **[Required: LSC]** The LSC shall generate an alarm message indicating that a secure telephone has been unplugged.

2. **[Required: LSC]** The NM system shall have the capability to mark certain EIs as "high-interest items." This feature is used by network control personnel to analyze failure of specific telephone calls (e.g., 4-star users).

6.2.6.9 Voice Quality

[Required] Because intelligibility of voice communications is critical to C2, the voice service quality rating, on at least 95 percent of the voice sessions, will have a MOS in accordance with the following scenarios:

- Fixed to Fixed – 4.0
- Fixed to Deployable – 3.6
- Deployable to Deployable – 3.2

[Required] The method used for obtaining the MOS shall be in accordance with DISR.

NOTE: The current method used is the E-Model for Fixed-to-Fixed scenarios and P.862 for Deployable scenarios.

The measurement of voice quality shall conform to the requirements found in Section 5.3.2.19.2.1.1, Quality of Service.

6.2.6.10 Call Setup Time

The following call setup times apply to the classified VVoIP network:

1. For LSC intra-enclave calls, the average delay should be no more than 1 second. For the 95 percent of calls, the delay should not exceed 1.5 seconds during normal traffic conditions.

2. For inter-enclave and worldwide calls within the classified environment, average delay should not exceed 6 seconds, with 95 percent of calls not to exceed 8 seconds during normal traffic conditions.

6.2.6.11 Unique Network Infrastructure Requirements for CVVoIP

The following requirements are found under the SBU network infrastructure requirements but are restated here to make the point that they are applicable to the HAIPE environment too. By keeping the Maximum Transmission Unit (MTU) as specified, the addition of encryption will not result in packet fragmentation.

1. **[Conditional]** If the classified Edge system appliance supporting VVoIP uses an Ethernet interface for connecting to the LAN, then its NIC MTU size shall be set to 1280 bytes. NOTE: This will allow for overhead associated with encryptors or VPNs.

2. **[Required]** The DISN Core Network shall be traffic engineered to ensure that VVoIP media E2E completion of sessions above ROUTINE are ensured under the worst-case failure conditions.

   NOTE: This requirement is to ensure that the DISN Core continues to try to find a path for sessions above ROUTINE if a path exists even though the path may be suboptimal (i.e., a satellite connection that does not meet the SLA). NOTE: This requirement assumes the DSCP discriminators exist between ROUTINE and above ROUTINE VVoIP sessions across the encryption boundaries (i.e., HAIPE).

Figure 6.2.6-2, Addition of Encryption within the FY 2009 Network Infrastructure, illustrates where encryption elements fit within the FY 2009 architecture.

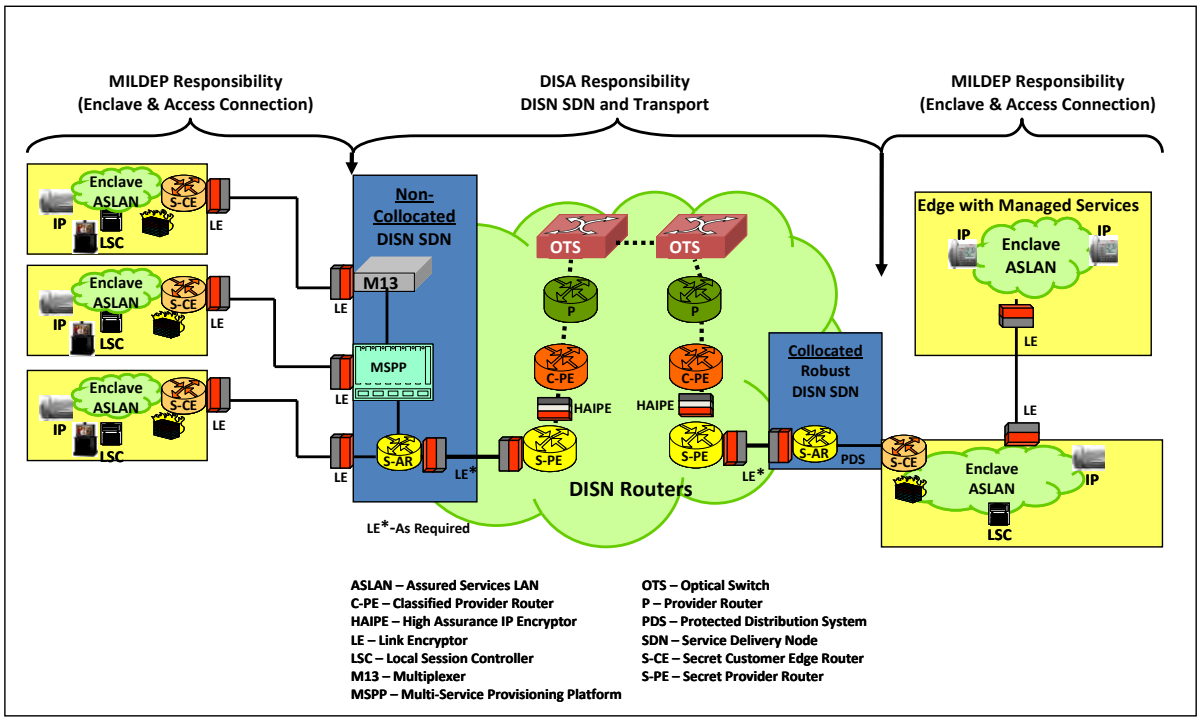

Figure 6.2.6-2. Addition of Encryption within the FY 2009 Network Infrastructure

6.2.6.12 Unique Information Assurance Requirements for CVVoIP

All Information Assurance requirements are specified in Section 5.4, Information Assurance Requirements. In addition, the following requirements are unique to the CVVoIP services:

1. **[Required: EI]** The system shall be capable of being enabled or disabled using enable or disable codes.

   NOTE: An enable code (password or PIN system) is required to restrict access to EIs. Classified EIs must be disconnected or disabled when they are unmanned by appropriately cleared persons or when use of the EI is no longer required. The LSC should not be used to disable the EI based on date/time conditions.

2. **[Required: EI]** If the system supports an enable or disable code, the enable code shall be unique for that facility.

3. **[Required: EI]** If the system supports an enable or disable code, the code shall be able to be modified by an authorized authority.

4. **[Required: EI]** If the system supports an enable or disable code, the system shall have a configurable code aging parameter and the default shall be 90 days.

5. **[Conditional: LSC, EI]** The system shall be capable of using three-factor authentication to include PKI certificates and biometric mechanisms for authenticating user credentials to the LSC via the EI.

   NOTE: The LSC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision due to the immaturity of the current standards. Vendors may choose to implement user authentication using PKI certificates as described in RFCs 3261 or 3893.

6. **[Required: EI]** The system shall be capable of meeting the DoD Public Key Enabled (PKE) requirements for PKI-based authentication.

   NOTE: PKI is required for EIs, whereas in the SBU it is conditional. In summary, the EI is required to support PKI and all the PKI requirements apply.

7. **[Required: Tier0 SS, DSSS, LSC, MG, BC]** The system shall be capable of detecting physical tampering to equipment cabinets and/or devices.

   NOTE: This requirement may be met by using anti-tamper tape and/or tamper-proof screws or locks.

8. **[Required: Tier0 SS, DSSS, LSC, MG, BC]** If the system supports classified users, the system shall be capable of ensuring that all unused network access device connections or physical ports are appropriately secured from unauthorized use by one of the following methods listed in preferential order:

   a. Ports are disabled (i.e., shut down).
   b. Ports are assigned to an unused VLAN, as applicable.
   c. A MAC-based port security is used on active ports.
   d. Port authentication is used by using 802.1X.
   e. A VLAN Management Policy Server (VMPS).

9. **[Required: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console) to include the following events by default, as a minimum:

   a. Invalid user authentication attempt

   b. Unauthorized attempts to access system resources

c. Changes made in a user's security profile and attributes

d. Changes made in security profiles and attributes associated with an interface or port

e. Changes made in access rights associated with resources (i.e., privileges required of a user and an interface or port to access)

f. Changes made in system security configuration

g. Creation and modification of the system resources performed via standard operations and maintenance procedures

h. Disabling a user profile

i. Events associated with privileged users

10. **[Conditional]** If the system contains resources that are deemed mission critical (e.g., a risk analysis classifies it critical), then the system should log any events associated with access to those mission-critical resources.

    a. Successful login attempts

    b. Failed login attempts to include the following:

        (1) Failed logon attempt due to an excessive number of logon attempts
        (2) Failed logon attempt due to blocking or blacklisting of a user ID
        (3) Failed logon attempt due to blocking or blacklisting of a terminal
        (4) Failed logon attempt due to blocking or blacklisting an access port

    c. Logouts
    d. Remote system access

    NOTE: Only the last two items are additions to the CVVoIP (logouts and remote system access).

11. **[Required: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** The security log event record shall be capable of including at least the following information:

    a. Date and time of the event (both start and stop)

    b. User ID including associated terminal, port, network address, or communication device

c. Event type

d. Names of resources accessed

e. Success or failure of the event

f. Origin of the request (e.g., terminal ID)

NOTE: Only the last item is an addition for the CVVoIP (origin of the request).

12. **[Required: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** The system shall be capable of supporting an out-of-band (OOB) or direct connection method for system device management.

13. **[Conditional: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** If the system uses an OOB management method, it shall be capable of using a separate dedicated (closed network).

NOTE: This OOB network must use dedicated infrastructure; however, some portions of its connectivity may be via segregated logical circuits.

14. **[Conditional: R]** If the system uses an OOB management method, the system shall be capable of limiting management connections to authorized source IP addresses.

15. **[Conditional: R]** If the system uses an OOB management method, the system shall be capable of maintaining a separation between the management and production networks.

NOTE: This requires physically separate networks.

16. **[Conditional: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** If the system uses an OOB management method, it shall be capable of ensuring system management access using the following four security restrictions:

a. Role-based authenticated access control
b. Strong two-factor authentication (e.g., Secure ID)
c. Encryption of management and logon sessions
d. Auditing of security-related events

17. **[Conditional: Tier0 SS, DSSS, LSC, MG, BC, R, LS]** If the system uses in-band management, it shall be capable of restricting the sessions to a limited number of authorized IP addresses.

6.2.7 Classified AS-SIP-Unique Requirements

Section 5.3.4, AS-SIP Requirements, provides the complete AS-SIP requirements, including those that apply to classified only. While the AS-SIP requirements for the classified VoIP are almost identical to that of the SBU VoIP, this section addresses the AS-SIP requirements that are unique to the classified VoIP.

6.2.7.1 Classified Signaling Environment

The classified signaling environment is unique in that it will use a mix of existing vendor-based H.323 and AS-SIP signaling during the transition period to all DISN CVVoIP. In addition, a unique MG capability exists as part of a Tier0 SS.

The signaling design during the transition period has to provide both backward and forward technology capabilities. Thus, CAS and PRI in the DRSN has to interoperate with H.323 signaling in the VoSIP Pilot to be followed by H.323 and AS-SIP interoperating in the CVVoIP system until all IP services are via AS-SIP. Once that is achieved, the DRSN interoperability must be maintained until its features can be replicated with IP technologies.

The signaling design is described in Section 6.2.5.1, FY 2008 Signaling Design. The design is also depicted in Figure 6.2.7-1, DISN CVVoIP FY 2009 Signaling Design.

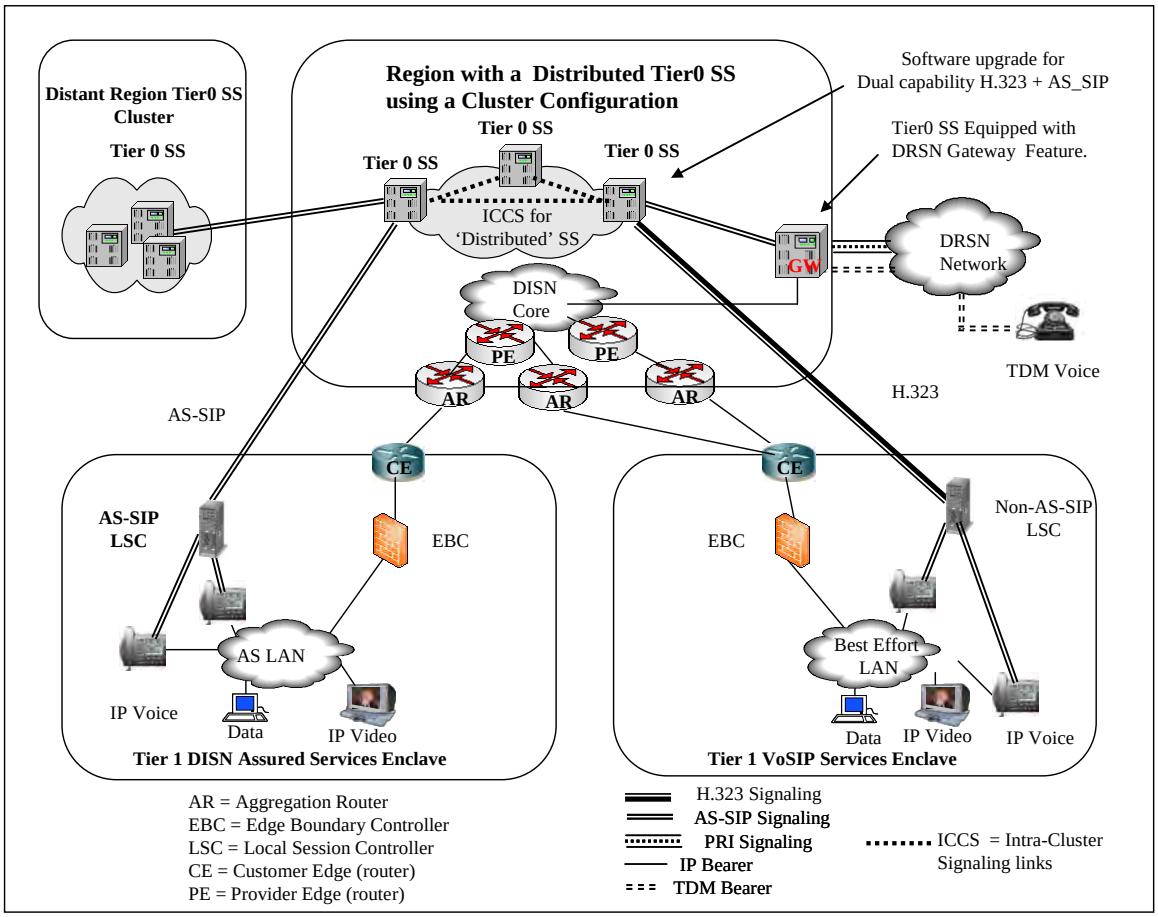

Figure 6.2.7-1. DISN CVVoIP FY 2009 Signaling Design

To simplify the signaling path description, the term Tier0 SS from here on refers to a geographic clustered Tier0 SS. (Please note that during a transition period, H.323 and AS-SIP will coexist at certain locations.) All session (call) signaling messages received by an LSC from local EIs and intended for a destination outside the secure service enclave is sent by the LSC in the form of an AS-SIP message to its assigned Tier0 SS. The Tier0 SS then forwards the AS-SIP message to the distant end by either forwarding the message directly to the distant-end LSC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end LSC. Similarly, all session (call) signaling messages sent from a remote location and intended for IP EIs associated with a given LSC will be routed to the Tier0 SS assigned to the destination LSC and the Tier0 SS will forward the AS-SIP signaling messages to the destination LSC.

6.2.7.1.1 IP Signaling Path Reference Cases

Based on the top-level signaling design depicted in Section 6.2.7.1, Classified Signaling Environment, the signaling paths that must be supported to provide the classified VVoIP services

are identified in Figure 6.2.7-2, IP Signaling Path Reference Illustration, and Table 6.2.7-1, Reference Case: IP-to-IP Calls over an IP Backbone.

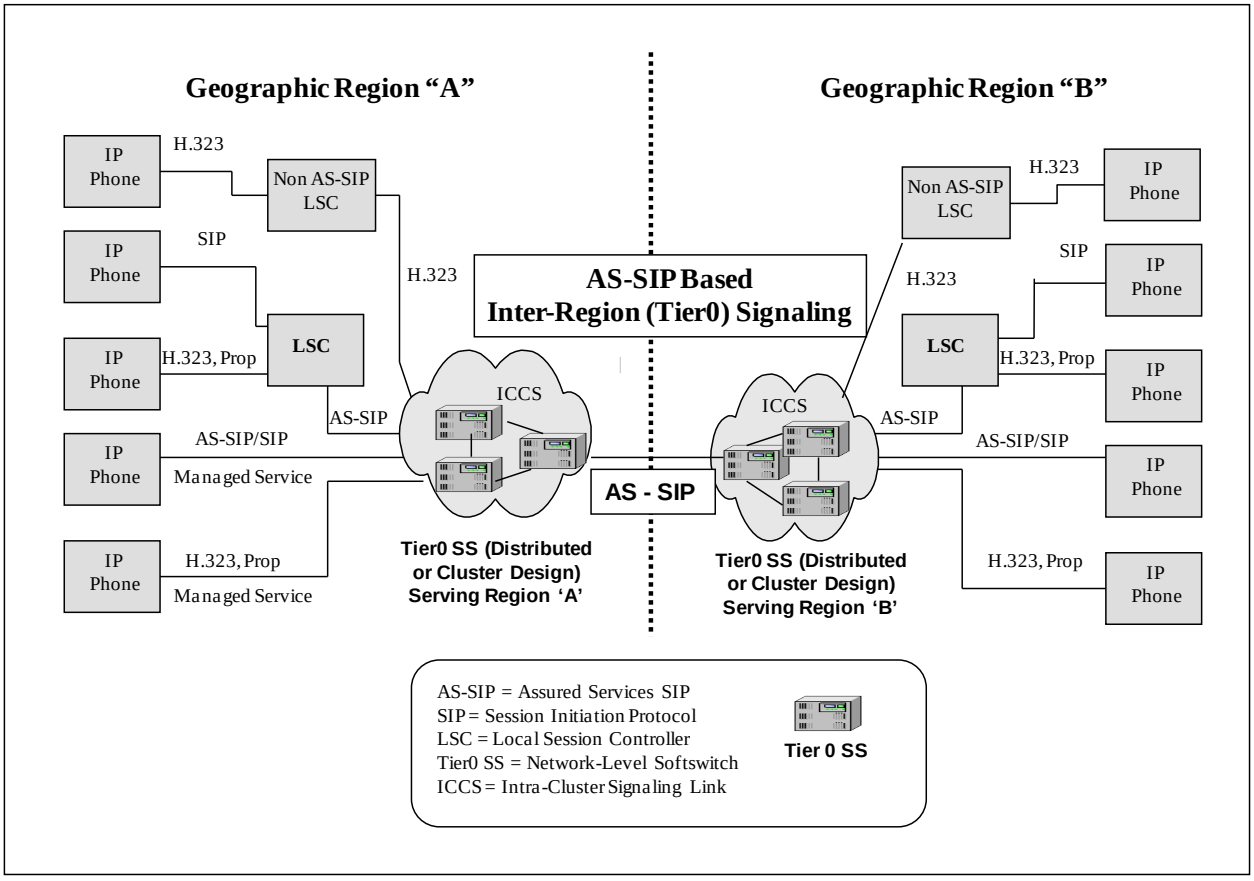

Figure 6.2.7-2. IP Signaling Path Reference Illustration

Table 6.2.7-1. Reference Case: IP-to-IP Calls over an IP Backbone

Ref. Case	Originator Phone	Originator Signaling	Network Signaling and Call Path							Terminator Signaling	Terminator Phone
1A	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1B	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1C	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1D	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1E	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1F	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1G	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1H	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1I	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1J	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1K	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1L	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1M	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	SIP	IP phone
1N	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	LSC	H323, Prop.	IP phone
1O	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1P	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone

Ref. Case	Originator Phone	Originator Signaling	Network Signaling and Call Path							Terminator Signaling	Terminator Phone
2A	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	SIP	IP phone
2B	IP phone	SIP	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2C	IP phone	SIP	LSC	AS-SIP	Tier0 SS					SIP	IP phone
2D	IP phone	SIP	LSC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2E	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	SIP	IP phone
2F	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2G	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS					SIP	IP phone
2H	IP phone	H323, Prop.	LSC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2I	IP phone	SIP			Tier0 SS	AS-SIP			LSC	SIP	IP phone
2J	IP phone	SIP			Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2K	IP phone	SIP			Tier0 SS					SIP	IP phone
2L	IP phone	SIP			Tier0 SS					H323, Prop.	IP phone
2M	IP phone	H323, Prop.			Tier0 SS	AS-SIP			LSC	SIP	IP phone
2N	IP phone	H323, Prop.			Tier0 SS	AS-SIP			LSC	H323, Prop.	IP phone
2O	IP phone	H323, Prop.			Tier0 SS					SIP	IP phone
2P	IP phone	H323, Prop.			Tier0 SS					H323, Prop.	IP phone

6.2.7.2 Differences Between SBU and Classified AS-SIP Requirements

Section 5.3.4, AS-SIP Requirements, defines both SBU and classified requirements. The classified-specific requirements are defined in Requirements 5.3.4.7.3.1.13 through 5.3.4.7.3.1.22; (Route Header Requirements); Requirement 5.3.4.7.3.2.1, (Proxy Require), Requirement 5.3.4.7.4.1.11, (418 response); Requirements 5.3.4.7.5b.1 through 5.3.4.7.5b.13 (SIP Preconditions); Requirements 5.3.4.7.9.1 through 5.3.4.7.9.11 (CAL Requirements); and Requirements 5.3.4.10.2.1.2.5 through 5.3.4.10.2.1.2.8 (Precedence Levels). In addition, sections specifying "domain name," "namespace," and/or domain subfields define "uc" as **Required** for the SBU environment, and "cuc" as **Required** for the classified environment.

The following sections describe additional differences between the SBU and classified AS-SIP requirements.

6.2.7.2.1 Nomenclature

The classified environment uses the term Tier0 SS (Tier0 SS) while Section 5.3.4, AS-SIP Requirements, uses the term SS to denote the SBU environment.

The classified environment uses "cuc" as the network domain name, while the SBU environment uses "uc" as the network domain name.

NOTE: Reference cases 2A through 2P (see Table 6.2.7-1, Reference Case: IP-to-IP Calls over an IP Backbone) represent the call paths when the same Tier0 SS serves both the calling party calling party's LSC (or the calling party's EI directly) and the called party's LSC (or the called party's EI directly). Reference cases are not shown for non-AS-SIP LSCs.

6.2.7.2.2 Route Header Requirements

The Route Header requirements for LSCs and SSs are predicated on the SBU network architecture in which EBCs are required at each enclave having at least one AS-SIP signaling appliance.

The current VoSIP architecture does not use EBCs; therefore, it is anticipated that during the transition toward full implementation of AS-SIP within the classified network there will be instances where EBCs may or may not be present at all locations encountered on an E2E AS-SIP call. Therefore, the classified requirements must include specifications for the various permutations of Route headers for the situations where an EBC is present at a Tier0 SS or at an LSC, or at both. If there is not an EBC at either location and there are no intermediary AS-SIP signaling appliances between an LSC and its Tier0 SS, then there may not be a need for a Route header. (See Requirements 5.3.4.7.3.1.13 through 5.3.4.7.3.1.22)

6.2.7.2.3 Proxy Require

In adherence with the enumerated RFCs, the AS-SIP EIs MUST be capable of generating, receiving, and processing SIP header fields as defined in Requirement 5.3.4.7.3.2.1:
The "Proxy-Require" must be generated for the classified network only.

6.2.7.2.4 418 Response

Requirement 5.3.4.7.4.1.11 states (NOTE: This paragraph applies to classified only.), "The LSCs MUST support the generating of a 418 (Incompatible CAL) response code upon receipt of an INVITE that cannot be resolved to a valid CAL. The 418 response SHOULD contain the CAL header with the reflected-access-level set to the last successfully resolved value in the request path. The local-access-level SHOULD be set to the access-level supported by the destination UAS or to the access-level supported for the routing domain that failed resolution at an intermediate Tier0 SS."

6.2.7.2.5 SIP Preconditions

Requirements 5.3.4.7.5b.1 through 5.3.4.7.5b.13 state that implementation of preconditions is conditional for the classified network. [RFC 3312]

6.2.7.2.6 CAL Requirements

Requirements 5.3.4.7.9.1 through 5.3.4.7.9.11 define CAL requirements. The purpose of the CAL header is to convey the classification level for a telephony or video session between the parties to the session.

6.2.7.2.7 Precedence Levels

Requirements 5.3.4.10.2.1.2.5 through 5.3.4.10.2.1.2.8 define precedence level requirements for the classified network. The classified adds a FLASH OVERRIDE-OVERRIDE (FOO) precedence level.

6.2.7.2.8 SIP URI Mapping of Telephone Number

Section 5.3.4.7.6, SIP URI and Mapping of Telephone Number into SIP URI, describes the SIP URI and telephone number mapping requirements. The following modifications apply to the classified version of AS-SIP:

1. Instead of uc.mil, use cuc.mil in the host name for classified SIP URIs.

2. Instead of uc.mil, use cuc.mil with the phone-context parameter.

3. The SBU Requirements 5.3.4.7.6.4 and 5.3.4.7.6.5 apply to interworking of phone numbers on the PSTN is conditional in the classified specification.

4. The 3-digit 911 and 411 numbers are conditional in the classified specification. There is no current requirement to support access to 911 services in the classified network.

6.2.7.2.9 64 kbps Transparent Calls (Clear Channel)

There are no requirements for clear channel service within the classified environment; therefore, the SBU AS-SIP requirements defined in UCR 2008, Section 5.3.4.7.7, 64kbps Transparent Calls (Clear Channel), do not apply.

6.2.7.2.10 Transport of Route Code Information over AS-SIP

There are no requirements for transport of route codes (used for hotline service) within the classified environment; therefore, the SBU AS-SIP requirements defined in UCR 2008, Section 5.3.4.7.8, Transport of Route Code Information over AS-SIP, do not apply.

6.2.7.2.11 Classified VoIP Information Signals

Table 5.3.4.10-4, UC Information Signals (from Section 5.3.4, AS-SIP Requirements), has been expanded for the classified environment to include secure dial tone, line busy tone, and reorder tone requirements as outlined in DRSN documentation. Table 6.2.7-2, CVVoIP Information Signals, is the expanded version.

Table 6.2.7-2. CVVoIP Information Signals

SIGNAL	FREQUENCIES (HZ)	SINGLE TONE LEVEL	COMPOSITE LEVEL	INTERRUPT RATE	TONE ON	TONE OFF
Secure Dial Tone	350 + 440 (Mixed)	-13 dBm0	-10 dBm0	Continuous		
Line Busy Tone	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	60 IPM	0.5 sec	0.5 sec
Reorder Tone (No circuit)	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	120 IPM	0.2 sec	0.3 sec
Audible Ringback (Routine Call)	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	10 IPM	2.0 sec	4.0 sec
Audible Ringback Precedence Call	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	30 IPM	1640 ms	360 ms
Alerting (Ring) Signal Routine	-	-	-	10 IPM	2.0 sec	4.0 sec
Alerting (Ring) Signal Precedence				30 IPM	1640 ms	360 ms
Preemption Tone	440 + 620 (Mixed)	-19 dBm0	-16 dBmo	Continuous	Steady on	
Call Waiting (Precedence Call)	440	-13 dBm0		Continuous at 6 IPM	100 ± 20 ms Three Bursts	9700 ms
Conference Disconnect Tone	852 and 1336 (Alternated at 100 ms Intervals)	-24 dBm0		Steady on	2000 ms (per occurrence)	
Override Tone	440			Continuous at 6 IPM	2000 ms (followed by) 500 ms on and 7500 ms off	
Camp On	440	-13 dBm0			Single burst 0.75 to 1 second	

6.2.7.2.12 Policing of Call Count Thresholds

Section 5.3.4.11, Policing of Call Count Thresholds, defines the requirements for policing of call count thresholds. The following augmentations to the AS-SIP requirements apply for classified:

FLASH-OVERRIDE-OVERRIDE is added to requirements that describe policing for precedence levels beginning with FLASH.

6.2.8 DRSN Switches and Peripheral Devices

Requirements for DRSN switches and peripheral devices are not included in UCR 2008. Specifications for these products are available on a need-to-know basis from the DISA NS DRSN Single Service Manager.

6.2.9 Physical Construction Unique Requirements

Physical construction requirements for classified elements within a secure enclave must adhere to current requirements for:

1. Cabling: All cabling must follow PDS guidelines.

2. Cabling or interfaces leaving a secure enclave must be encrypted.

3. Equipment must comply with TEMPEST requirements.

6.2.10 UC Secure Preset Conference

This section provides a description of requirements that will enable SBU voice subscribers equipped with an NSA Type 1 encryption device to conference in the secure mode.

6.2.10.1 Introduction

The DoD voice communications within the UC (i.e., VoSIP, VVoIP, DSN) is challenged with the need to communicate in a secure mode with multiple subscribers and to communicate transparently with other DoD secure voice networks.

The DoD SBU voice network is the DSN that is a part of the DoD Unified Communications. The DSN provides the capability for SBU communications between its subscribers as a standard feature. The DSN also provides the capability for unique subscribers to communicate in a secure mode using various encryption devices. The UC SBU voice currently is not equipped with the capability for any subscriber type to communicate simultaneously with multiple subscribers on a secure mode either on a preset or meet-me basis, and, it is not equipped to communicate transparently with other secure networks (i.e., VoSIP, DRSN).

The DoD established the need for the UC SBU voice subscribers to communicate with multiple subscribers in a secure mode that will enhance the current UC SBU voice subscriber feature that allows voice communications beyond the SBU classification based on the NSA accreditation level of the device used for the UC SBU voice session.

Current capabilities of the UC SBU voice for subscriber communications with multiple subscribers will have to be expanded to implement a secure mode feature of the existing capabilities. This section describes and outlines the necessary enhancements needed to comply with the DoD mandate for UC SBU voice secure communications that will allow communications above the SBU classification.

6.2.10.2 Feature Requirements

A UC SBU voice secure interface(s) will provide the capability for UC SBU voice subscribers equipped with an NSA Type I encryption device to communicate

- In the secure mode with multiple subscribers who are equipped with interoperable NSA devices on a preset DN assigned to the originator to initiate the session;

- With multiple subscribers equipped with interoperable NSA devices on a "meet-me" basis; and

- To another network subscriber that uses interoperable NSA devices.

To reduce the risk of new development for such a feature, it is recommended that such an interface operates at the 56 kbps rate via a standard Telcordia Technologies GR-506-CORE 2W loop and that optional interface(s) can use a single DS0 off an ISDN PRI also, using the ANSI T1.619a protocol. The interface is fully automated and transparent to the subscriber and meets the DoD standards for secure communications that use NSA Type I devices.

The following description expands the current UCR requirements for conferencing and adds the UC SBU Voice Secure Gateway Interface. The conferencing features are expanded to include a "SECURE" environment for the UC SBU voice subscribers who are equipped with an NSA Type I encryption device to conduct a secure preset conference session and to conduct a "random" secure conference session using the "meet-me" conference bridge.

The UC SBU Voice Secure Gateway allows for a UC SBU voice subscriber equipped with an NSA Type I encryption device to communicate with a secure system subscriber equipped with the compatible encryption device provided that the secure system has a direct DS0 or DS1 (PRI) interface. These additional features provide the means for the current UC SBU voice subscribers who are equipped with an NSA Type I encryption device to conduct secure sessions up to the classification allowed by the NSA Type I encryption device.

The current secure interface for typical applications is depicted in Figure 6.2.10-1, Examples of Current Secure Interface Arrangements, and Figure 6.2.10-2, Additional Examples of Current Secure Interface Arrangements. These interfaces are not vendor unique and are shown as typical

implementations of these requirements, and are not intended to be the only implementation that satisfies the requirements.

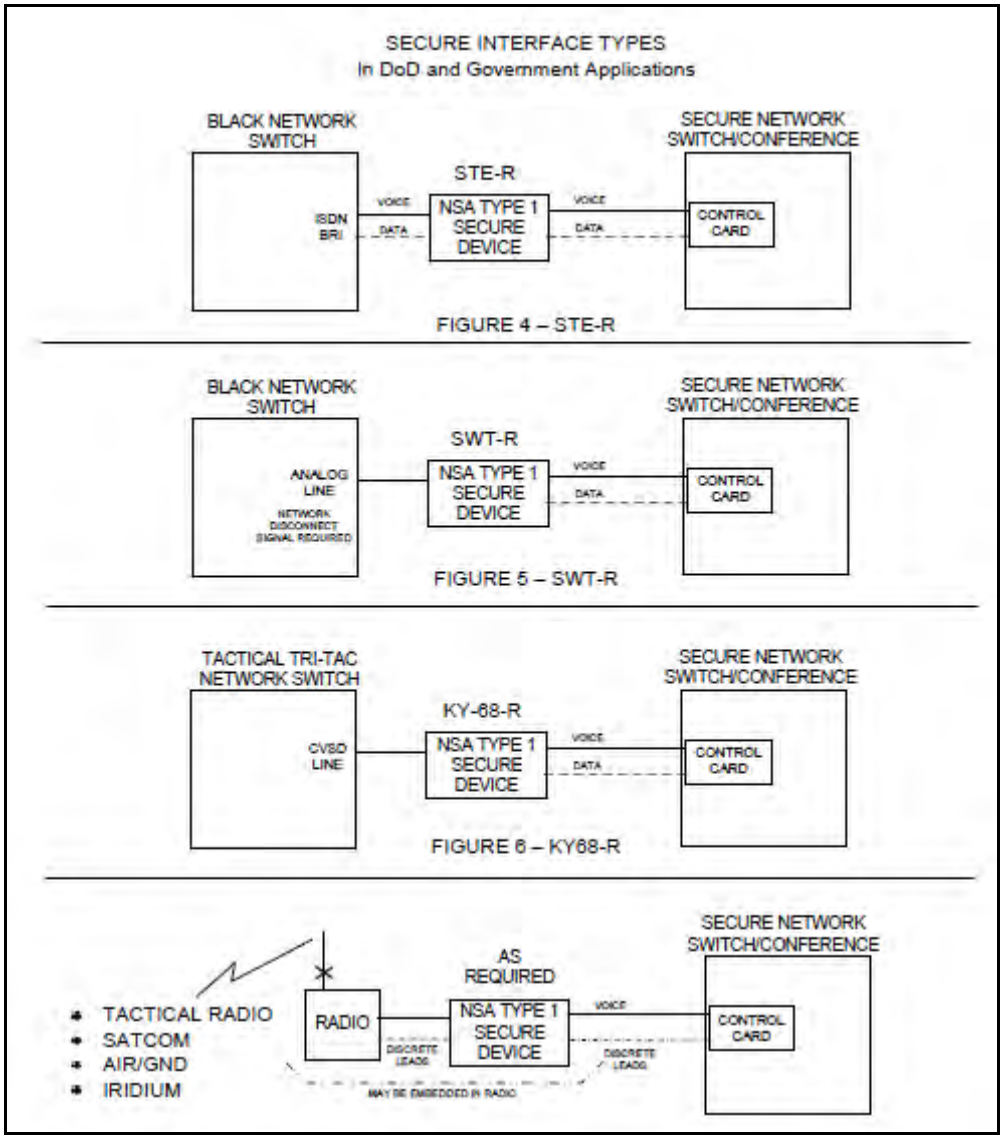

Figure 6.2.10-1. Examples of Current Secure Interface Arrangements

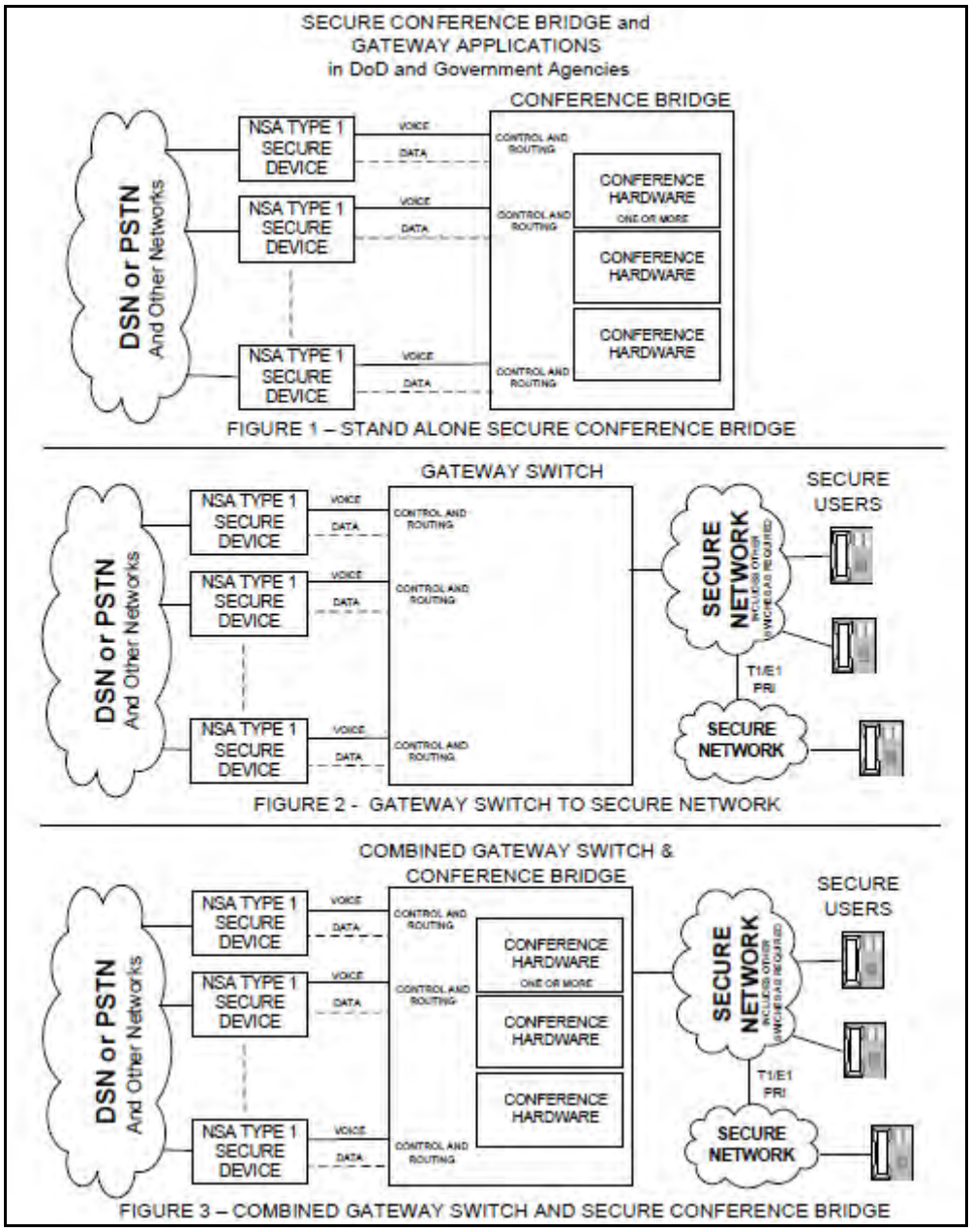

Figure 6.2.10-2. Additional Examples of Current Secure Interface Arrangements

6.2.10.3 UC SBU Voice Secure Conference Features

(Features listed here are additional to the features listed in UCR 2008, Section 5.2.)

(Network system interface with secure preset and meet-me conference bridges that allows UC SBU voice users with NSA Type I encryption device to originate or participate in conference sessions across the UC voice multi-networks.)

6.2.10.3.1 Feature Description

The secure conference bridge system (preset or meet-me) is equipped with individual ports with automated supervision and control interfaces that conforms to standard telephony two-wire loop (DS0 minimum rate of 56 kbps) (in accordance with Telcordia Technologies GR-506-CORE) and is equipped with an automated "ON-HOOK" and "OFF-HOOK" type function and can be any one of the specified GR-506 two-wire signaling types. The port interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling, specified in Telcordia Technologies GR-506-CORE, for DTMF for originating a call. Call origination can be from the conferee participant port only of the preset bridge. Meet-me bridge ports do not have an originating feature. Calls that are originated to or from the preset bridge are always secure via control and supervision of the NSA Type I encryption device used. Calls terminating to a meet-me bridge port are equipped with an NSA Type I encryption device that ensures only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through into the bridge.

Preset and meet-me bridges are equipped with an optional ISDN DS1 interface user-network interface in which the interface structure is composed of multiple B channels and one D channel. The bit rate of the D channel in this structure is 64 kbps. When a 1544-kbps PRI is provided, the interface structure is 23B+1D.

Requirements for this feature shall be in accordance with Telcordia Technologies SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268. The UC SBU voice user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.

The PRI provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk-path of the session.

6.2.10.4 UC Preset Conference Bridge Requirements

In addition to the requirements stated in UCR 2008, Section 5.2.1.6.1 inclusive, the bridge shall provide the following capabilities: (See the notional diagram in Figure 6.2.10-3, Secure Preset Conference Capability.)

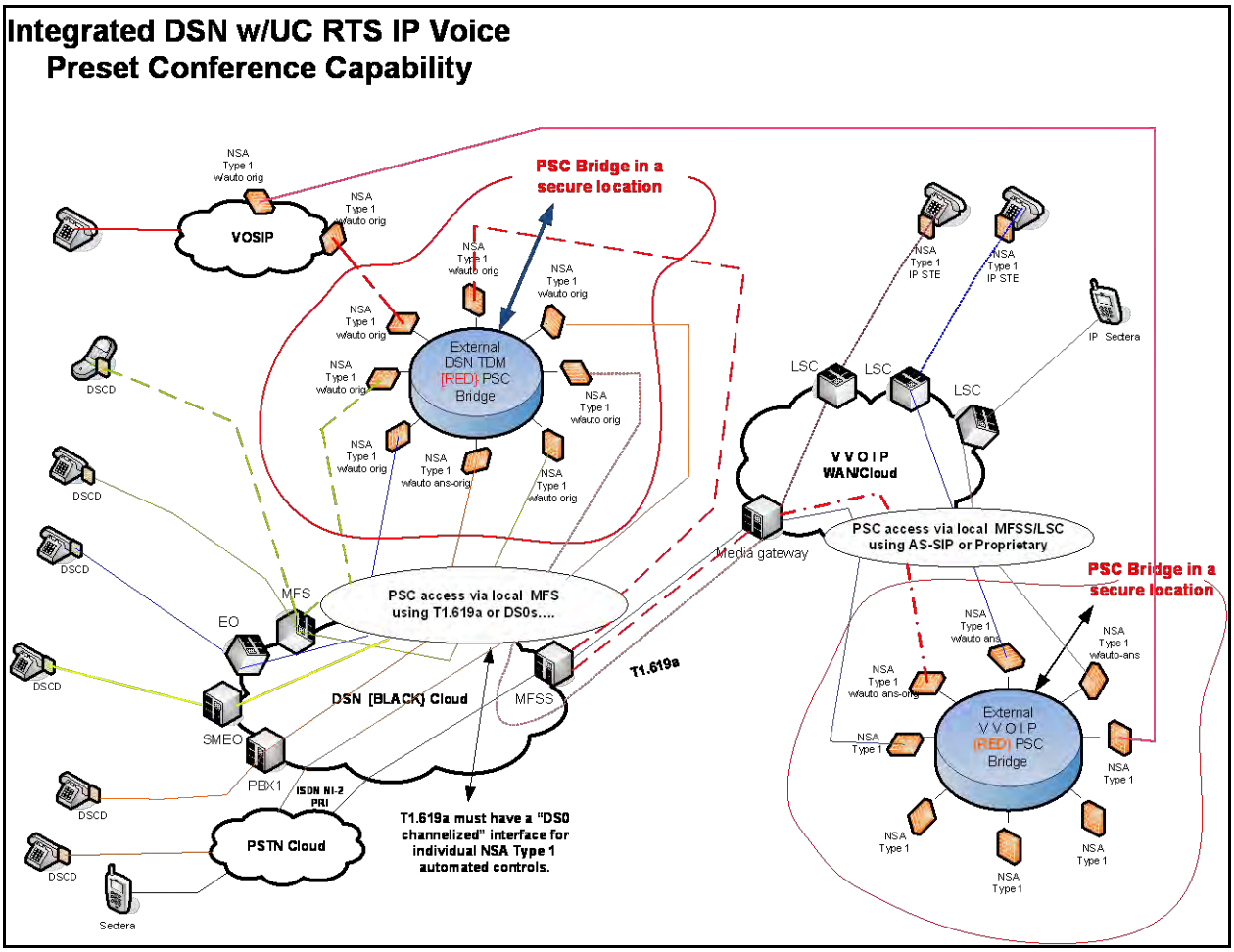

Figure 6.2.10-3. Secure Preset Conference Capability

1. All bridge port access shall be via an NSA Type 1 approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports in accordance with the features listed in this document (i.e., VoSIP, VVoIP, Tactical WAN access must be via the NSA-compatible device).

2. Each bridge shall be equipped with a unique preset conference originator port (i.e., the port that starts the conference) and preset conference participant ports (i.e., the ports that dial the DN of the participant) that establish a conference up to the maximum number of participants as specified previously.

3. The bridge shall be programmable to establish an originating preset conference based on the conference ID that accessed the conference originating port of the bridge.

4. Conference ID shall be based on the originator's calling ID and the originator's dialed code.

5. A conference dialed code shall be able to establish a preset conference consisting of the maximum number of participants (see UCR 2008, Section 5.2.1.6.1, inclusive) and shall use multiple bridge ports when required for the conference.

6. Conference bridge ports shall be limited to the maximum number of participants (see UCR 2008, Section 5.2.1.6.1, inclusive) based on the number of cascaded bridges required to connect the required quantity of participants.

7. The bridge shall provide a feature for the conference originator to selectively release (terminate) a participant. Such a feature must be interoperable with bridges that are cascaded.

8. The bridge shall provide a feature for the conference originator to selectively recall a participant. Such a feature must be interoperable across bridges that are cascaded.

9. The bridge shall provide a feature for the conference originator to selectively add-on a participant. Such a feature must be interoperable with bridges that are cascaded.

10. The bridge shall provide a feature for the conference originator (when the originator is equipped with an alphanumeric display) to be informed of a participant's status (i.e., answer, disconnect). Such a feature must be interoperable with bridges that are cascaded.

11. The bridge shall be programmable for a minimum of a 100 preset conference dialed codes.

12. Bridge ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive) specifications that allows for remote/distant access to the bridge.

13. Bridge ports (conference originator and participant) shall be via DS0 allocations that may be via a T1.619a DS1 interface.

14. Each DS0 port access (originating and terminating) to the bridge shall be encrypted via an NSA Type 1 device.

15. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type 1 encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control can be either before the actual bridge DS0 port interface to the DSN switch port or after the DS0 port interface to the bridge itself) that will permit the NSA Type 1 encryption device to encrypt the two-way conversation and allow the cut-through of the DS0 port into the bridge when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.

16. Each bridge DS0 port interface can only be activated and put in-service when it is connected serially with a NSA Type 1 encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

6.2.10.5 UC Secure Meet-Me Conference Bridge Requirements

In addition to the requirements stated in UCR 2008, Section 5.2.1.6.1 inclusive, the bridge shall have the following capabilities (see Figure 6.2.10-4 for a notional diagram):

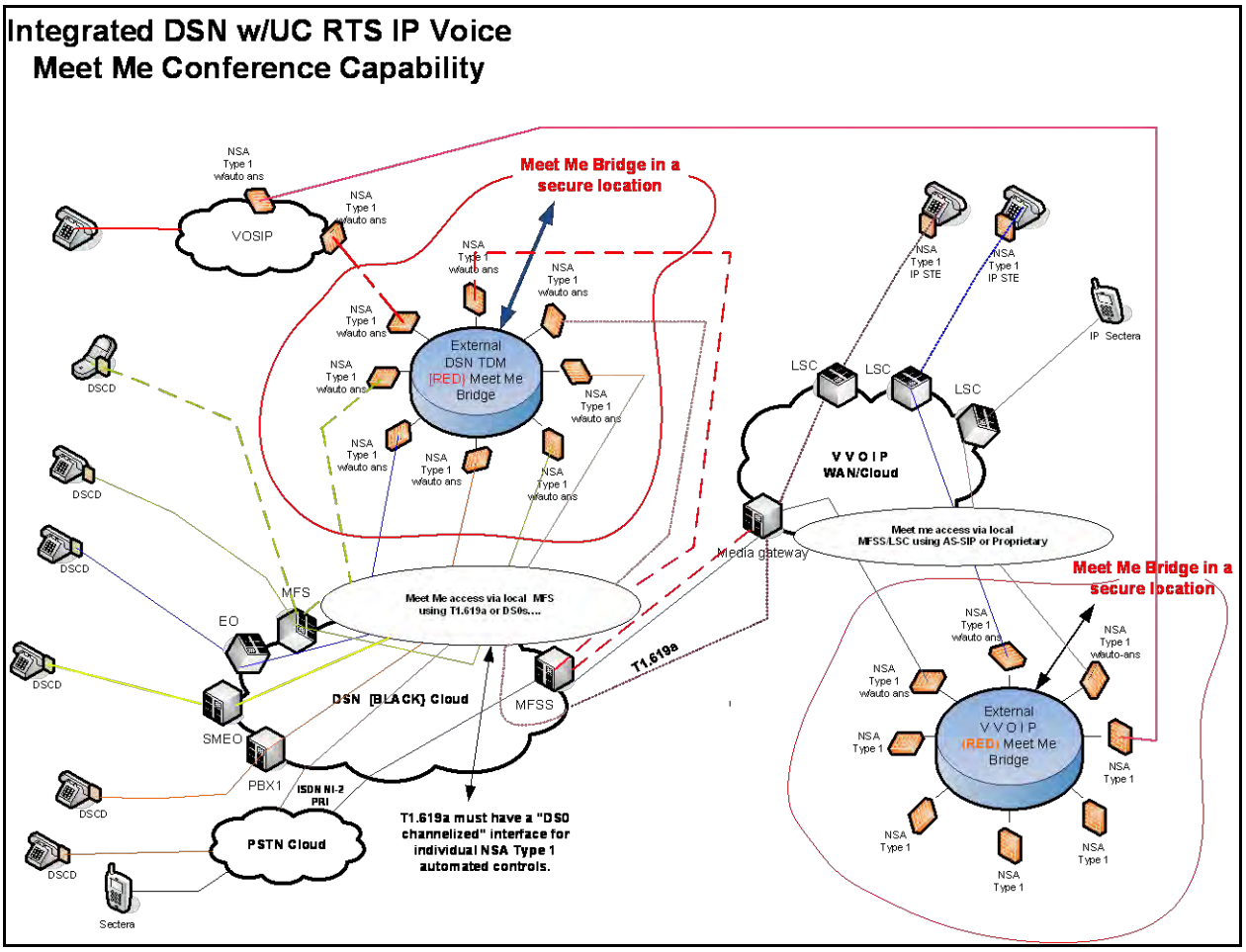

Figure 6.2.10-4. Secure Meet-Me Conference Arrangement

1. All bridge port access shall be via an NSA Type 1 approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports IAW the features listed in this document (i.e., VoSIP, VVoIP, and Deployed WAN access must be via the NSA-compatible device).

2. Bridge ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive) specifications that allows for remote/distant access to the bridge.

3. Each bridge shall be programmable to a specific number of participants.

4. Each bridge shall be configurable to cascade with other bridge(s) to expand the number of participants up to 100 participants. Cascading of bridges shall be via a NSA Type 1 encryption device.

5. Each bridge port access shall be assigned a unique DSN DN.

6. Each port access (originating and terminating) to the bridge shall be encrypted via an NSA Type 1 device.

7. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type 1 encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control can be either before the actual bridge DS0 port interface to the DSN switch port or after the DS0 port interface to the bridge itself) that will permit the NSA Type 1 encryption device to encrypt the two-way conversation and allow the cut-through of the DS0 port into the bridge when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.

8. Each bridge DS0 port interface can only be activated and put in-service when it is connected serially with an NSA Type 1 encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

6.2.10.6 UC Secure Network Gateway Requirements

(Network system interface that allows secure sessions across the UC multi-networks that are equipped with NSA Type I encryption devices.)

6.2.10.6.1 Feature Description

The gateway provides for UC SBU access to a secure classified system at the DS0 (minimum bit rate of 56 kbps) or DS1 (PRI) bit rate using NSA Type I encryption devices. The DS0 interface uses a standard telephony 2-wire loop (IAW Telcordia Technologies GR-506-CORE) equipped with automated "ON-HOOK" and "OFF-HOOK" type function, and can be any one of the specified Telcordia Technologies GR-506-CORE two-wire signaling types. The DS1 interface uses an NI-2 PRI T1.619a protocol that uses "channelized DS0" NSA Type I encryption devices and is equipped with an automated D channel-type signaling interface that controls the cut-through of the selected DS0 channel/session.

The DS0 interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call. Call origination can be from either input of the interface. Calls

that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk path of the session.

The DS1 interface is an ISDN primary access interface and is an ISDN user-network interface in which the interface structure is composed of multiple B channels and one D channel. The bit rate of the D channel in this structure is 64 kbps. When a 1544-kbps PRI is provided, the interface structure is 23B+1D.

Requirements for this feature shall be in accordance with Telcordia Technologies SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.

The PRI interface provides for automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway are always secure via control and supervision of the NSA Type I encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk path of the session.

The UC Network Gateway shall have the following capabilities (see Figure 6.2.10-5, Notional Diagram Illustrating Secure Network Gateway, for a notional diagram):

1. All gateway interface port access shall be via an NSA Type 1 approved device that interoperates with the caller or called party's NSA-compatible device for encryption and supervisory control of the bridge ports IAW the features listed in this document (i.e., VoSIP, VVoIP, Tactical WAN access must be via the NSA-compatible device).

2. Each network secure gateway DS0 port (originating and terminating ports) shall interface with an NSA Type 1 encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control can be either before the actual gateway DS0 port interface to the DSN switch port or after the DS0 port interface to the gateway itself) that will permit the NSA Type 1 encryption device to encrypt the two-way conversation and allow the cut-through of the DS0 port into the gateway when the NSA device acknowledges and confirms that the connected line is cryptographically synchronized.

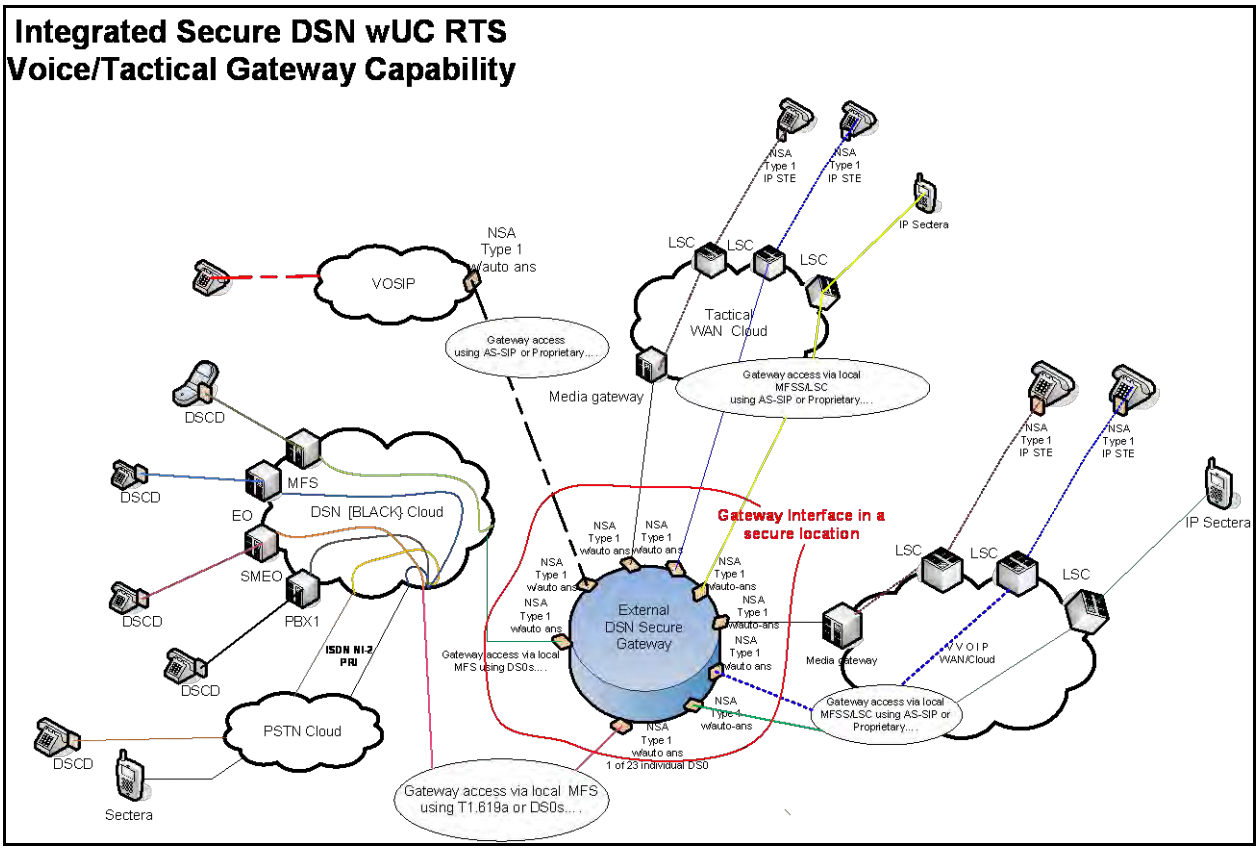

Figure 6.2.10-5. Notional Diagram Illustrating Secure Network Gateway

3. The gateway interface shall operate at the DS0 (minimum bit rate of 56 kbps) or DS1 (PRI) bit rate using NSA Type I encryption devices.

4. The DS0 interface shall comply with the standard telephony two-wire loop IAW Telcordia Technologies GR-506-CORE, GR-513-CORE, GR-1089-CORE, and ANSI T1.401-1993, and shall be equipped with an automated "ON-HOOK" and "OFF-HOOK" type function and can be any one of the specified GR-506-CORE two-wire signaling types.

5. Each DSN outgoing gateway interface shall be equipped with a unique DSN DN where the DN can provide a single port or multiple port access to the gateway device/system.

6. Each gateway port interface shall be equipped with the capability to provide automated supervision and control of the DSN outgoing connection that is interfaced with an NSA Type I encryption device. Such a control shall only allow cut-through of the session when the NSA Type I encryption device is cryptographically synchronized with the DSN's originator NSA Type I device.

7. Each gateway port interface shall be equipped with the capability to provide automated supervision and control of the non-DSN incoming connection to the DSN switch that is

interfaced with an NSA Type I encryption device. Such a control shall only allow cut-through of the session when the NSA Type I encryption device is cryptographically synchronized with the DSN's terminator NSA Type I device.

8. Gateway ports shall comply with Telcordia Technologies GR-507-CORE, Section 7.5 (inclusive) specifications that allows for remote/distant access to the gateway.

9. Gateway ports (originator and terminator) shall be via DS0 allocations that may be via a T1.619a DS1 interface.

10. Each DS0 port access (originating and terminating) to the gateway that uses a T1.619a interface shall be encrypted via an NSA Type 1 device.

11. The DS1 interface shall be an ISDN primary access interface and is an ISDN user-network interface in which the interface structure is composed of multiple B channels and one D channel. The bit rate of the D channel in this structure is 64 kbps. When a 1544-kbps PRI is provided, the interface structure is 23B+1D. Requirements for this feature shall be in accordance with Telcordia Technologies SR-NWT-002120, SR-NWT-002343, and TR-NWT-001268. The DSN user-to-network signaling physical layer specification for the PRI operating at 1.544 Mbps shall be ANSI T1.408 and ANSI T1.619a.

12. The PRI interface shall provide an automated supervision and control of the incoming and outgoing signaling that conforms to the line signaling specified in Telcordia Technologies GR-506-CORE for DTMF for originating a call via the control of the selected D channel of the PRI. Call origination can be from either input of the interface. Calls that are originated to or from the gateway shall be "secure" via control and supervision of the NSA Type I encryption device used. The NSA Type I PRI channelized encryption device ensures that only encrypted sessions will be able to communicate, and non-encrypted sessions are not allowed to be cut-through on the talk path of the session.

13. Each gateway DS0 port interface can only be activated and put in-service when it is connected serially with an NSA Type 1 encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

SECTION 7
REQUIREMENTS SUMMARY

7.1 REQUIREMENTS SYNOPSIS

Section 7, Requirements Summary, provides a summary of where requirements for the various UC products are described in UCR 2008.

7.1.1 Overview of Approved Products

The UCR covers six categories of approved products as follows:

1. The SBU UC products for IP E2E systems that support SBU voice and video services.

2. Applicable to UCR 2008 only: Circuit-switched products with IP on the line side only that support SBU voice and video services.

3. Classified UC products for IP E2E systems that support classified voice and video services.

4. Network infrastructure products (e.g., DISN SDN/MILDEP Intranet and terrestrial transport components products). The ASLAN products, which are Access, Distribution, and Core devices, are a subset of the network infrastructure products.

5. Deployed products.

6. Encryption products.

Instant Messaging and Chat Collaboration UCs are not considered to be stand-alone UC products; these are applications that create the possibility of real-time text-based communication between two or more participants over the network infrastructure. General requirements for IM and Chat Collaboration applications are described in Section 5.7, Presence/Awareness, Instant Messaging, and Chat Requirements. These UC features are included in the SBU UC products for IP E2E systems that support SBU voice and video services; classified UC products for IP E2E systems that support SBU voice and video services; and in Tactical products.

Figure 7-1, Overview of UC Product Categories within the DoD UC APL, provides an overview of the structure of the DoD UC APL in terms of services and network infrastructure. The various UC products for each of the six UC product categories are found under their appropriate section of the UC APL. Many UC products, however, show up under multiple UC product categories since they can be used under multiple categories. Examples include the LSCs, CE Routers, EBCs, and ASLANs, which can be used for both SBU and Classified voice and video services.

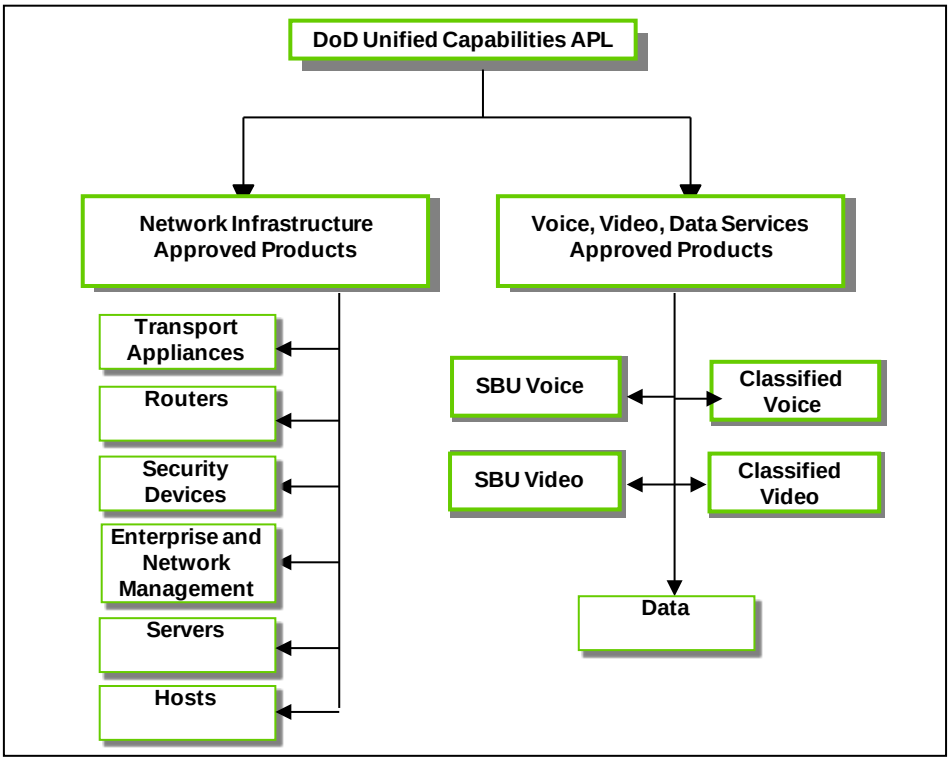

Figure 7-1. Overview of UC Product Categories within the DoD UC APL

7.1.2 SBU UC Products for E2E Systems that Support SBU Voice and Video Services

Table 7-1, IP-Based UC products that Support SBU Voice and Video Services, delineates the UCR 2008 sections where requirements for these products are found.

Table 7-1. IP-Based UC Products that Support SBU Voice and Video Services

PRODUCT AND APPLIANCE FUNCTION		GENERAL REQUIREMENTS	INFORMATION ASSURANCE REQUIREMENTS	IPV6	SIGNALING TYPE	
PRODUCT	APPLIANCE				AS-SIP	TDM
MFSS	TDM Side	5.2	5.4	5.3.5		5.2
	SS Side	5.3.2	5.4	5.3.5	5.3.4	5.3.4
WAN SS	NA	5.3.2	5.4	5.3.5	5.3.4	NA
LSC	CCA	5.3.2.9	5.4	5.3.5	5.3.4	
	Media Gateway	5.3.2.12	5.4	5.3.5	5.3.4	5.2
	Signaling Gateway	5.3.2.13			5.3.4	5.2
AS-SIP EI	NA	5.3.2	5.4	5.3.5	5.3.4	NA
AS-SIP TDM Gateway	NA	5.3.2.7.4	5.4	5.3.5	5.3.4	
AS-SIP IP Gateway	NA	5.3.2.7.5	5.4	5.3.5	5.3.4	
DSMCU		1.4				
LAN Access Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
LAN Distribution Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
LAN Core Switch	NA	5.3.1	5.4	5.3.5	5.3.4	NA
Wireless LAN Products		5.3.1	5.4	5.3.5	5.3.4	NA
EBC	NA	5.3.2.15	5.4	5.3.5	5.3.4	NA
CE Router	NA	5.3.2.14	5.4	5.3.5	5.3.4	NA

7.1.3 Circuit-Switched Products with IP on the Line Side Only that Support SBU Voice and Video Services

Circuit-switched products with IP on the line side only that support SBU voice and video services are described in UCR 2008.

7.1.4 Classified UC Products for E2E Systems that Support SBU Voice and Video Services

Table 7-2, Classified UC Products for IP E2E that Support Classified Voice and Video Services, delineates the sections where requirements for these products are found. Classified product requirements consist of general requirements found throughout Section 5.3.2, Assured Services Requirements, plus unique classified requirements found throughout Section 6.2, Unique Classified Unified Capabilities Requirements. The combination of requirements found across Sections 5.3.2 and 6.2 provides the total requirements that apply to the classified products.

Table 7-2. Classified UC Products for IP E2E that Support Classified Voice and Video Services

PRODUCT	UNIQUE REQUIREMENTS	GENERAL REQUIREMENTS	IA REQUIREMENTS	IPV6	AS-SIP
Tier0 SS	6.2	5.3.2	5.4	5.3.5	5.3.4
DSSS	6.2	5.3.2	5.4	5.3.5	5.3.4
LSC	6.2	5.3.2	5.4	5.3.5	5.3.4 and 6.2
LAN Access Switch	NA	5.3.1	5.4	5.3.5	5.3.4
LAN Distribution Switch	NA	5.3.1	5.4	5.3.5	5.3.4
LAN Core Switch	NA	5.3.1	5.4	5.3.5	5.3.4
EBC	NA	5.3.2	5.4	5.3.5	5.3.4
CE Router	NA	5.3.2	5.4	5.3.5	5.3.4

7.1.5 DRSN Switches and Peripheral Devices

Requirements for TDM-based DRSN equipment are not included in UCR 2008. Specifications for DRSN products are available on a need to know basis from the DISA NS DRSN Single Service Manager.

7.1.6 DISN Network Infrastructure Products

Table 7-3 delineates the network infrastructure UC products, which can be used by all MILDEPs for their Intranets. These UC products do not currently include data firewalls but will in future updates.

Table 7-3. DISN Network Infrastructure UC Product Categories

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
M13	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
MSPP	5.5	System providing access to the DISN WAN from the Edge by multiplexing lower bandwidth connections to higher speed circuits
Aggregation Router	5.5	System serving as a port expander for a PE Router
Provider Edge Router	5.5	System providing robust, high-capacity IP routing at the entry points to the DISN WAN

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
Provider Router	5.5	System providing robust, high-capacity IP routing in the DISN WAN
Optical Switch	5.5	Switching system providing high-speed optical transport in the DISN WAN

LEGEND
DISN Defense Information Systems Network
IP Internet Protocol
MSPP Multi-Service Provisioning Platforms
PE Provider Edge
WAN Wide Area Network

7.1.7 Deployed UC Products

Table 7-4 delineates the Deployed UC products. Deployed switching system requirements consist of general requirements found throughout UCR 2008, Section 5.2, Circuit-Switched Capabilities and Features, plus unique Deployed requirements found throughout Section 6.1.3, Deployable Voice Exchanges. The combination of requirements found throughout UCR 2008, Sections 5.2 and 6.1 provides the total requirements that apply to the Deployed products.

Table 7-4. Deployed UC Product Categories and Paragraph Reference

PRODUCT	GENERAL REQUIREMENTS SECTION	UNIQUE REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DVX-C	5.2	6.1.3	Deployed voice switch with ASF capabilities to support assured service requirements. This switch is used for rapid deployment situations and contingencies in the Deployed environment.
DVX Legacy (DVX-L)	5.2	6.1.3	Deployed voice switch with ASF capabilities to support assured service requirements. This switch is part of the TRI-TAC systems and thus termed Legacy.
Deployable DSN PBX1	5.2	6.1.3	A DSN PBX1 used in the Deployed arena When used in the Deployed arena, the PBX1 is connected to a DSN EO through a STEP/Teleport
Deployed Network Elements	NA	9.3	Network elements used in the deployed environment.
Deployed LANs	5.3.1	5,3,1 and 6.1.5	LAN used in the deployed environment
Deployed Tactical Radio	6.1.7	6.1.7	Radio systems used in the deployed environment.

PRODUCT	GENERAL REQUIREMENTS SECTION	UNIQUE REQUIREMENTS SECTION	ROLE AND FUNCTIONS
DCVX	NA	6.1.6	Deployed cellular system with ASF capabilities to support assured service requirements. This system is used for rapid deployment situations and contingencies.

LEGEND

ASF	Assured Services Features	DVX-L	Deployable Voice Exchange–Legacy
COTS	Commercial Off-the-Shelf	EO	End Office
DCVX	Deployed Cellular Voice Exchange	LAN	Local Area Network
DSNY	Defense Switched Network	PBX1	Private Branch Exchange 1
DVX	Deployable Voice Exchange	STEP	Standardized Tactical Entry Point
DVX-C	Deployable Voice Exchange–COTS	TRI-TAC	Tri-Service Tactical Communications

7.1.8 Security Devices

Table 7-5, Security Devices and Paragraph Reference, summarizes the security products used in the IP environment. The requirements for encryption products are found in UCR 2008, Section 5.6, Generic Encryption Device Requirements.

Table 7-5. Security Devices and Paragraph Reference

ITEM	REQUIREMENTS SECTION	ROLE AND FUNCTIONS
HAIPE	5.6	HAIPE is a programmable IP INFOSEC device with traffic protection, networking, and management features that provide IA services for IPv4 and IPv6 networks.
Link Encryptors	5.6	Link encryptors provide data security in a multitude of network elements by encrypting point-to-point, netted, broadcast, or high-speed trunks.
Firewalls	5.8	A System that blocks unauthorized access while permitting authorized communications
Intrusion Protection System (IPS)	5.8	A system that detects and protects against unwanted attempts at accessing, manipulating and/or disabling an IT system
VPN Concentrator and Terminations	5.8	A device that sets up a secure link between an external end user and an internal network

LEGEND

HAIPE	High Assurance Internet Protocol Encryptor	IPv4	Internet Protocol Version 4
IA	Information Assurance	IPv6	Internet Protocol Version 6
INFOSEC	Information Security		