TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

APPENDIX B
UNIQUE CLASSIFIED UNIFIED CAPABILITY

B.1 PURPOSE AND SCOPE

This section describes technical requirements that are unique to providing classified Unified Capabilities (UC). Classified requirements consist of the Sensitive but Unclassified (SBU) requirements with modifications as described in this section. This issue of the Unified Capabilities Requirements (UCR) specifies technical requirements for assured interoperability and Information Assurance of the following set of UC:

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

More specifically, meeting the requirements specified in this section will allow classified UC products to be tested and placed on the UC Approved Products List (APL).

The current Classified Voice and Video over Internet protocol (IP) (CVVoIP) system is a single security level network operating over the Defense Information Systems Network (DISN) SECRET Aggregation Routers (ARs) that include secure voice capabilities that interface with the Defense RED Switch Network (DRSN) at selected locations. The CVVoIP system described is not intended to replace the DRSN and its many unique features.

The contents of this section are arranged as follows:

- Section B.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 Voice and Video over IP (VVoIP) services.
- Section B.2, General Requirements Overview, provides a summary of the CVVoIP requirements that drive the CVVoIP design.
- Section B.3, Migration to AS-SIP Signaling for DISN CVVoIP, addresses the Voice over Secure IP (VoSIP) migration to a multivendor IP-based, assured, secure CVVoIP system.
- Section B.4, Initial CVVoIP Technical Design, addresses the CVVoIP IP technical design.
- Section B.5, Modifications to the SBU Assured Services Requirements To Include CVVoIP-Unique Requirements, describes the modifications to the SBU Assured Services (AS) requirements as necessary to include CVVoIP-unique requirements. Topics discussed include voice End Instrument (EI), Session Controller (SC) requirements, network-level Softswitch (SS), Media Gateway (MG), Signaling Gateway (SG), Session Border Controller (SBC), addressing schema, Network Management (NM), voice quality, Wide Area Network (WAN) requirements, and the Information Assurance requirements.

- Section B.6, Classified AS-SIP-Unique Requirements, defines the modifications to the SBU UC Session Initiation Protocol (SIP) requirements as necessary for classified AS.
- Section B.7, DRSN Switches and Peripheral Devices, discusses special construction requirements that include Protected Distribution System (PDS) cabling, encryption of facilities leaving a secure enclave, and TEMPEST.
- Section B.8, Physical Construction Unique Requirements, discusses the special construction requirements for classified elements within a secure enclave.
- Section B.9, UC Secure Preset Conference, describes the requirements that will enable SBU voice subscribers equipped with a National Security Agency (NSA) Type I encryption device to conference in the secure mode.

B.1.1 Policy and Requirements Documents for DRSN and CVVoIP

All the policies identified in Section 3, Policy, apply to CVVoIP. Table B.1-1, Major Policy and Requirements Drivers for Defense Information Systems Network (DISN) CVVoIP Services, lists the major policy and requirements documents that are unique to Multi-Level Security (MLS) voice services provided by the DRSN and to single security level DISN CVVoIP services.

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

TITLE	DATE OR VERSION
Joint Requirements Oversight Council (JROC), JROC Memorandum (JROCM) 202-02, "Global Information Grid (GIG) Mission Area Initial Capabilities Document (MA ICD)" 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	22 November 2002
Department of Defense Directive (oODD) 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

TITLE	DATE OR VERSION
"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)," For Official Use Only (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
National Security Telecommunications and Information Systems Security, NSTISSI No. 4002, "Classification Guide for COMSEC Information (U)," SECRET/Not Releasable to Foreign Nationals (S/NF)	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"	

B.2 GENERAL REQUIREMENTS OVERVIEW

A high-level summary of the requirements for CVVoIP are provided by a combination of the documents referenced in Table B.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 Command and Control (C2) communications service offering. These performance attributes have been proven in real world operations stretching from OPERATION DESERT SHIELD/DESERT STORM through OPERATION IRAQI FREEDOM.

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

- Multilevel secure service.
- Rapid, high-quality, secure communications and conferencing capabilities for senior leaders and warfighters.
- Assured services.
- Information Assurance.
- End-to-End (E2E) interoperability.
- Network Operations (NetOps).

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-commercial off-the-shelf (COTS) MLS operator console features have been developed in response to the Combatant Commands' (COCOMs') command center requirements. These unique features, which are part of the way those command centers conduct their business, will not be required for CVVoIP.

B.2.1 Assured Services

The CVVoIP system shall provide AS features as described in Section 2, Session Control Products.

B.2.2 Multilevel Secure Voice Services

The CVVoIP services are provided using the SECRET-level Secure IP Router Network (SIPRNet) as the IP transport infrastructure. The CVVoIP services use the Confidential Access Level (CAL) parameter within the Assured Services Session Initiation Protocol (AS-SIP) signaling protocol to identify the security level of a session. The security level indicated by the CAL parameter is transmitted to the DRSN via the CVVoIP-DRSN Gateway as described in Section B.5.4, DRSN to CVVoIP Media Gateway With Signaling Interworking.

B.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 E2E voice quality requirements for the IP-based environment of CVVoIP are based on Mean Opinion Score (MOS) measurements as defined in Section B.5.8, Voice Quality. The objective of the DRSN subset of secure voice 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.

B.2.4 C2 Requirements

This section provides a summary of the system-wide C2 requirements for classified services. The term "system" as used in this section refers to the combination of the DRSN and CVVoIP environments. Once IP technology matures to the necessary level, the full complement of C2 requirements may be provided by the CVVoIP system.

For the near-term, the following requirements will be met by a combination of the CVVoIP 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/Electromagnetic Interference (EMI) compliance.
- Integrated RED-BLACK instruments (DRSN only):
  - Instruments located in a Sensitive Compartmented Information Facility (SCIF) must meet the Committee on National Security Systems (CNSS) 5000-series instructions and procedures (DRSN and CVVoIP).
- Secure conferencing:
  - Ad hoc conference (3-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.
  - Multilevel Precedence and Preemption (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 Military Strategic, Tactical, and Relay (MILSTAR) and Secure Terminal Equipment (STE) terminals (DRSN only)].
  - Media conversion.
  - Protocol conversion.
  - Speakers, recorders.
  - Other networks, such as MILSTAR.SECN, Defense Satellite Communications System (DSCS)/Early Pentagon Capability (EPC), Homeland Security, FBI, and Department of State (DRSN only).

B.2.5 Key CVVoIP Voice Services Features

The key CVVoIP voice services features and attributes are shown in Table B.2-1, Key CVVoIP Voice Service Features.

Table B.2-1. Key CVVoIP Voice Service Features

FEATURE NAME	FEATURE FUNCTIONAL PURPOSE
Automatic Number Identification (ANI)	Provides caller ID to both users
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

B.2.6 General Security Features

The DRSN RED Switches, classified SCs, 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, CVVoIP users and classified SCs are to be configured only 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 must be approved or implemented as defined by the SIPRNet Connection Approval Process. The DRSN RED Switches and CVVoIP SCs, must interconnect with other RED Switches and/or peripheral devices (to include, but not limited to, Deployed secure voice switches or enclaves, radio interfaces, audio systems, voice announcers, and multimedia and/or secure voice over data capabilities) through encrypted ISTs or by means of a PDS. Other secure systems must interconnect to the DRSN using Defense Information Systems Agency (DISA)-established interface criteria and encryption devices or a PDS.

B.2.7 Special Security Features

Currently, the following special security features are 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.

- 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 is 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 (S), TOP SECRET (TS), or TS/Sensitive Compartmented Information (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.
- 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.

- Automatic Security Authentication (ASA). The ASA ensures DRSN calls are set up in accordance with (IAW) 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 3b) of SECRET calling a user classmarked with a VSAL of TOP SECRET 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 3a) 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.
  - 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., TOP SECRET), 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.
  - 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 established automatically 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.

- 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 IAW DRSN security guidelines.

B.2.8 Network Security

- The DRSN RED Switches, CVVoIP SCs, 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 and CVVoIP SCs will provide the following:
  - In-the-clear calling within each RED enclave by means of PDSs and protected Assured Services Local Area Networks (ASLANs).
  - Cryptographically protected calling between RED enclaves supported by DRSN RED Switches and CVVoIP SCs.
  - DRSN RED Switches, and CVVoIP SCs interface to external cryptographic equipment for all other calling.
- The NSA-approved encryption equipment provides Communications Security (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 Telecommunications Security (TSEC)/KG-84 family of equipment (including KIV-7) provides Transmission Security (TRANSEC) to ISTs to locations (including quarters) receiving DRSN service via Digital Phone Adapter (DPA), Digital Trunk Adapter (DTA), 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.
- The DRSN and 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 or limited exclusion area within the quarters and must comply with requirements set forth in the security guides for DRSN and VoSIP/CVVoIP.

B.2.9 Network Interfaces

A key feature of the DRSN is its ability to interface and interoperate with a variety of Department of Defense (DoD) and commercial networks. The CVVoIP system interfaces to the DRSN through a gateway. (See Section B.5.4, DRSN to CVVoIP Media Gateway With Signaling Interworking.)

B.2.10 CVVoIP 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 must follow the SIPRNet Connection Approval Process. The Joint Interoperability Test Command (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 effects 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.

B.2.11 DRSN and 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 Systems Security Manager (SSM), on behalf of the U.S. Strategic Command (USSTRATCOM), and is responsive to the Chairman of the Joint Chiefs of Staff (CJCS), the COCOMs, the Military Departments (MILDEPs), and Defense agencies and activities.

- DISA must possess read-access capabilities and limited or 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.
- DISA must maintain a Configuration Management (CM) database of all switch configurations (continental United States [CONUS] and outside CONUS [OCONUS]) and provide access to agencies, activities, and MILDEPs as authorized by the Office of the Secretary of Defense (OSD); the Director, DISA; and the Joint Staff.
- 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 SCs) 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 Operations and Maintenance (O&M) activities before implementing DRSN and Tier0 switch network-level database changes and/or network controls.
- During emergencies, DISA has the authority to use direct write capabilities to implement switch database revisions required for operation and management of the DRSN and CVVoIP system.

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

B.2.12 Conferencing Requirements

The CVVoIP services will not provide the full conferencing features inherent with the DRSN, but CVVoIP users must be able to join and participate in conferences set up by external conference systems and the DRSN. The SC must support use of the CAL/SAL functionality as part of conferencing. The CVVoIP SC must be capable of providing a minimum of 5 simultaneous preset conferences with a minimum of 25 participants (local and external). Each preset pattern must be able to coexist with other conferences as independent conferences. Expanded requirements for secure preset and meet-me conferences based on SBU voice subscribers equipped with NSA Type I encryption devices are provided in Section B.9, UC Secure Preset Conference.

B.2.13 CVVoIP Equipment Certification and Testing Policy

Interoperability and Information Assurance testing of CVVoIP equipment will be executed in accordance with DoDI 8100.04.

B.3 MIGRATION TO AS-SIP SIGNALING FOR DISN CVVOIP

The core system must be able to support both H.323 and AS-SIP until a migration to all AS-SIP is completed.

B.4 INITIAL CVVOIP TECHNICAL DESIGN

Figure B.4-1, Overview of Initial CVVoIP Assured Services Design, illustrates the CVVoIP technical design for assured classified services at a single security level. The red text illustrates the significant changes introduced to achieve E2E CVVoIP with assured service. The design is similar to the one that is used by the SBU VVoIP with the following significant differences:

- The SECRET Provider Edge (PE) (S-PE) Routers, the SECRET Customer Edge (CE) (S-CE) Routers, and the SECRET Aggregation Routers (S-ARs) versus the U-PE, U-CE, and U-ARs will be used.
- A High Assurance IP Encryptor (HAIPE) will be used with the S-PE Router.
- The AS-SIP protocol version used for CVVoIP is a modification of the SBU version (See Section B.6, Classified AS-SIP-Unique Requirements).
- The bearer stream will use the Real-Time Transport Protocol (RTP) rather than Secure Real-Time Transport Protocol (SRTP). This is acceptable since all CVVoIP enclaves are protected by encryption devices.

- The use SBCs are not required. For CVVoIP the UC signaling and bearer traffic go through existing SIPRNet data firewalls; these data firewalls have been configured with port ranges to allow UC traffic to pass.

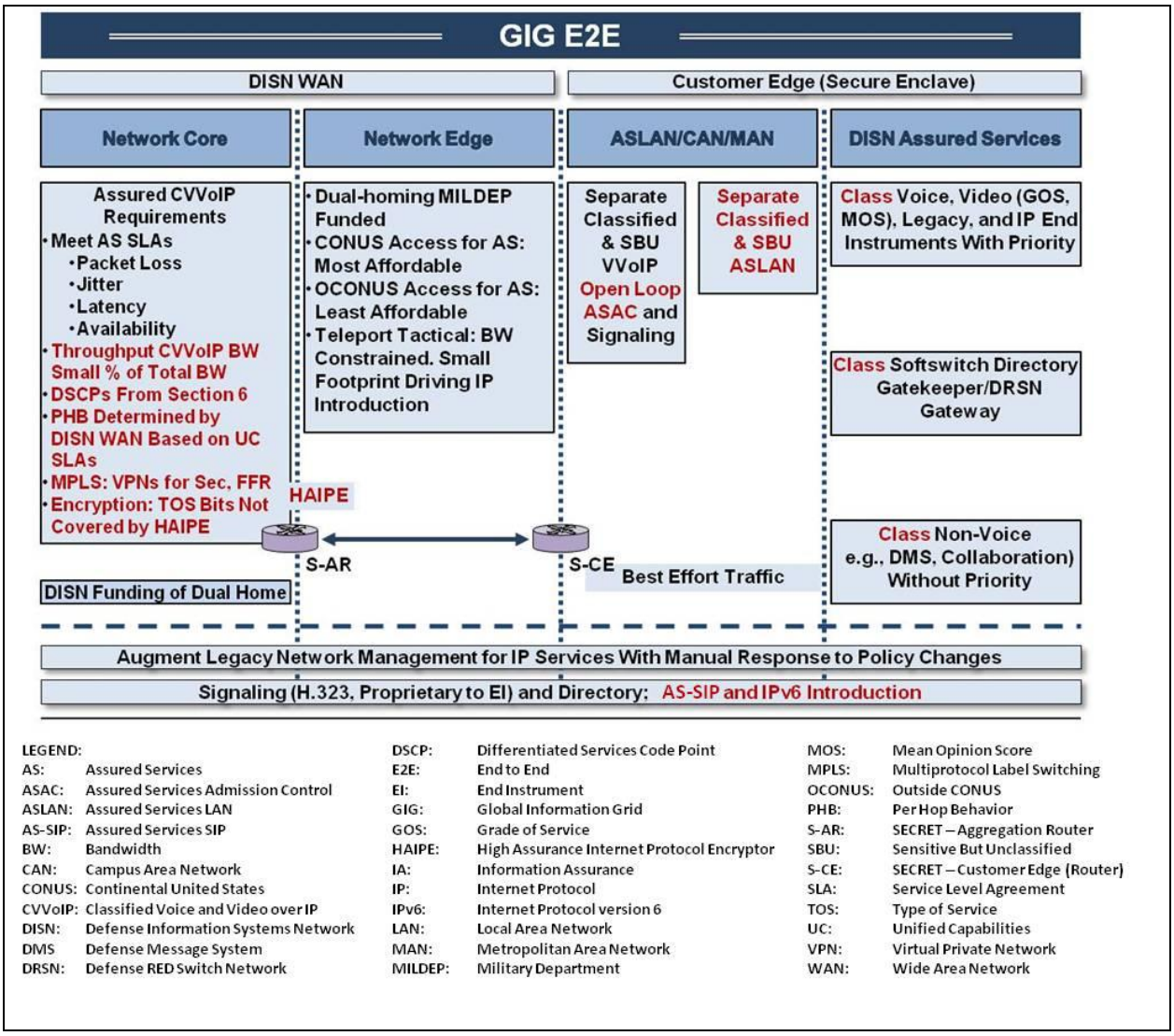

Figure B.4-1. Overview of Initial CVVoIP Assured Services Design

The classified SS (referred to as Tier0 SSs) is pure IP without a Time Division Multiplexing (TDM) signaling capability, except they provide a unique media and signaling interface to the DRSN.

Both networks depend on the robustness of the DISN WAN and its ability to meet Service-Level Agreements (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 the Integrated Services Digital Network (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. Users will be encouraged to convert to IP video services when AS-SIP with the full H.323 feature set is available. Nevertheless, until NSA develops an IP replacement for the KIV, multilevel secure services will have to be over the DSN ISDN circuit-switched services.

B.4.1 Signaling Design

The signaling design has to provide both backward and forward technology capabilities. Thus, Client Access Server (CAS) and PRI in the DRSN has to interoperate with H.323 signaling in the current CVVoIP network 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 is depicted in Figure B.4-2, DISN CVVoIP Hybrid Signaling Design.

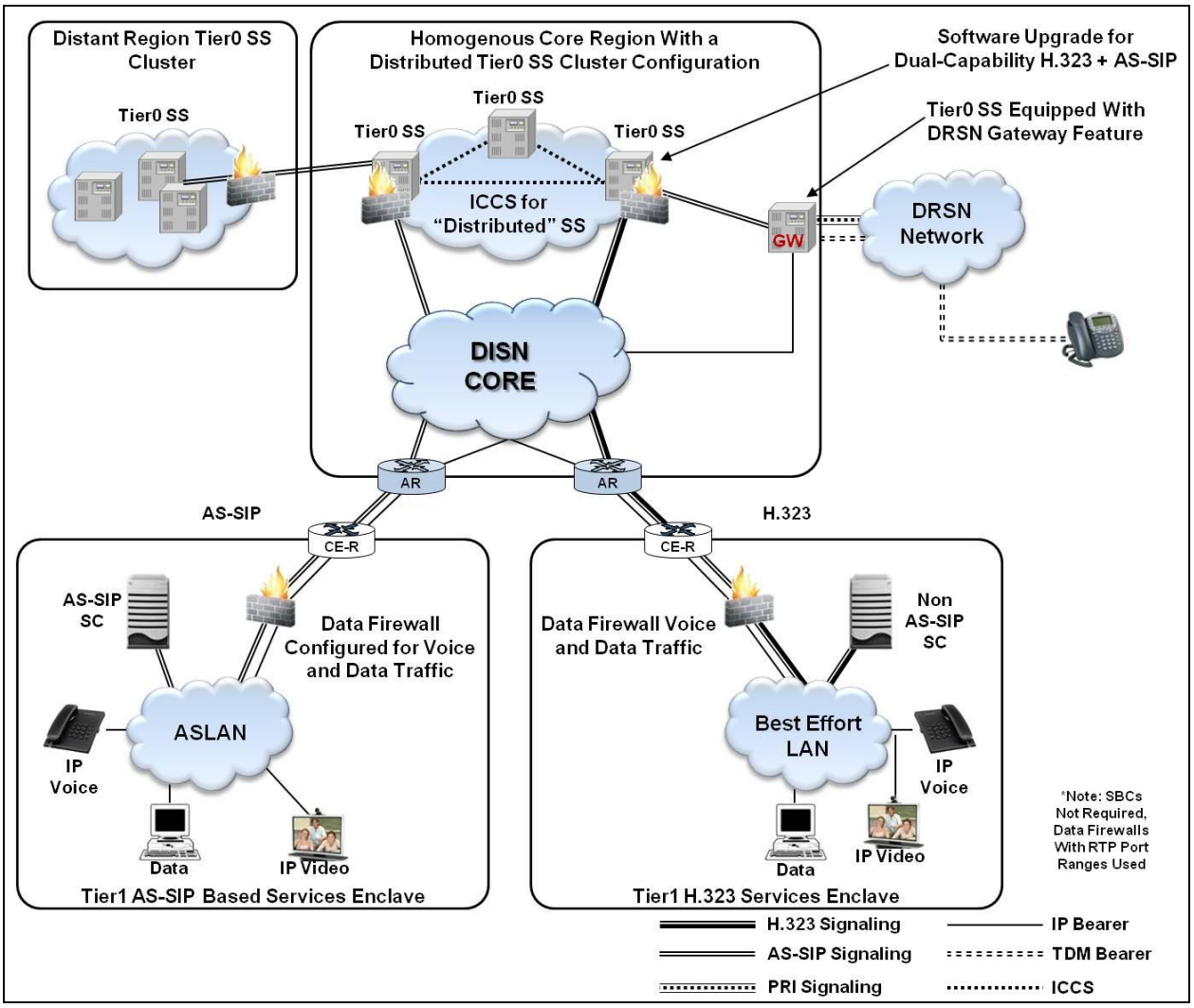

Figure B.4-2. DISN CVVoIP Hybrid Signaling Design

The hybrid signaling design is constructed as a two-tier hierarchy consisting of a "local" level and a "backbone" level. At the local level, SCs 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 SCs. The backbone, or Tier0 signaling, level is a robust, homogeneous design based on current vendor-unique geographic cluster arrangements of Tier0 SS. 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 to AS-SIP based 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 B.5.3, Network-Level Softswitches.)

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 SCs as well as a few, select Tier0 SSs provide "Managed Services" to a limited set of EIs and, therefore, a Tier0 SS may have an SC function associated with it also.

Every SC 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 by 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 non-service 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. 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 SC from a local EI and intended for a destination outside the secure service enclave is sent by the SC 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 SC or to a Tier0 SS located in a different geographic area; this Tier0 SS then, in turn, forwards the message to the distant-end SC. Similarly, all session signaling messages sent from a remote location and intended for IP EIs associated with a given SC will be routed to the Tier0 SS assigned to the destination SC and the Tier0 SS will forward the AS-SIP signaling messages to the destination SC.

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

Originating SC --- Tier0 SS 1 ---------- Tier0 SS 2 --- Destination SC

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

Originating SC --- Tier0 SS --- Destination SC

The access link between the CE Router and the AR is resource constrained and the SC 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 SC has exceeded its provisioned threshold for voice traffic or video traffic.

B.4.2 Bearer Design

The CVVoIP local service enclaves and core locations are protected by encryption devices and data firewalls with ports open to accommodate voice, video, and data traffic. As a result, bearer design for the CVVoIP system will use the Real Time Protocol (RTP). SBCs are currently not employed within CVVoIP system, but may be installed as an option at certain local service enclaves and at Tier0 core locations.

B.5 MODIFICATIONS TO THE SBU ASSURED SERVICES REQUIREMENTS TO INCLUDE CVVOIP-UNIQUE REQUIREMENTS

Section 2, Session Control Products, addresses the functions, methods, protocols, and associated technical parameters for the EI, SC, SS, SBC, and NM components of the DISN VVoIP System. AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, 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.

B.5.1 Voice End Instrument

CLA-000010 [**Required: Voice EI**] Voice Instruments require two-factor authentication [This may be achieved by using a Common Access Card (CAC)-enabled instrument or other security means].

CLA-000020 [**Required: Voice EI**] Voice instruments must display the security level (CAL) of the call.

B.5.2 Classified SC Requirements

B.5.2.1 SBU SC Requirements Not Applicable to Classified SC

The following SC requirements defined in Section 2.10, Session Controller, do not apply to the classified SC:

1. MG, SG for SS7 (the classified SCs do not interface to external networks).
2. Public safety features [e.g., Public Safety Announcement Bulletin (PSAB), E911 access].

B.5.2.2 Classified SC Unique Requirements

The following general requirements are unique to classified SCs:

- Located in secure enclave.
- PDS cabling per DRSN requirements.
- Dynamic Host Configuration Protocol (DHCP) not allowed, strict control of EI assignments using static IP addresses.
- Use the classified version of AS-SIP signaling, including sending CAL/SAL display information to the end instrument.
- Expanded conferencing features to include minimum of five simultaneous presets with a minimum of 25 participants (local and external). Each preset conference pattern must be able to coexist with other conferences as independent conferences. The conferencing capability must support the CAL/SAL functionality.
- Automatic Security Authentication (ASA) with a mix of fixed and variable SAL.

B.5.3 Network-Level Softswitches

Section 2.11, Network-Level Softswitches, describes the network-level SSs used in the SBU network. The CVVoIP system uses a unique backbone SS referred to as a Tier0 SS. During the 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 SCs. When augmented, the Tier0 SS will become an APL product referred to as a DSSS. Figure B.5-1, DSSS Reference Model, provides the functional reference model for the DSSS.

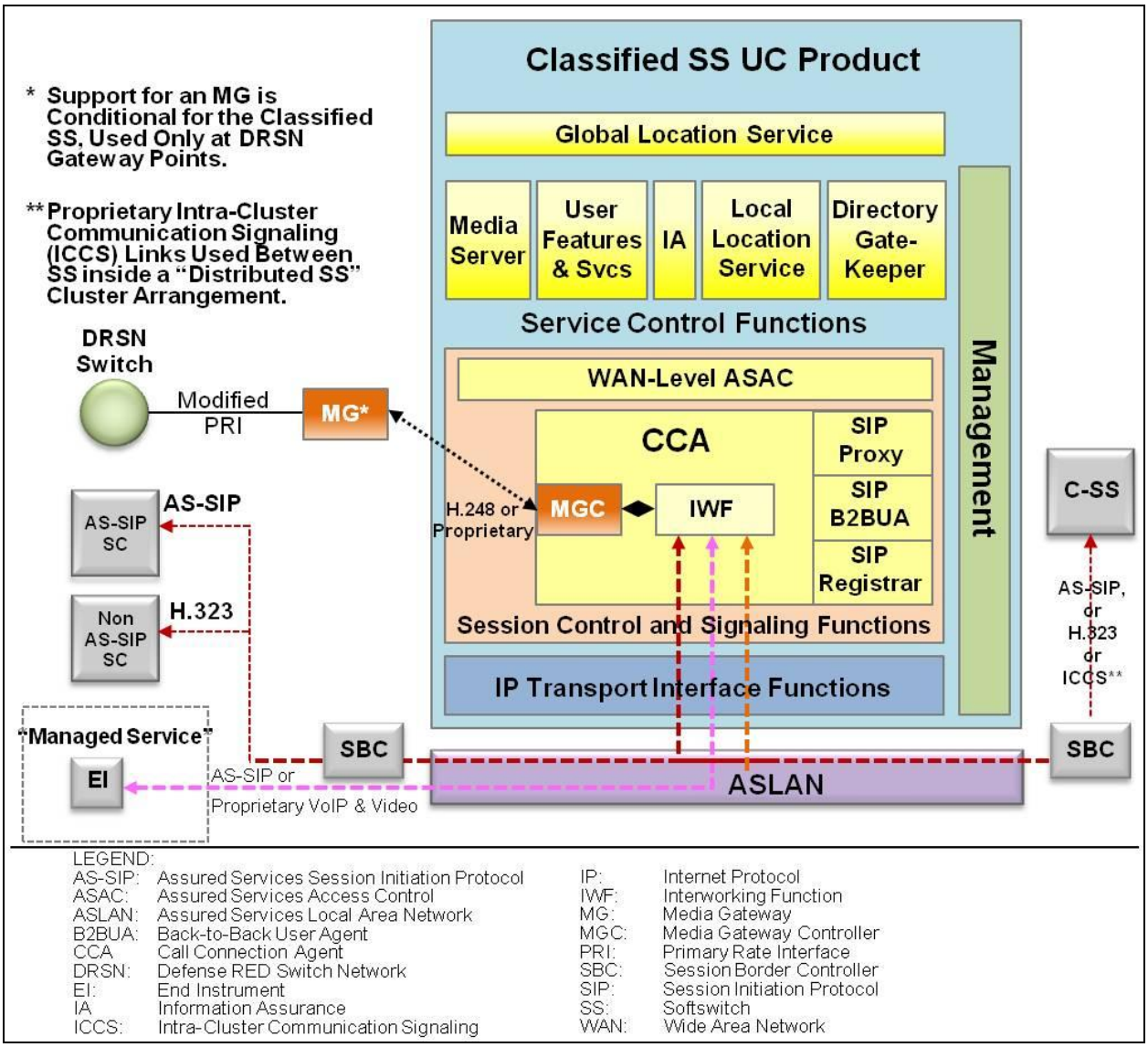

Figure B.5-1. DSSS Reference Model

CLA-000030 [**Required: Tier0 SS, DSSS**] The product must provide both H.323 Directory/Gatekeeper functionality and AS-SIP as well as interworking between the two signaling methods. (This is a transitional requirement until CCVoIP becomes all AS-SIP-based).

CLA-000040 [**Required: Tier0 SS, DSSS**] 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 SC or the SC function of a Tier0 SS. The subscribers are located in a remote secure enclave and provided secure (encrypted) access to the SC.

CLA-000050 [**Required: Tier0 SS, DSSS**] Numbering plan/addressing compatibility with DRSN, Tactical Global Block Numbering Plan (GBNP), and SIPRNet IP addressing schema.

CLA-000060 [**Optional: Tier0 SS, DSSS**] There are no TDM capabilities except as noted for the MG function at selected locations.

CLA-000070 [**Not Required: Tier0 SS, DSSS**] Public safety features (e.g., PSAB, E911 access) are not required.

B.5.4 DRSN to CVVoIP Media Gateway With Signaling Interworking

B.5.4.1 General

As the Classified Voice and Video over Internet Protocol (CVVoIP) service evolves, the classified IP telephony component (CVoIP) will coexist with the Defense RED Switch Network (DRSN) for an unspecified period, as the DRSN will continue to serve as the foundation of a DoD multilevel secure C2 voice capability. During this period of coexistence, the requirement exists to provide interoperability and transparency of features and capabilities between the DRSN domain and the CVoIP domain. The bridge between these domains is a Media Gateway and Signaling Interworking function. This "bridge" is based on the use of an ISDN Primary Rate (PRI) user-network interface in which the interface structure is composed of multiple B channels, one D-channel and a User-User Information Element (UUIE) on the DRSN side of the "bridge" and an IP signaling protocol on the CVVoIP side of the "bridge." This "bridge" provides, among other things, a methodology and capability for the interworking and interoperability of SALs used in the DRSN Domain and Confidential Access Levels (CALs) used in the CVVoIP domain. The required Media Gateway and Signaling Interworking function for the CVVoIP is exclusively instantiated as a function of and at the DISA Tier0 Softswitch infrastructure. This section establishes the CVVoIP Media Gateway and signaling Interworking requirements between the DRSN domain and the CVVoIP domain.

It is assumed that the reader has some familiarity with the function and operation of SALs used in the DRSN domain and CALs used in the CVVoIP. The reader's attention is further directed to the CVVoIP "CAL General Requirements" established by and in AS-SIP 2013, Section 4.9.2, Presence of CAL Header in INVITE Requests, 200 Responses, 418 Responses, and in Section B.2.7, Special Security Features, for CVVoIP signaling appliances.

B.5.4.2 DRSN Signaling Protocol

A base assumption for the DRSN/MG interface is that the Classified Voice over IP (VoIP) (CVoIP) network side is configured as homogenous with respect to the DISA-defined SAL methodology. Adjudication, changes to the call SAL and call clearing as a result of mismatch are contained within DRSN.

CLA-000080 [**Required: MG**] The DRSN Signaling Protocol interface 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 Primary Rate Interface (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 Media Gateway user-to-network signaling physical layer specification for the PRI operating at 1.544 megabits per second (Mbps) shall be American National Standards Institute (ANSI) T1.408.

CLA-000090 [**Required: MG**] The MG shall support the option to operate in accordance to the 4ESS Primary Rate specification: AT&T TR41459. Physical layer specifications previously defined apply for the 4ESS variant.

CLA-000100 [**Required: MG**] Requirements for ISDN SAL service shall be in accordance with ANSI Standards T1.621-1992 User-to-User Signaling Supplementary Service.

CLA-000110 [**Required: MG**] ISDN PRI Setup Message shall contain the User-User Information Element, as shown in Table B.5-1, ISDN PRI User-User Information Element (Setup/Connect).

Table B.5-1. ISDN PRI User-User Information Element (Setup/Connect)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	1
7	0	1	0	1	1	1	0	1
	SAL Protocol Identifier							
8	Length of SAL Message							
9	Message Type ID							
10	Precedence Level							
11	0/1	Security Access Level Designation						
	V/F							
12	0	0	0	0	0	0	0	0
	0	0	0	0	1	0	1	0
13	0	0	0	0	1	0	1	0
	User-Specific Protocol							
14–29	Caller ID							
Octet 4-7: (Static Definition) MG ingress: no processing								

MG egress: must be populated with the information indicated in Table B.5-1
Octet 9: Message Type ID Bits 8 7 6 5 4 3 2 1 0 0 0 0 1 0 1 0 (Call – Sent with SETUP message) 0 0 0 0 0 0 1 0 (Answer – Sent with CONNECT message) MG ingress: reject call if value other than in Table B.5-1, or misaligned with the indicated PRI message MG egress: set appropriately to PRI message
Octet 10: Precedence Level Bits: 8 7 6 5 4 3 2 1 0 0 0 0 0 0 0 0 (No precedence) 0 0 0 0 0 0 0 1 (Routine – lowest) 0 0 0 0 0 0 1 0 (Priority) 0 0 0 0 0 0 1 1 (Immediate) 0 0 0 0 0 1 0 0 (Flash) 0 0 0 0 0 1 0 1 (Flash Override) 0 0 0 0 0 1 1 0 (Flash Override Override – highest) 1 1 1 1 1 1 1 1 (Not Used)
Octet 11: Security Access Level – SAL Bit 8: Set to 0 for Variable Security Access Level, set to 1 for Fixed Security Access Level Bits 7 6 5 4 3 2 1: Security Access Level (SAL) value. Valid values – 2 thru 99.
Octet 12: (Static Definition) MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-1.
Octet 13: (User Specific Protocol) This octet is not applicable to UC. MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-1.
Octet 14-29: Caller ID (optional, if text is provided it must comply with the following instructions, otherwise should be left null) The remaining octets allow the passing of Caller ID information between switch nodes. Octet 14 is the left most character and octet 29 is the right most character. The information from this field is used for end instruments with display capabilities to display the Caller ID of the calling party. Valid values: A-Z a-z 0-9 !@#$%^&*()-_+={}[]<>

CLA-000120 [**Required: MG**] The Setup Message User-User Information Element shall comply with population and processing guidance in Table B.5-1 and the table notes.

CLA-000130 [**Required: MG**] ISDN PRI Connect Message shall contain the User-User Information Element, as shown in Table B.5-1.

CLA-000140 [**Required: MG**] The Connect Message User-User Information Element shall comply with population and processing guidance in Table B.5-1 and the table notes.

CLA-000150 [**Required: DRSN and IP Signaling Appliance**] The Signaling Appliance shall contain a SAL/CAL Adjudication Map Approved by DISA for the adjudication and verification of SAL/CAL for calls and sessions

CLA-000160 [**Required: DRSN and IP Signaling Appliance**] The received SAL/CAL value shall be verified (per the DISA Adjudication Map) against the SAL/CAL configured for the MG interface and the call rejected with cause code 54 ("Incoming calls barred within Closed User Group") in the event of incompatibility.

CLA-000170 [**Required: DRSN and IP Signaling Appliance**] The SAL/CAL Adjudication Map shall be protected from unauthorized access.

CLA-000180 [**Required: DRSN and IP signaling Appliance**] Modifications to the SAL/CAL Adjudication Map shall be audited events.

CLA-000190 [**Required: DRSN and IP Signaling Appliance**] The DRSN/IP signaling appliance shall perform SAL/CAL adjudication (per the DISA Adjudication Map) between the SAL/CAL presented by the MG signaling and the EI(s) and update the MG SAL/CAL when adjudication results in a SAL/CAL adjustment.

CLA-000200 [**Required: DRSN and IP Signaling Appliance**] For ingress signaling containing SAL/CAL data, the text value corresponding to the numeric value shall be delivered to the EI (for display).

CLA-000210 [**Required: EI**] The latest SAL text received from the Signaling Appliance shall be continuously displayed on the EI for the duration of the call.

CLA-000220 [**Required: MG**] The MG shall support the User Information Message containing the User-User Information Element (from the DRSN signaling appliance) as shown in Table B.5-2, ISDN PRI UUIE (User Information for SAL), for the signaling of SAL level change during a connection.

Table B.5-2. ISDN PRI UUIE (User Information for SAL)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	0	0	0	1	1	1	0
	Operation							
5	0	0	0	0	0	1	1	1
	SAL Change							

6	Sale Numeric Value 2–99
7	Fixed/Variable SAL
Octet 4: (Static Definition) MG ingress: No processing MG egress: must be populated with the information indicated in Table B.5-2.	
Octet 5: Operation Type Bits 8 7 6 5 4 3 2 1 0 0 0 0 0 1 1 1 (SAL Change)	
Octet 6: Security Access Level - SAL Bits 8 7 6 5 4 3 2 1 Security Access Level (SAL) value. Valid values - 2 thru 99.	
Octet 7: Fixed/Variable SAL Bits 8 7 6 5 4 3 2 1 0 0 0 0 0 0 0 1 (Fixed SAL) 0 0 0 0 0 0 1 0 (Variable SAL)	

CLA-000230 [**Required: MG**] The User-User Information Element in the User Information Message for SAL change signaling processing shall comply with the processing guidance in Table B.5-2 and the table notes.

CLA-000240 [**Optional: MG**] The MG shall support User Information Message containing the User-to-User Information Element (from the DRSN signaling appliance) as shown in Table B.5-3, ISDN PRI UUIE (User Information for Caller ID), for the signaling of Caller ID change during a connection.

Table B.5-3. ISDN PRI UUIE (User Information for Caller ID)

Bit:	8	7	6	5	4	3	2	1
	User-User Information							
Octet 1:	0	1	1	1	1	1	1	0
	Element Identifier							
2	Length of User-User Contents							
3	0	0	0	0	0	0	0	0
	User-Specific Protocol							
4	0	0	0	0	1	0	1	1
	Operation							
5	0	0	0	0	0	0	0	0
	User-Specific Protocol							
6–21	Caller ID							
Octet 4: (Static Definition) MG ingress: No processing								

MG egress: must be populated with the information indicated in Table B.5-3.
Octet 5: (Static Definition) MG ingress: no processing MG egress: must be populated with the value indicated in Table B.5-3.
Octet 6-21: Caller ID The remaining octets allow the passing of Caller ID information between switch nodes. Octet 6 is the left most character and octet 21 is the right most character. The information from this field is used for end instruments with display capabilities to display the Caller ID of the calling party. Valid values – A-Z a-z 0-9 !@#$%^&*()-_+={}[]<>

CLA-000250 [**Optional: MG**] The User-User Information Element in the User Information Message for Caller ID change signaling processing shall comply with the processing guidance in Table B.5-3 and the table notes.

CLA-000260 [**Required: DRSN and IP Signaling Appliance**] The Signaling Appliance shall contain a mapping for numeric SAL/CAL values and their corresponding, DISA assigned, text.

CLA-000270 [**Required: DRSN and IP Signaling Appliance**] The SAL/CAL numeric-text mapping data shall be protected from unauthorized access.

CLA-000280 [**Required: DRSN and IP Signaling Appliance**] Modifications to the SAL/CAL numeric-text mapping shall be audited events.

CLA-000290 [**Required: MG**] The MG shall contain a DISA approved mapping to translate numeric SAL values to CAL values and vice versa.

CLA-000300 [**Required: MG**] The MG shall convert all received numeric SAL values to their corresponding numeric CAL value on signaling transmission.

CLA-000310 [**Required: MG**] The MG shall convert all received numeric CAL values to their corresponding numeric SAL value on signaling transmission.

CLA-000320 [**Required: MG**] The SAL/CAL numeric mapping data shall be protected from unauthorized access.

CLA-000330 [**Required: MG**] Modifications to the SAL/CAL numeric mapping shall be audited events.

B.5.4.3 Call Scenarios

The following call scenarios across the gateway are illustrated in the subsequent sections:

- Basic Calls:
  - MG to DRSN.
  - DRSN to MG, no SAL adjustment required on answer.
  - DRSN to MG, SAL adjustment required on answer.

  - Transfer from Secure VoIP EI, after connection, to a local phone.
- SAL Violation:
  - SAL violation on MG SETUP (pre-ring).
  - SAL violation on MG incoming call, DRSN user answer.
  - SAL violation after answer due to DRSN party change.
- Changes during call: SAL change during call due to DRSN party change.

B.5.4.3.1 Basic Call Scenarios

NOTE: All SAL adjudication is performed in the DRSN or IP Signaling Appliances. All privileges of acceptance, rejection, and adjustment of offered SALs will be contained within these signaling appliances. The primary obligation of the MG (with respect to SALs) is to translate (as may be required) numeric values from the IP domain (CAL) to the DRSN domain (SAL).

Figure B.5-2, Illustration of a Basic MG to DRSN Call I, illustrates a MG to DRSN Call.

NOTE: For MG to DRSN calls, the assigned SAL/CALs applied in determining the end-to-end SAL/CAL include the DRSN trunk SAL and any CAL assigned to the IP side of the MG.

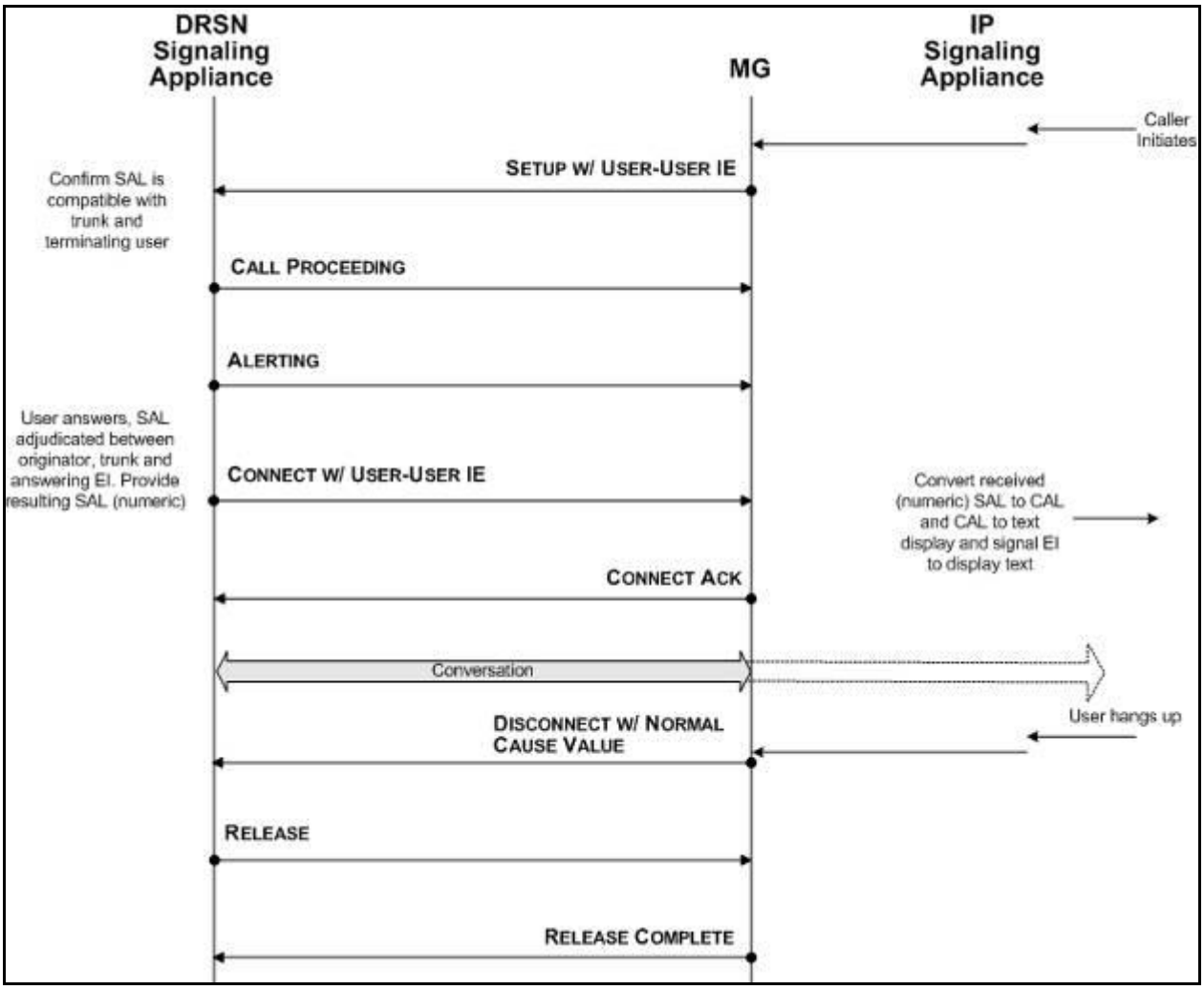

Figure B.5-2. Illustration of a Basic MG to DRSN Call I

Figure B.5-3, Illustration of a Basic DRSN to MG Call, With No SAL Adjustment, illustrates a DRSN to MG, with no SAL adjustment.

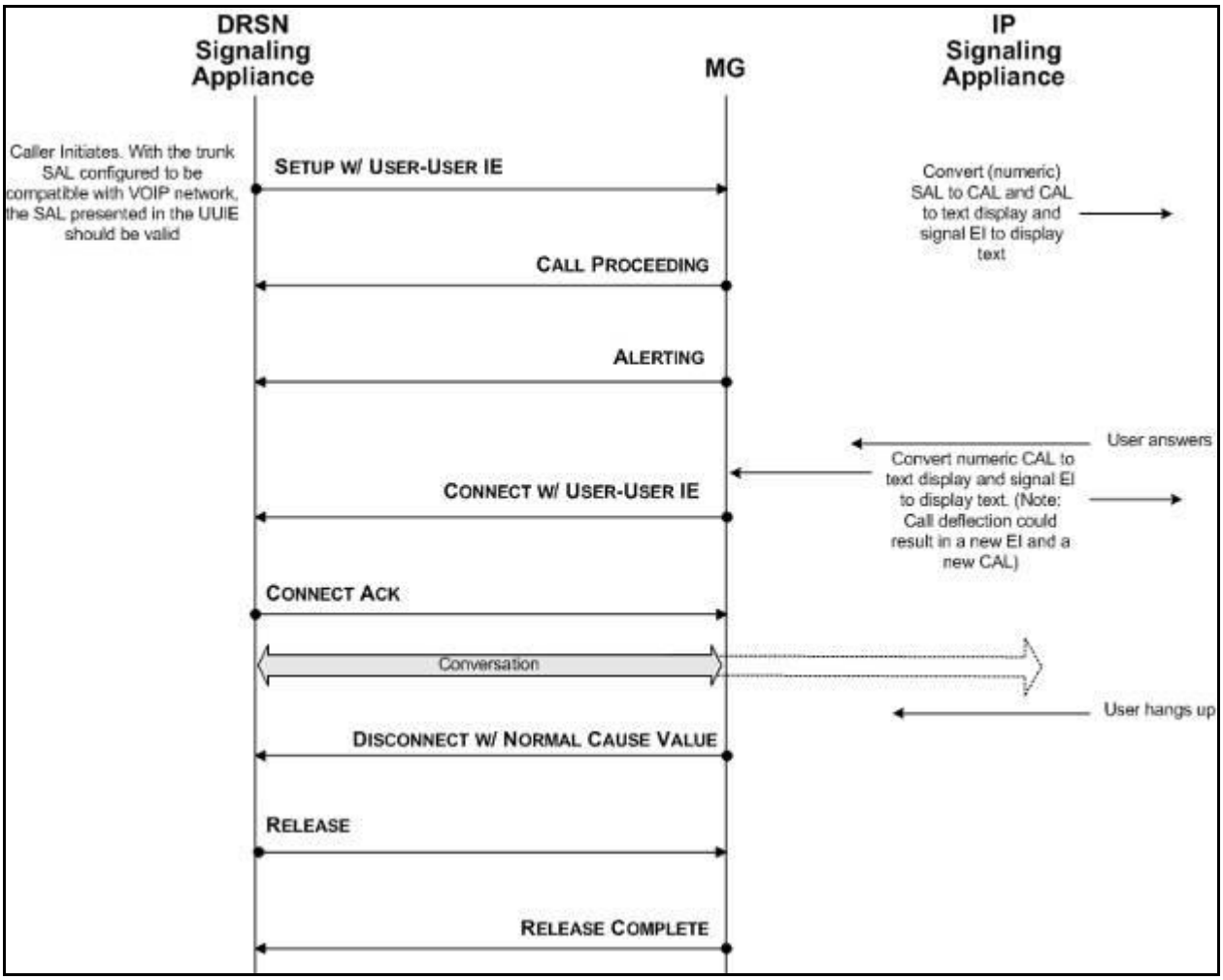

Figure B.5-3. Illustration of a Basic DRSN to MG Call, With No SAL Adjustment

Figure B.5-4, Illustration of a Basic DRSN to MG Call, With SAL Adjustment Required, illustrates a basic DRSN to MG, with SAL adjustment required.

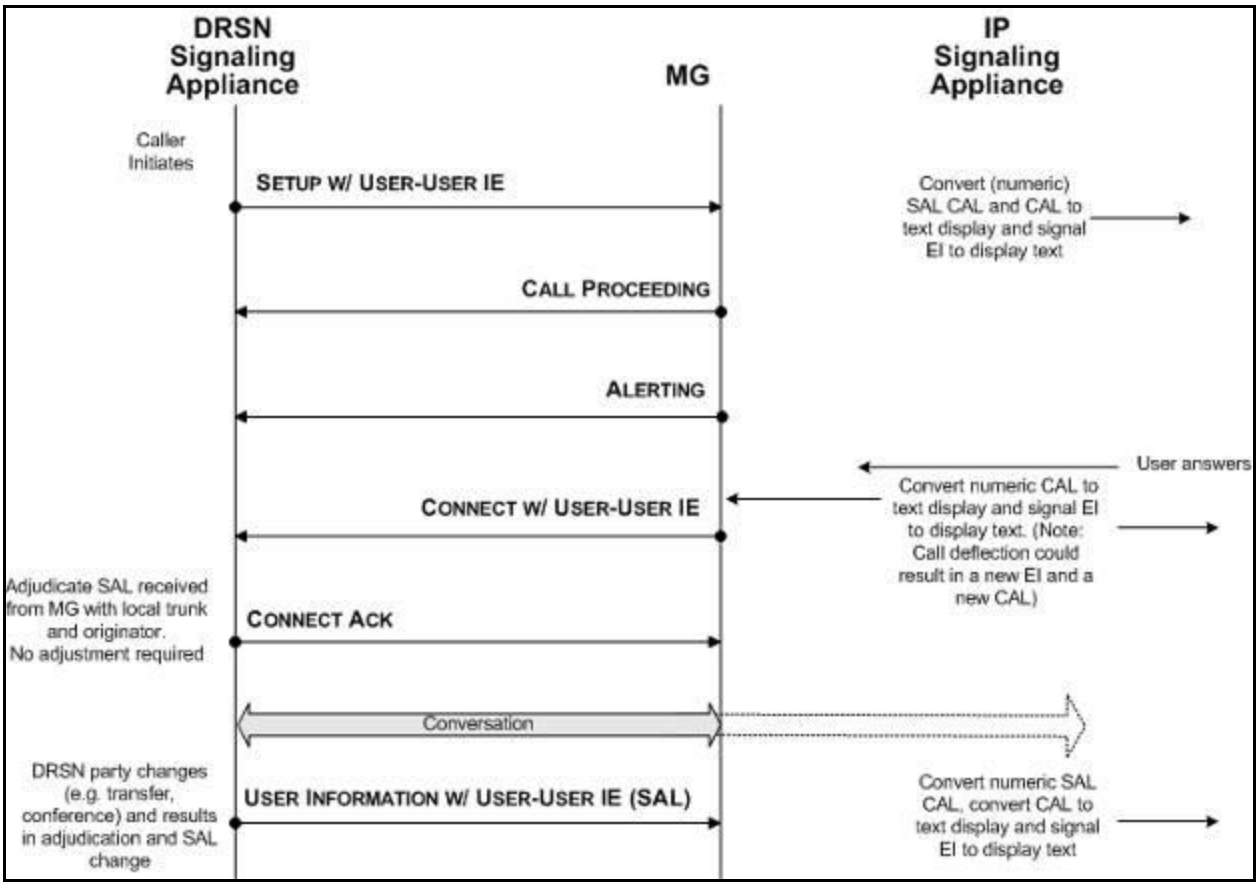

Figure B.5-4. Illustration of a Basic DRSN to MG Call, With SAL Adjustment Required

This scenario will be valid if IP communities assign a variety of "caveats" within a security domain. Such an event might result in local adjudication or when a CONNECT with a SAL variation is received.

Figure B.5-5, Illustration of Transfer Invoked From VoIP EI to a Local VoIP EI With Different Security Domain Caveat, illustrates Transfer invoked from VoIP EI to a local VoIP EI with different security domain caveat.

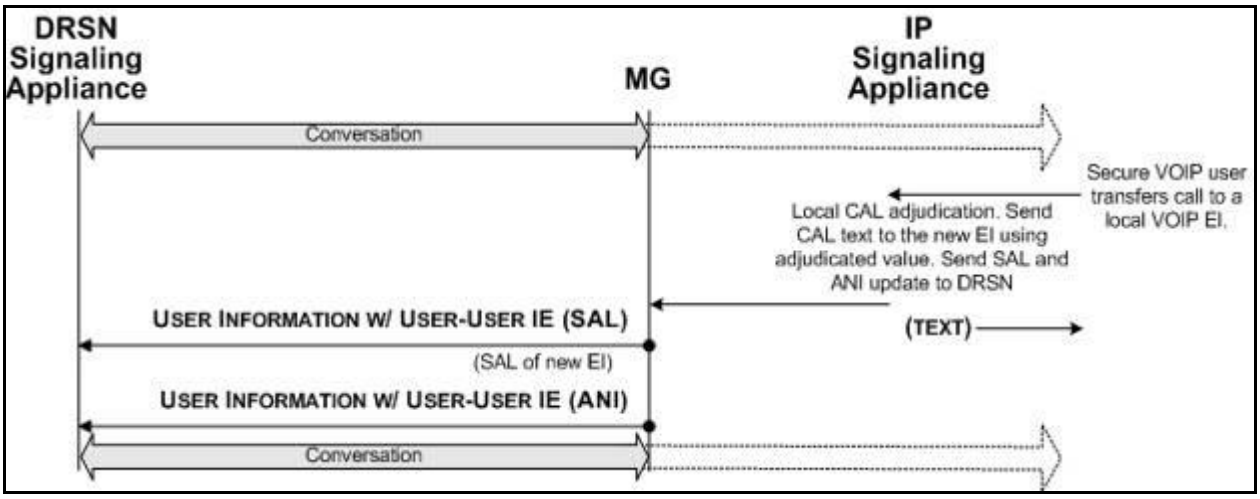

Figure B.5-5. Illustration of Transfer Invoked From VoIP EI to a Local VoIP EI With Different Security Domain Caveat

B.5.4.3.2 SAL Violation Scenarios

Figure B.5-6, Illustration of SAL Violation on MG SETUP (pre-ring), illustrates SAL violation on MG SETUP (pre-ring). The SAL provided on the MG SETUP was either incompatible with the trunk SAL (indicating misconfiguration) or was incompatible with the destination EI SAL.

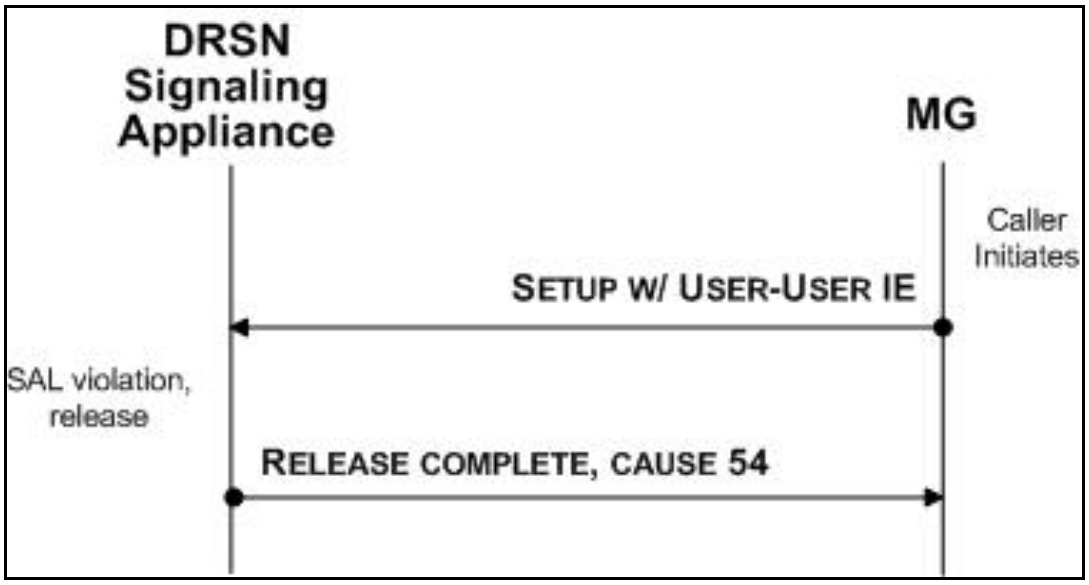

Figure B.5-6. Illustration of SAL Violation on MG SETUP (pre-ring)

Figure B.5-7, Illustration of SAL Violation on an MG Incoming Call, DRSN User Answer, illustrates SAL violation on a MG incoming call, DRSN user answer. The call was originally allowed to proceed since the originator, trunk and termination party SALs were compatible. Some party other than the original destination (e.g., Station Hunt Group, Call Pickup) answered the call and resulted in a violation.

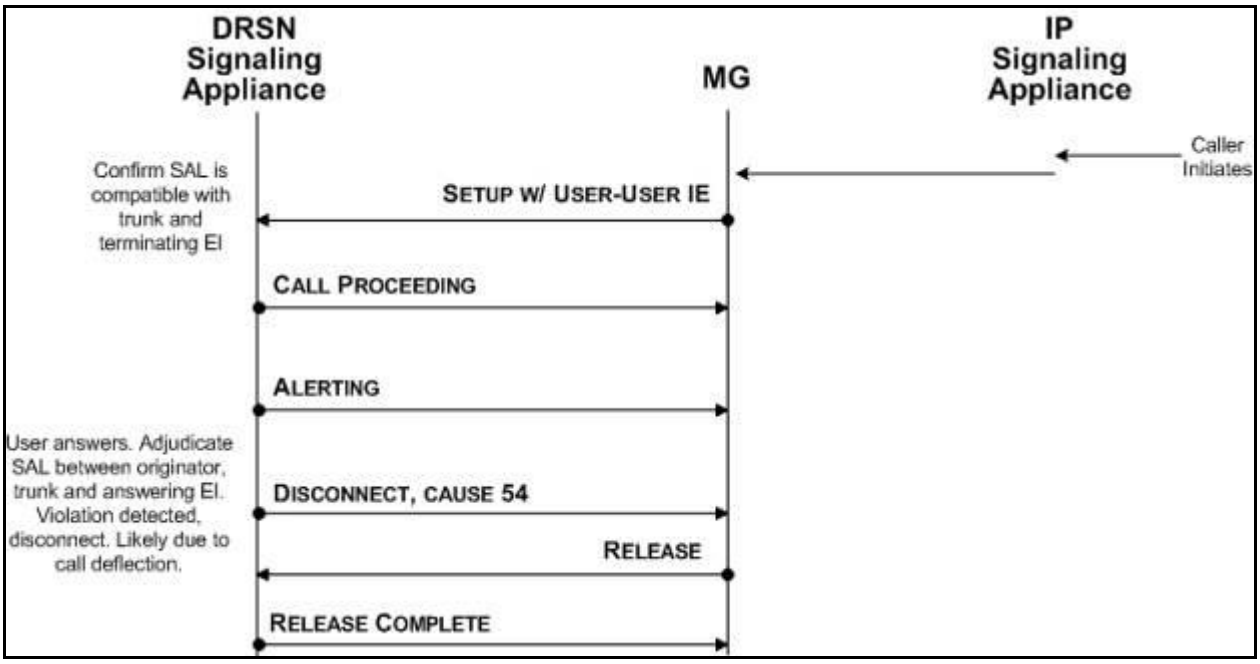

Figure B.5-7. Illustration of SAL Violation on an MG Incoming Call, DRSN User Answer

Figure B.5-8, Illustration of SAL Violation After Stable Call Resulting From DRSN Party Change, illustrates a SAL violation after a stable call because of a DRSN party change. The DRSN party performed an action that involved the addition of a new SAL into the conversation, resulting in a SAL violation.

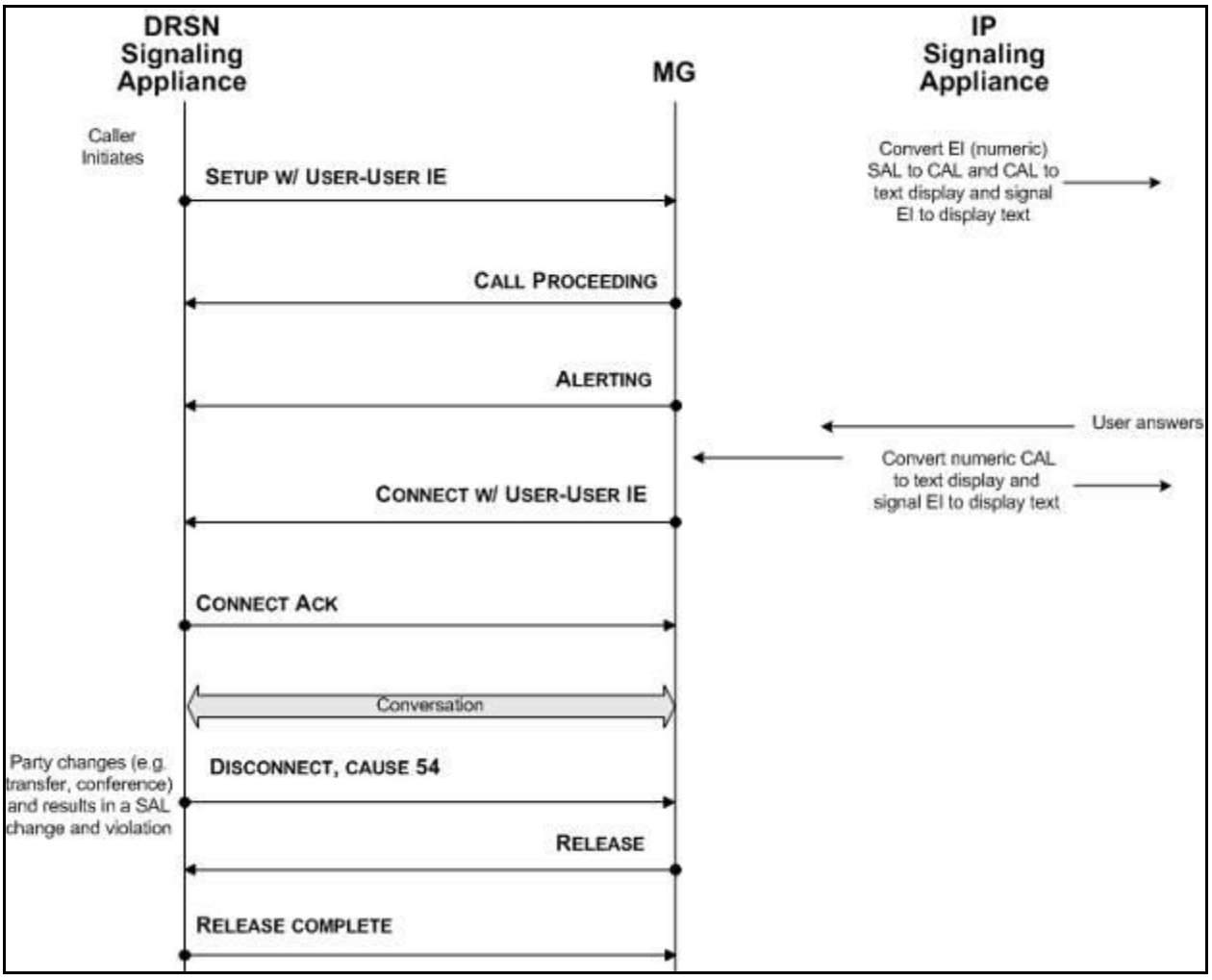

Figure B.5-8. Illustration of SAL Violation After Stable Call Resulting From DRSN Party Change

B.5.4.3.3 Changes During Call

Figure B.5-9, Illustration of a SAL Change During Call Resulting From DRSN Party Change, illustrates a SAL change during call because of DRSN party change. A DRSN party has performed an action that results in a new party and SAL becoming involved in the conversation.

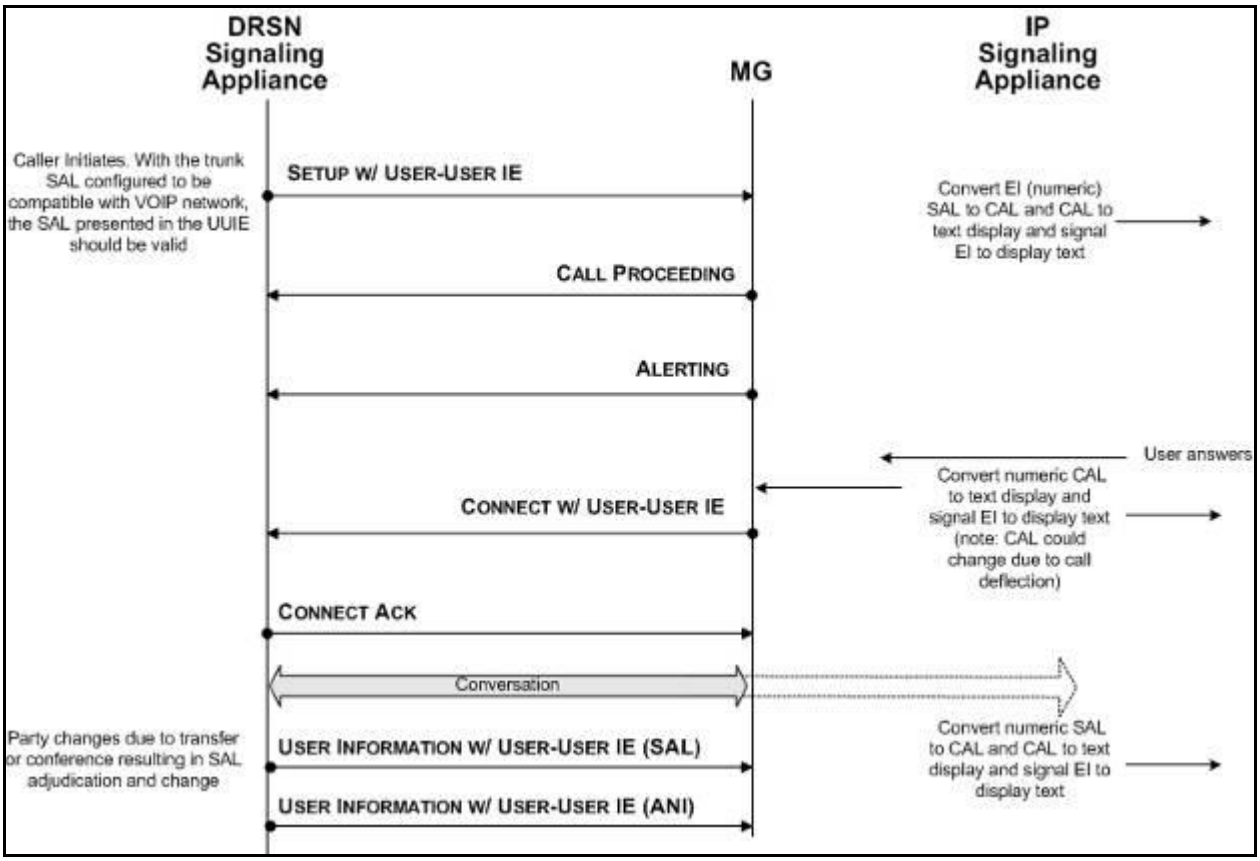

Figure B.5-9. Illustration of a SAL Change During Call Resulting From DRSN Party Change

B.5.5 Session Boundary Controller

All requirements for the SBC specified in Section 2, Session Control Products, apply to the CVVoIP system. The use SBCs are optional within the CVVoIP.

- Where used, the SBC must be dedicated to CVVoIP services and not shared with SBU services.

B.5.6 Addressing Schema for SC

The following additional requirements are unique to the classified SCs:

CLA-000340 [**Required: SC**] The classified SCs must have a DRSN and CVVoIP (as established by VoSIP) numbering plan capability.

CLA-000350 [**Required: SC**] The classified SCs must have interoperability with the Tactical GBNP.

CLA-000360 [**Required: SC**] The classified SCs must have SIPRNet IP addressing schema.

B.5.7 Network Management

All requirements specified in Section 2.17, Management of Network Appliances, for NM apply to the classified SC, SBC, and Tier0 SS.

The following unique features are required for classified:

CLA-000370 [**Required: SC**] The SC shall generate an alarm message indicating that a registered CVVoIP EI has been unplugged.

CLA-000380 [**Required: SC**] The SC shall generate an alarm message indicating that a registered CVVoIP EI that was previously unplugged has been plugged back in.

B.5.8 Voice Quality

CLA-000390 [**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 IAW the following scenarios:

a. Fixed-to-Fixed – 4.0.

b. Fixed-to-Deployable – 3.6.

c. Deployable-to-Deployable – 3.2.

CLA-000400 [**Required**] The method used for obtaining the MOS shall be in accordance with the DoD Information Technology Standards Registry (DISR) mandated standard International Telecommunications Union – Telecommunication (ITU-T), P.800, "Methods for Subjective determination of Transmission," August 1996.

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 2.19.3.1.1, Quality of Service.

B.5.9 Call Setup Time

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

- For SC intraenclave 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.
- For interenclave 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.

B.5.10 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.

CLA-000410 [**Optional**] If the classified Edge system appliance supporting VVoIP uses an Ethernet interface for connecting to the Local Area Network (LAN), then its Network Interface Card (NIC) MTU size shall be set to 1280 bytes.

NOTE: This will allow for overhead associated with encryptors or Virtual Private Networks (VPNs).

CLA-000420 [**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 Differentiated Services Code Point (DSCP) discriminators exist between ROUTINE and above ROUTINE VVoIP sessions across the encryption boundaries (i.e., HAIPE).

Figure B.5-10, Addition of Encryption Within the Network Infrastructure, illustrates where encryption elements fit within the current network design.

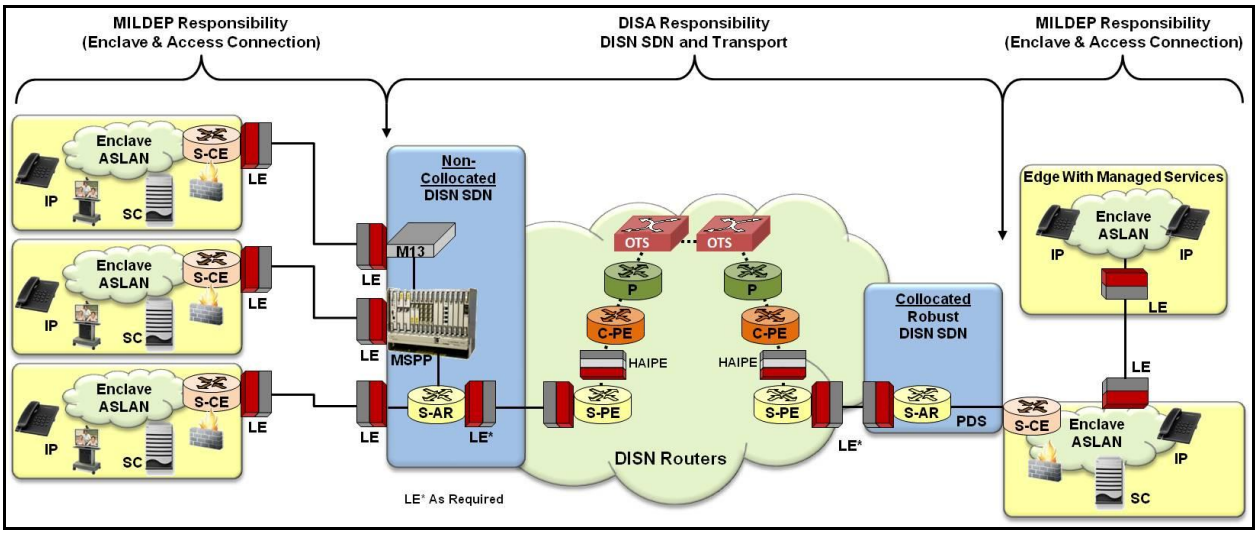

Figure B.5-10. Addition of Encryption Within the Network Infrastructure

B.5.11 Unique Information Assurance Requirements for CVVoIP

All Information Assurance requirements are specified in Section 4, Information Assurance. In addition, the following requirements are unique to the CVVoIP services:

CLA-000430 [**Required: EI**] The product shall be capable of being enabled or disabled using two-or three-factor authentication.

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

CLA-000440 [**Required: EI**] If the product supports an enable or disable code, the enable code shall be unique for that facility.

CLA-000450 [**Required: EI**] If the product supports an enable or disable code, the code shall be able to be modified by an authorized authority.

CLA-000460 [**Required: EI**] If the product supports an enable or a disable code, the product shall have a configurable code aging parameter, and the default shall be 90 days.

CLA-000470 [**Optional: SC, EI**] The product shall be capable of using three-factor authentication to include Public Key Infrastructure (PKI) certificates and biometric mechanisms for authenticating user credentials to the SC via the EI.

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

CLA-000480 [**Required: E**I] The product shall be capable of meeting the DoD Public Key Enabled (PKE) requirements for PKI-based authentication.

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

CLA-000490 [**Optional: Tier0 SS, DSSS, SC, MG, BC**] The product 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.

CLA-000500 [**Required: Tier0 SS, DSSS, SC, MG, BC**] If the product supports classified users, the system shall be capable of ensuring that all unused network access device connections or physical ports are secured appropriately 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 Virtual LAN (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) is used.

CLA-000510 [**Required: Tier0 SS, DSSS, SC, 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.

CLA-000520 [**Optional**] 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 logon attempts to include the following:

(1) Failed logon attempt because of an excessive number of logon attempts.

(2) Failed logon attempt because of blocking or blacklisting of a user ID.

(3) Failed logon attempt because of blocking or blacklisting of a terminal.

(4) Failed logon attempt because of 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).

CLA-000530 [**Required: Tier0 SS, DSSS, SC, 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).

CLA-000540 [**Required: Tier0 SS, DSSS, SC, MG, BC, R, LS**] The product shall be capable of supporting an out-of-band (OOB) or direct connection method for product device management.

CLA-000550 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product 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.

CLA-000560 [**Optional: R**] If the product uses an OOB management method, the product shall be capable of limiting management connections to authorized source IP addresses.

CLA-000570 [**Optional: R**] If the product uses an OOB management method, the product shall be capable of maintaining a separation between the management and production networks.

NOTE: This requires physically separate networks.

CLA-000580 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product 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.

CLA-000590 [**Optional: Tier0 SS, DSSS, SC, MG, BC, R, LS**] If the product uses in-band management, it shall be capable of restricting the sessions to a limited number of authorized IP addresses.

B.6 CLASSIFIED AS-SIP-UNIQUE REQUIREMENTS

AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, provides all the 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.

B.6.1 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 B.4.1, Signaling Design. The design is also depicted in Figure B.6-1, DISN CVVoIP Hybrid Signaling Design.

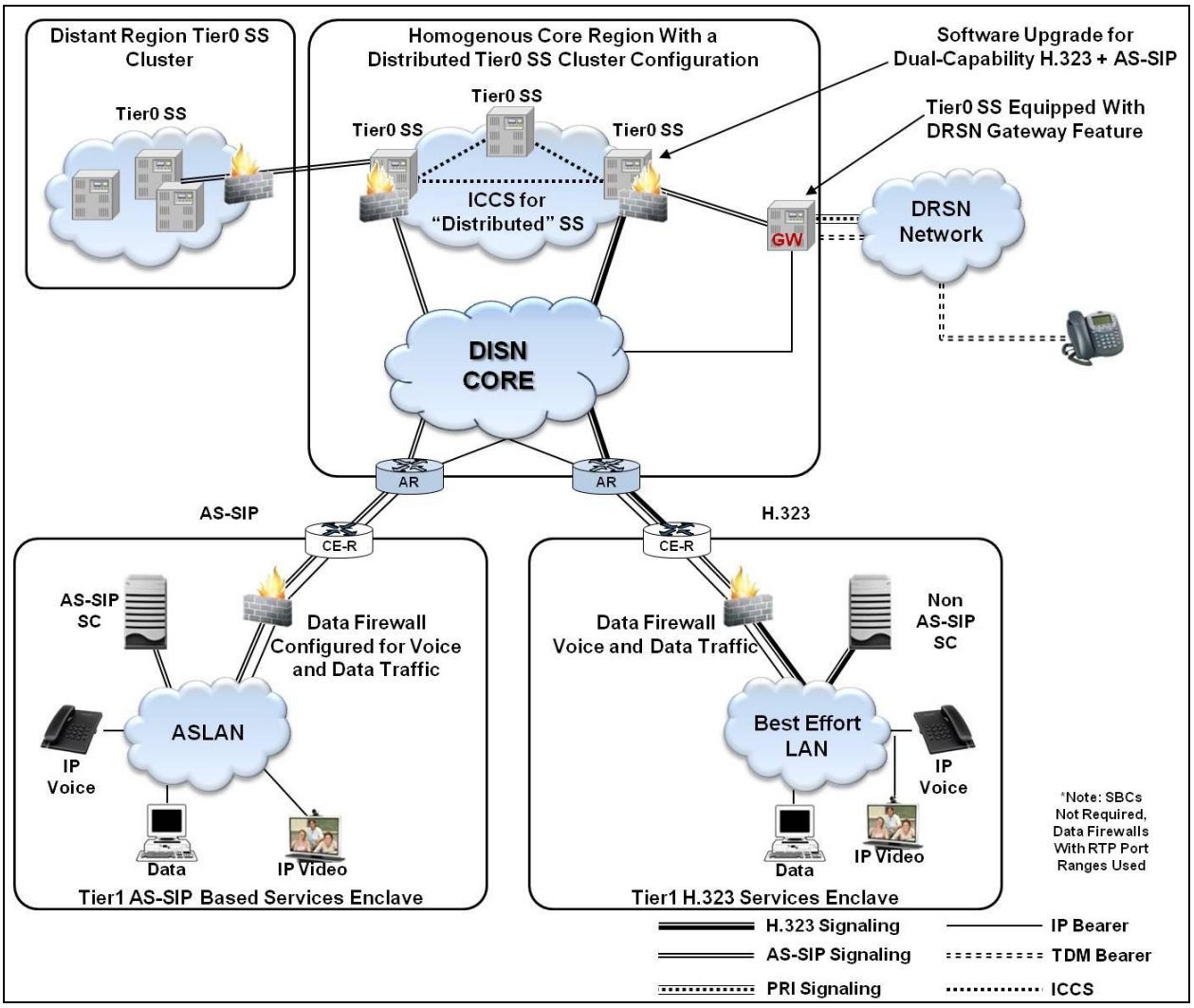

Figure B.6-1. DISN CVVoIP Hybrid Signaling Design

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

B.6.1.1 IP Signaling Path Reference Cases

Based on the top-level signaling design depicted in Section B.6.1, Classified Signaling Environment, the signaling paths that must be supported to provide the classified VVoIP services are identified in Figure B.6-2, IP Signaling Path Reference Illustration, and Table B.6-1, Reference Case: IP-to-IP Calls Over an IP Backbone.

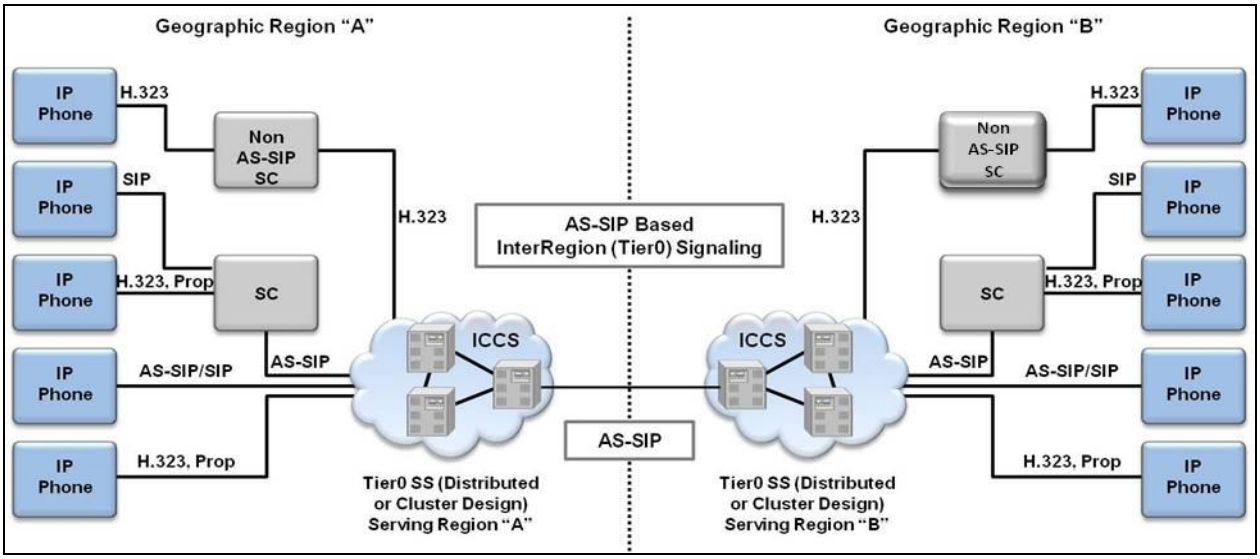

Figure B.6-2. IP Signaling Path Reference Illustration

Table B.6-1. 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	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1B	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone
1C	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1D	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1E	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1F	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone
1G	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			SIP	IP phone
1H	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP	Tier0 SS			H323, Prop.	IP phone
1I	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	SIP	IP phone
1J	IP phone	SIP			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	H323, Prop.	IP phone

REF. CASE	ORIGINATOR PHONE	ORIGINATOR SIGNALING	NETWORK SIGNALING AND CALL PATH							TERMINATOR SIGNALING	TERMINATOR 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	SC	SIP	IP phone
1N	IP phone	H323, Prop.			Tier0 SS	AS-SIP	Tier0 SS	AS-SIP	SC	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
2A	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP			SC	SIP	IP phone
2B	IP phone	SIP	SC	AS-SIP	Tier0 SS	AS-SIP			SC	H323, Prop.	IP phone
2C	IP phone	SIP	SC	AS-SIP	Tier0 SS					SIP	IP phone
2D	IP phone	SIP	SC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2E	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP			SC	SIP	IP phone
2F	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS	AS-SIP			SC	H323, Prop.	IP phone
2G	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS					SIP	IP phone
2H	IP phone	H323, Prop.	SC	AS-SIP	Tier0 SS					H323, Prop.	IP phone
2I	IP phone	SIP			Tier0 SS	AS-SIP			SC	SIP	IP phone
2J	IP phone	SIP			Tier0 SS	AS-SIP			SC	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			SC	SIP	IP phone
2N	IP phone	H323, Prop.			Tier0 SS	AS-SIP			SC	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

B.6.2 Differences Between SBU and Classified AS-SIP Requirements

AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, defines both SBU and classified requirements. The classified-specific requirements are defined in AS-SIP 2013, Sections 4.3.1.4 and 4.3.1.5 (Route Header Requirements); AS-SIP 2013, Section 4.3.2, (Proxy Require header), AS-SIP 2013 Section 4.4.1 requirement number AS-SIP 001480, (418 response); AS-SIP 2013, Section 4.5.2 (SIP Preconditions); AS-SIP, Section 4.7 (CAL Requirements); and AS-SIP 2013, Section 6.1.1.5 (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.

B.6.2.1 Nomenclature

The classified environment uses the term Tier0 SS (Tier0 SS) while AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs, 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 B.6-1, 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 SC (or the calling party's EI directly) and the called party's SC (or the called party's EI directly). Reference cases are not shown for non-AS-SIP SCs.

B.6.2.2 Route Header Requirements

The Route header requirements for SCs and SSs are predicated on the SBU network design in which SBCs are required at each enclave having at least one AS-SIP signaling appliance.

The current CVVoIP network design defines SBCs as optional; therefore, it is anticipated that during the transition toward full implementation of AS-SIP within the classified network there will be instances where SBCs 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 SBC is present at a Tier0 SS or at an SC, or at both. If there is not an SBC at either location and there are no intermediary AS-SIP signaling appliances between an SC and its Tier0 SS, then there may not be a need for a Route header. (See AS-SIP 2013, Sections 4.3.1.4 and 4.3.1.5)

B.6.2.3 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 AS-SIP 2013, Section 4.3.2:

The "Proxy-Require" must be generated for the classified network only.

B.6.2.4 418 Response

AS-SIP 2013, Section 4.4.1, requirement AS-SIP 00148 states (NOTE: This paragraph applies to classified only), "The SCs 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 [User Agent Server] UAS or to the access-level supported for the routing domain that failed resolution at an intermediate Tier0 SS."

B.6.2.5 SIP Preconditions

AS-SIP 2013, Section 4.5.2, states that implementation of preconditions is conditional for the classified network. [RFC 3312]

B.6.2.6 CAL Requirements

AS-SIP 2013, Section 4.9, defines 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.

B.6.2.7 Precedence Levels

AS-SIP 2013, Section 6.1.1.5, defines precedence level requirements for the classified network. The classified adds a FLASH OVERRIDE-OVERRIDE (FOO) precedence level.

B.6.2.8 SIP URI Mapping of Telephone Number

AS-SIP 2013, Section 4.6, SIP URI and Mapping of Telephone Number Into SIP URI, describes the SIP Uniform Resource Identifier (URI) and telephone number mapping requirements. The following modifications apply to the classified version of AS-SIP:

- Instead of uc.mil, use cuc.mil in the host name for classified SIP URIs.
- Instead of uc.mil, use cuc.mil with the phone-context parameter.
- The SBU Requirements [SIP-46170] and [SIP-46180] apply to interworking of telephone numbers on the Public Switched Telephone Network (PSTN) and they are conditional in the classified specification.
- 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.

B.6.2.9 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 Section 4.7, 64 Kbps Transparent Calls (Clear Channel), do not apply.

B.6.2.10 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 Section 4.8, Transport of Route Code Information over AS-SIP, do not apply.

B.6.2.11 Classified VoIP Information Signals

Table 6.1-4, UC Information Signals (from Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs), 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 B.6-2, CVVoIP Information Signals, is the expanded version.

Table B.6-2. 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 sec	
LEGEND Hz: Hertz IPM: Impulse Per Minute ms: Millisecond sec: Second						

B.6.2.12 Policing of Call Count Thresholds

Section 7, SS 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.

B.7 DRSN SWITCHES AND PERIPHERAL DEVICES

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

B.8 PHYSICAL CONSTRUCTION UNIQUE REQUIREMENTS

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

- All cabling must follow PDS guidelines.
- Cabling or interfaces leaving a secure enclave must be encrypted.
- Equipment must comply with TEMPEST requirements.

B.9 UC SECURE PRESET CONFERENCE

This section provides descriptions of network configuration requirements that will enable SBU voice subscribers equipped with an NSA Type I encryption device to conference in the secure mode.

B.9.1 Introduction

The DoD voice community has a 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.

B.9.2 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 following ways:

- In the secure mode with multiple subscribers who are equipped with interoperable NSA devices on a preset Directory Number (DN) assigned to the originator to initiate the session.
- With multiple subscribers equipped with interoperable NSA devices on a "meet-me" basis.
- 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 B.9-1, Examples of Current Secure Interface Arrangements, and Figure B.9-2, 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.

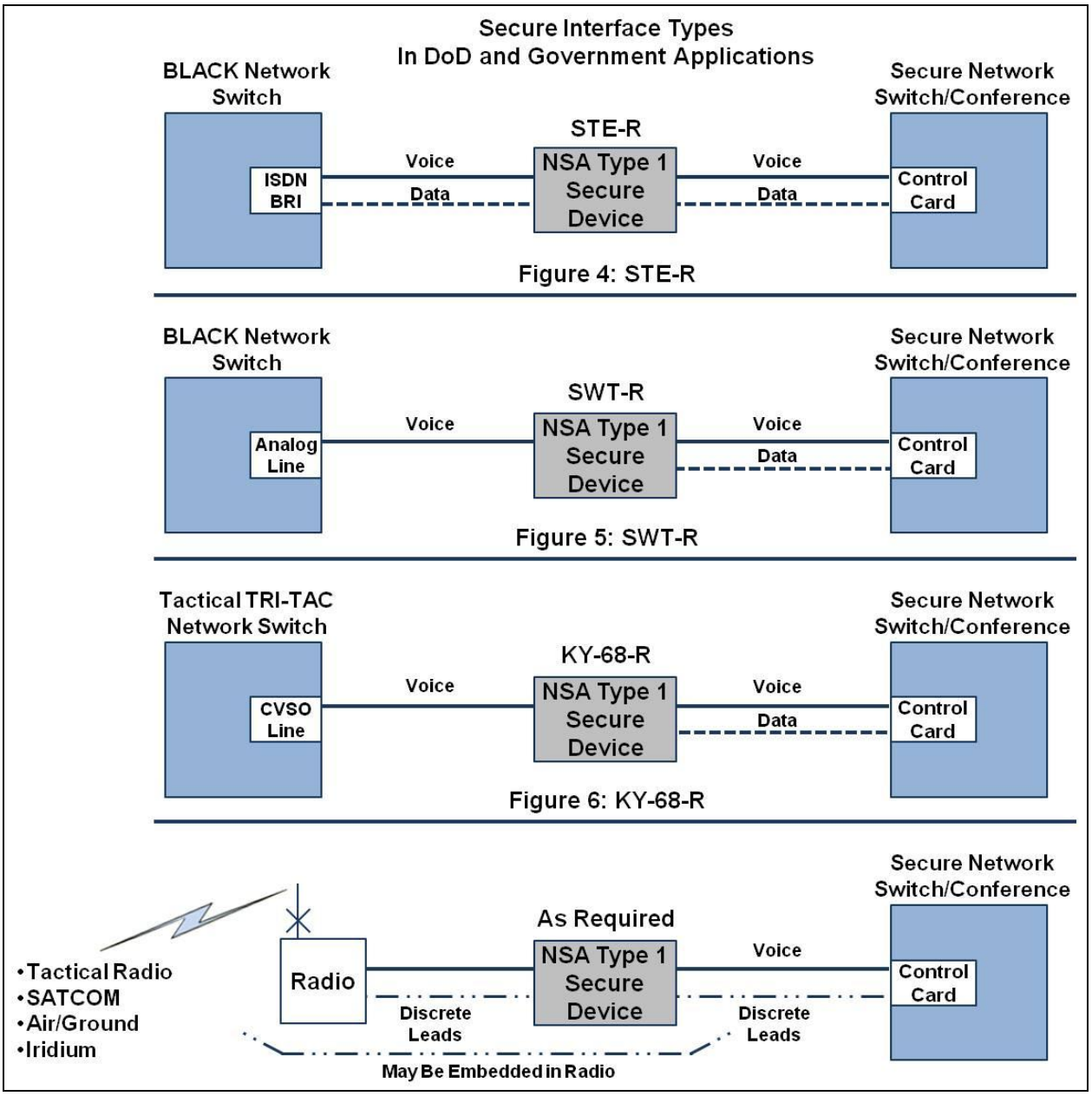

Figure B.9-1. Examples of Current Secure Interface Arrangements

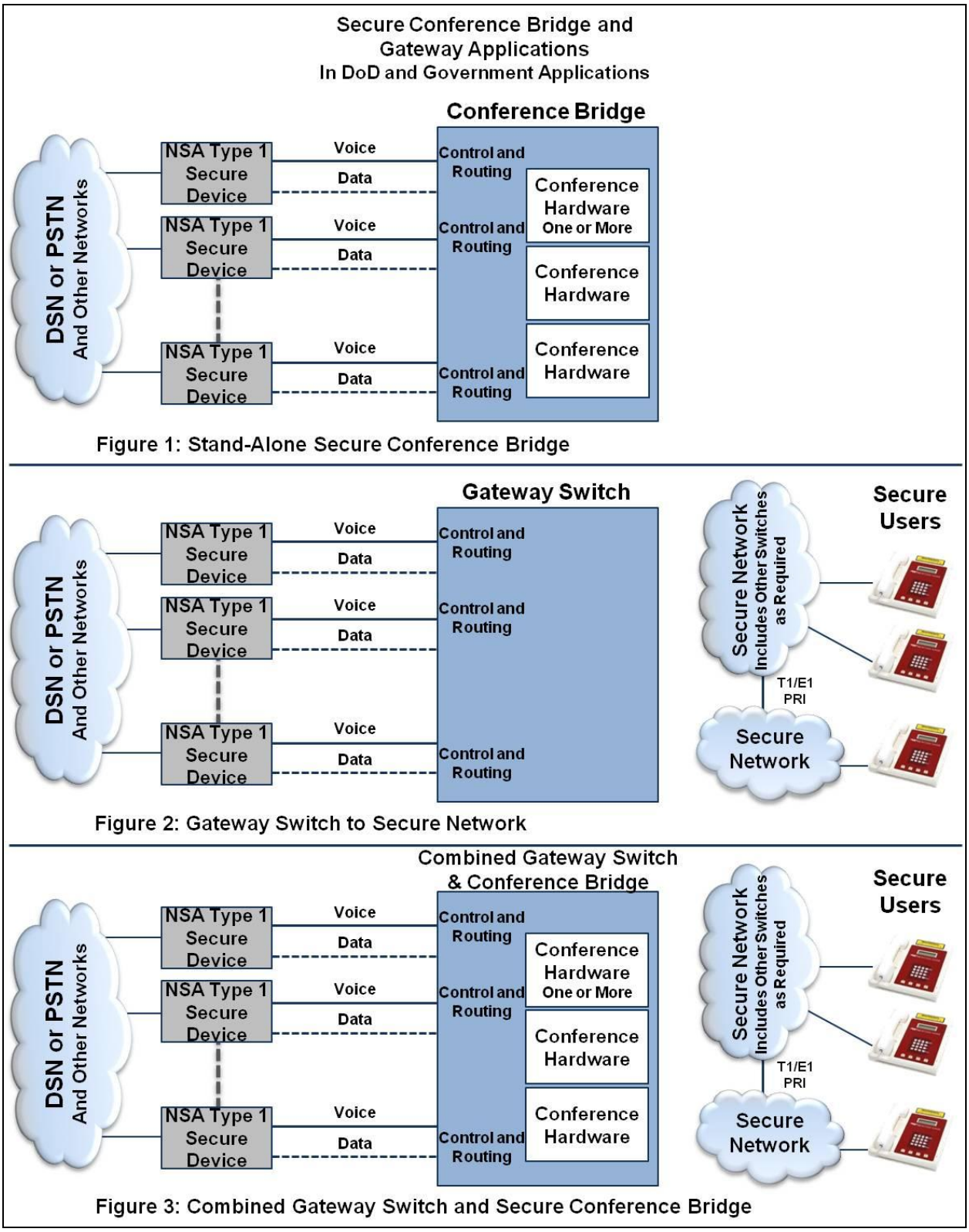

Figure B.9-2. Additional Examples of Current Secure Interface Arrangements

B.9.3 UC SBU Voice Secure Conference Features

(Features listed in this section are in addition to the features listed in, Section 3.4, UC Audio and Video Conference System Requirements).

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

B.9.3.1 Feature Description

The secure conference bridge system (preset or meet-me) is equipped with individual ports with automated supervision and control interfaces that conform to standard telephony two-wire loop (DS0 minimum rate of 56 Kbps) (IAW Telcordia Technologies GR-506-CORE). The system is 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. 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 Dual Tone Multifrequency (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 where 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 IAW 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.

B.9.4 UC Preset Conference Bridge Requirements

The bridge shall provide the following capabilities (see the notional diagram in Figure B.9-3, Secure Preset Conference Capability):

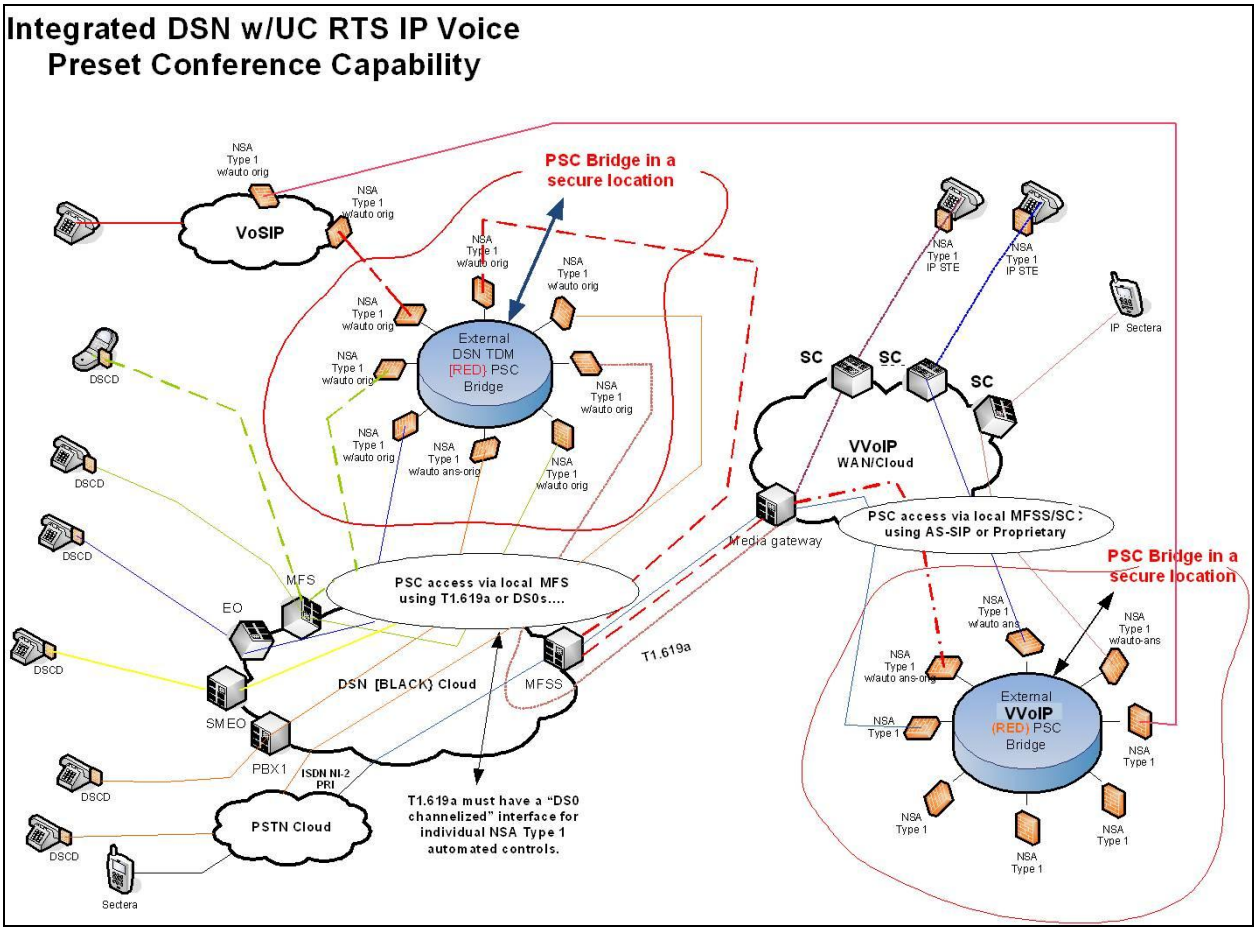

Figure B.9-3. Secure Preset Conference Capability

1. All bridge port access shall be via an NSA Type I-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 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 Section 3.4) 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 Section 3.4) 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 allow for remote or 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 I device.
15. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be 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 I 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 be activated and put in-service only when it is connected serially with a NSA Type I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

B.9.5 UC Secure Meet-Me Conference Bridge Requirements

In addition to the requirements stated in Section 3.4, the bridge shall have the following capabilities (see Figure B.9-4, Secure Meet-Me Conference Arrangement, for a notional diagram):

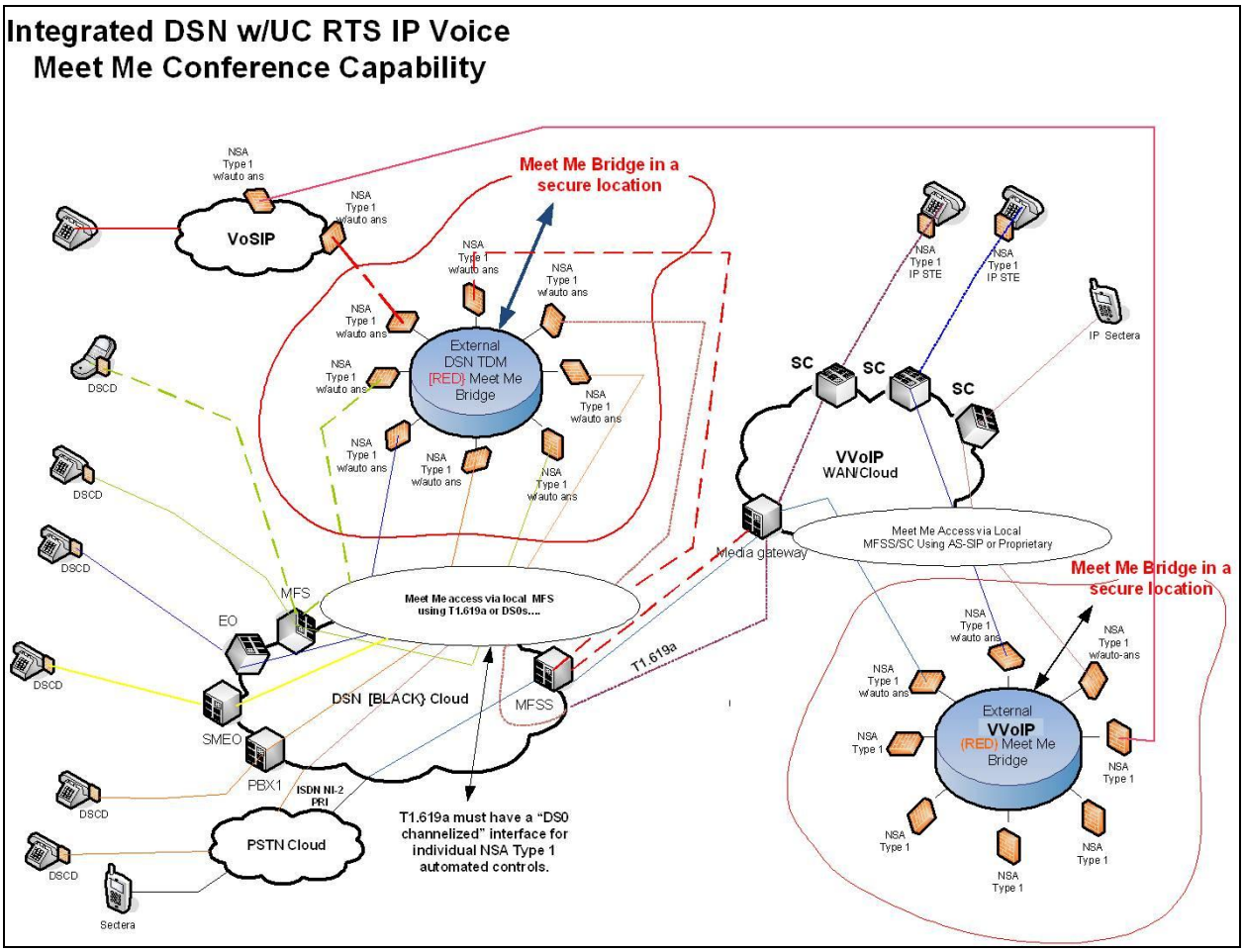

Figure B.9-4. Secure Meet-Me Conference Arrangement

1. All bridge port access shall be via an NSA Type I-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 allow for remote or 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 an NSA Type I 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 I device.

7. Each bridge DS0 port (originating and terminating ports) shall interface with an NSA Type I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be 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 I 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 be activated and put in-service only when it is connected serially with an NSA Type I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).

B.9.6 UC Secure Network Gateway Requirements

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

B.9.6.1 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 or 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 IAW 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 B.9-5, Notional Diagram Illustrating Secure Network Gateway, for a notional diagram):

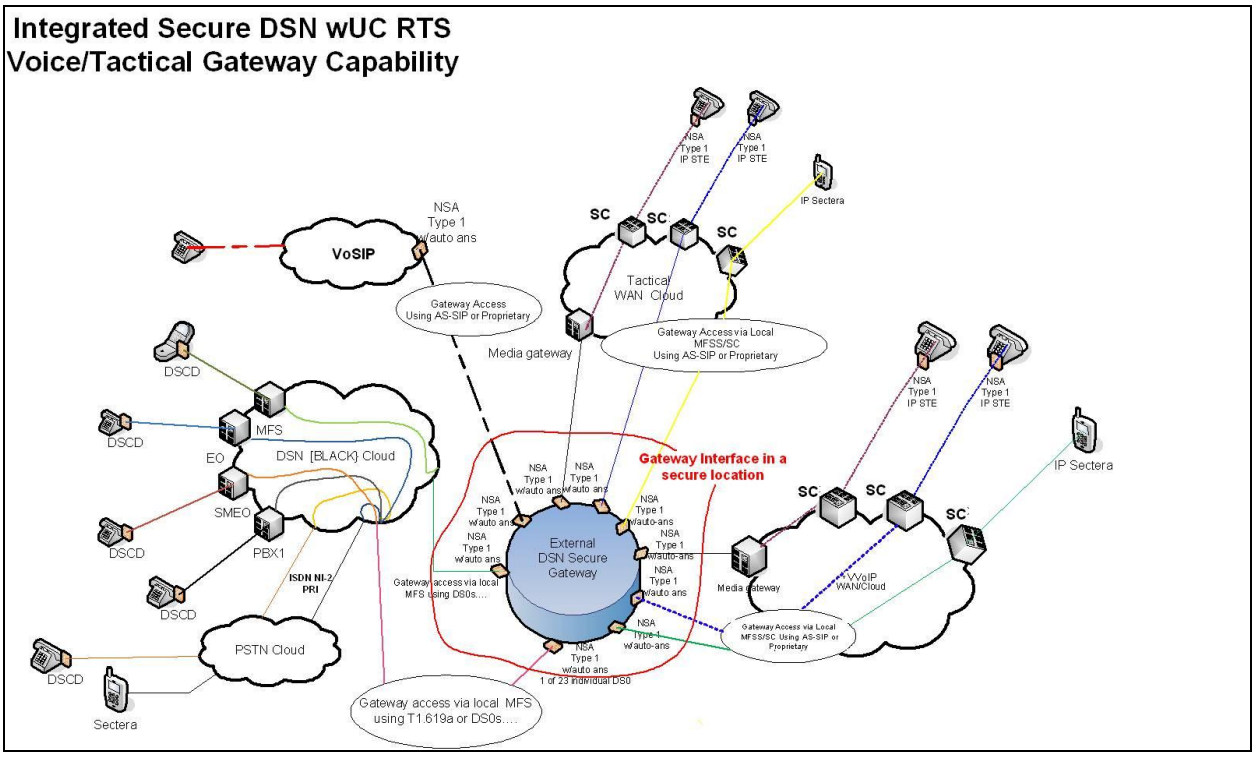

Figure B.9-5. Notional Diagram Illustrating Secure Network Gateway

1. All gateway interface port access shall be via an NSA Type I-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 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 I encryption device that provides a fully automated supervision (answer and cut-through) control (this supervision control either can be 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 I 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.

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. The interface 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 or 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 synchronized cryptographically 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 synchronized cryptographically 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 allow for remote or 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 I 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 IAW 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 I encryption device (either automated provisioning or manual provisioning is allowed to provide the control).