Changes to UCR 2008, Change 2, made by UCR 2008, Change 3 Section 5.4, Information Assurance Requirements

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2 #1.a	Removed due to overlap with STIG requirement VVoIP 1050	Immediate
5.4.6.2 #1.c	Removed due to overlap with STIG requirement VVoIP 1200	Immediate
5.4.6.2 #1.c.1	Changed from Required to Conditional clarified that the signature on software must be verified prior to installation	18 months
5.4.6.2 #3	Removed due to overlap with STIG requirement APP 3700	Immediate
5.4.6.2 #5	Removed due to overlap with STIG requirement VVT/VTC 1000	Immediate
5.4.6.2 #9	Removed due to overlap with STIG requirement VVoIP 1015	Immediate
5.4.6.2.1.1 #1	Removed due to overlap with STIG requirement NET 0340 and APP 3440	Immediate
5.4.6.2.1.1 #1.a	Removed due to overlap with APP 3340	Immediate
5.4.6.2.1.1 #1.b	Removed due to overlap with APP 3340	Immediate
5.4.6.2.1.1 #1.d	Removed due to overlap with STIG requirement NET 0340 and APP 3440	Immediate
5.4.6.2.1.1 #1.e	Removed due to overlap with STIG requirement NET 0340 and APP 3440	Immediate
5.4.6.2.1.1 #1.f	Removed due to overlap with STIG requirement APP 3660	Immediate
5.4.6.2.1.1 #1.f.1	Removed due to overlap with STIG requirement APP 3650, APP 3660, APP 3670, APP 3680, APP 3690	Immediate
5.4.6.2.1.1 #1.f.2	Removed due to overlap with STIG requirement APP 3320, APP 3330, APP 3340, APP 3350, APP 3360, APP 3370, APP 3380, APP 3390, APP 3400, APP 3405, APP 3410, APP 3415, APP 3420, APP 3430	Immediate
5.4.6.2.1.2 #1.b	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.1	Removed due to overlap with STIG requirement APP 3310	Immediate
5.4.6.2.1.2 #1.b.2	Removed due to overlap with STIG requirement APP 3330 and APP 3340	Immediate
5.4.6.2.1.2 #1.b.2.a	Removed due to overlap with STIG requirement APP 3330 and APP 3340	Immediate
5.4.6.2.1.2 #1.b.3	Removed due to overlap with STIG requirement APP 3340	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.2 #1.b.4	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.4.a	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.4.b	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.6	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.6.a	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.6.b.ii.B	Removed because this STIG requirement no longer exists in the DRSN STIG, which was the original basis for this UCR requirement.	Immediate
5.4.6.2.1.2 #1.b.7	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.7.a	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.8	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.8.a	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.8.b	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.8.c	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.8.d	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.b.9	Removed due to overlap with STIG requirement APP 6220	Immediate
5.4.6.2.1.2 #1.b.9.a	Removed due to overlap with STIG requirement APP 6220	Immediate
5.4.6.2.1.2 #1.b.9.b	Removed due to overlap with STIG requirement APP 6220	Immediate
5.4.6.2.1.2 #1.b.9.c	Removed due to overlap with STIG requirement APP 6220	Immediate
5.4.6.2.1.2 #1.b.11	Removed due to overlap with STIG requirement APP 3350	Immediate
5.4.6.2.1.2 #1.b.12	Removed due to overlap with STIG requirement APP 3660	Immediate
5.4.6.2.1.2 #1.b.13	Removed due to overlap with STIG requirement APP 3660	Immediate
5.4.6.2.1.2 #1.c	Removed due to overlap with STIG requirement APP 3380	Immediate
5.4.6.2.1.2 #1.d	Removed due to overlap with STIG requirement APP 3380	Immediate
5.4.6.2.1.2 #1.d.1	Removed due to overlap with STIG requirement APP 3380	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.2 #1.f.3	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.2 #1.h	Removed due to overlap with STIG requirement APP 3410	Immediate
5.4.6.2.1.2 #1.i	Removed due to overlap with STIG requirement APP 3390	Immediate
5.4.6.2.1.2 #1.i.2	Removed due to overlap with STIG requirement APP 3400	Immediate
5.4.6.2.1.2 #1.i.2.a	Removed due to overlap with STIG requirement APP 3400	Immediate
5.4.6.2.1.2 #1.i.3	Clarified that “real time” means within “30 seconds”	18 months
5.4.6.2.1.2 #1.i.4	Removed due to overlap with STIG requirement APP 3390	Immediate
5.4.6.2.1.3 #1.h	Removed due to overlap with STIG requirement APP 3450 and APP 3470	Immediate
5.4.6.2.1.3 #1.h.3.h	Removed due to overlap with STIG requirement APP 3380	Immediate
5.4.6.2.1.3 #1.h.3.n	Removed due to overlap with STIG requirement APP 3340	Immediate
5.4.6.2.1.3 #1.i	Removed due to overlap with STIG requirement APP 3500	Immediate
5.4.6.2.1.3 #1.j	Removed due to overlap with STIG requirement APP 3330	Immediate
5.4.6.2.1.3 #1.q	Updated requirement to reflect that remote administration is a requirement for devices beyond just FW, IPS, VPN, and NAC	18 months
5.4.6.2.1.3 1.h.3.y	Removed due to overlap with APP 3690	Immediate
5.4.6.2.1.3 1.r.1.g	Removed due to lack of clarity	Immediate
5.4.6.2.1.3 1.r.3.b	Removed because the “modify security functions” requirement belongs to the System Administrator, not the Cryptographic Administrator.	Immediate
5.4.6.2.1.4 #1.e.1.a	Removed due to overlap with STIG requirement NET-NAC-010	Immediate
5.4.6.2.1.4 #1.e	Changed to require the use of 802.1X-2010 instead of 802.1X-2004	18 months
5.4.6.2.1.5 #1.a	Removed due to overlap with STIG requirement APP 3300 and APP 3280	Immediate
5.4.6.2.1.5 #1.a.1	Removed due to overlap with STIG requirement APP 3330	Immediate
5.4.6.2.1.5 #1.a.2	Removed due to overlap with STIG requirement APP 3280	Immediate
5.4.6.2.1.5 #1.a.2.a	Removed due to overlap with STIG requirement APP 3280	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.5 #1.a.2.b	No change to requirement. Minor wording change in parenthetical.	Immediate
5.4.6.2.1.5 #1.b	Removed due to overlap with STIG requirement APP 3290	Immediate
5.4.6.2.1.5 #1.b.1	Removed due to overlap with STIG requirement APP 3290	Immediate
5.4.6.2.1.5 #1.b.2	Removed due to overlap with STIG requirement APP 3290	Immediate
5.4.6.2.1.5 #1.c	Removed due to overlap with STIG requirement APP 3680, APP 3480, APP 3690	Immediate
5.4.6.2.1.5 #1.d	Removed due to overlap with STIG requirement APP 3510, APP 3350	Immediate
5.4.6.2.1.5 #1.g	Split this requirement into 1.g and 1.g.1 in this section so that the emergency calling requirement could be assigned a higher severity level.	Immediate
5.4.6.2.1.5 #1.g.1	Same requirement that was previously captured in 1.g, however the emergency calling portion of UCR 2008 Change 2 1.g was moved here so that it could be assigned a higher severity level.	Immediate
5.4.6.2.1.5 #1.f	Removed due to overlap with STIG requirement APP 3220, APP 3340, APP 3360	Immediate
5.4.6.2.1.6 #1	Removed due to overlap with STIG requirement APP 3290, APP 3280, and APP 3300	Immediate
5.4.6.2.1.6 #1.a.2.a	Removed due to overlap with STIG requirement APP 3150	Immediate
5.4.6.2.1.6 #1.b.1	Removed due to overlap with STIG requirement APP 3220	Immediate
5.4.6.2.1.6 #1.b.2	Removed due to overlap with STIG requirement APP 3220	Immediate
5.4.6.2.1.6 #1.b.2.a	Removed due to overlap with STIG requirement APP 3180	Immediate
5.4.6.2.1.6 #1.b.2.c	Removed due to overlap with STIG requirement APP 3220	Immediate
5.4.6.2.1.6 #1.b.2.d	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.6 #1.b.2.e.i	Minor clarification of wording, no material change in the requirement	18 months
5.4.6.2.1.6 #1.c	Removed due to overlap with STIG requirement APP 3320	Immediate
5.4.6.2.1.6 #1.e	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.e.3	Removed due to overlap with STIG requirement APP3290	Immediate
5.4.6.2.1.6 #1.e.3.b	Added clarifying note indicating that use of a local CRL Distribution Point is still acceptable	18 months

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.6 #1.e.3.c	Requirement for products that use OCSP to support the delegated trust model (DTM) is unchanged. However, updated the requirement to reflect that both the DTM and the OCSP Trusted Responder (OCSP uses self-signed certificate) model need to be supported. In addition, changed the effective date to be Immediate instead of 18 months from UCR 2008 Change 2. All UC APL solutions that use OCSP must now support OCSP DTM in order interoperate with DoD PKI OCSP responders in the field.	Immediate
5.4.6.2.1.6 #1.f	Removed due to overlap with STIG requirement APP 3290	Immediate
5.4.6.2.1.6 #1.f.2	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.1	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.2	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.4	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.4.a	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.4.b	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.4.c	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.g.4.d	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.h.2.a	Removed due to overlap with STIG requirement APP 3305	Immediate
5.4.6.2.1.6 #1.i	Added clarifications to this requirement	18 months from publication of UCR 2008 Change 2
5.4.6.2.1.6 #1.j.2	Removed FW, IPS, VPN, and NAC from this requirement since this requirement is focused towards VVoIP devices	Immediate
5.4.6.2.1.6 #1.j.4	Changed from conditional requirement to non-conditional.	18 months
5.4.6.2.1.6 #1.j.5	Added requirement to ensure that identities claimed by a SIP Address of Record and sip.instance (RFC 5626) media feature tag are mapped to the TLS certificate Subject Common Name field.	18 months
5.4.6.2.1.7 #1	Removed due to overlap with STIG requirement APP 3480	Immediate
5.4.6.2.1.7 #1.a	Removed due to overlap with STIG requirement APP 3480	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.7 #1.b	Removed due to overlap with STIG requirement APP 3220	Immediate
5.4.6.2.1.7 #1.c	Removed due to overlap with STIG requirement NET 0162	Immediate
5.4.6.2.1.7 #1.d.2	Removed due to overlap with STIG requirement NET-VLAN-010	Immediate
5.4.6.2.1.7 #1.d.2.c.i	Removed due to overlap with STIG requirement VVoIP 5700	Immediate
5.4.6.2.1.7 #1.d.2.d	Removed due to overlap with STIG requirement NET 1433	Immediate
5.4.6.2.1.7 #1.d.2.d.ii	Removed due to overlap with STIG requirement NET-NAC-032	Immediate
5.4.6.2.1.7 #1.d.2.e	Removed due to overlap with STIG requirement NET-VLAN-010	Immediate
5.4.6.2.1.7 #1.d.2.f	Removed due to overlap with STIG requirement NET-VLAN-010	Immediate
5.4.6.2.1.7 #1.d.2.g	Removed due to overlap with STIG requirement NET-VLAN-010	Immediate
5.4.6.2.1.7 #1.d.2.h	Removed due to overlap with STIG requirement NET-VLAN-010	Immediate
5.4.6.2.1.7 #1.d.3	Removed due to overlap with STIG requirement VVoIP 5200	Immediate
5.4.6.2.1.7 #1.d.3.b	Removed due to overlap with STIG requirement NET 0910	Immediate
5.4.6.2.1.7 #1.d.3.c	Removed due to overlap with STIG requirement VVoIP 1005	Immediate
5.4.6.2.1.7 #1.d.4	Removed due to overlap with STIG requirement VVoIP 5210, VVoIP 5235, VVoIP 5210	Immediate
5.4.6.2.1.7 #1.d.5	Removed due to overlap with STIG requirement VVoIP 5210, VVoIP 5235	Immediate
5.4.6.2.1.7 #1.d.5.a.i	Removed due to overlap with STIG requirement AC34.045	Immediate
5.4.6.2.1.7 #1.d.5.a.ii	Removed due to overlap with STIG requirement AC34.050	Immediate
5.4.6.2.1.7 #1.a	Removed because Section 5.3 already extensively covers this requirement	Immediate
5.4.6.2.1.7 #1.e	Removed due to overlap with STIG requirement VVoIP 1020, VVoIP 1021	Immediate
5.4.6.2.1.7 #1.e.1	Removed due to overlap with STIG requirement VVoIP 1020, VVoIP 1021	Immediate
5.4.6.2.1.7 #1.f	Removed due to overlap with STIG requirement APP 3480, APP 3360	Immediate
5.4.6.2.1.7 #1.f.1	Removed due to overlap with STIG requirement APP 3480, APP 3360	Immediate
5.4.6.2.1.7 #1.f.2	Removed due to overlap with STIG requirement APP 3480	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.1.7 #1.l.1	Minor revision clarifying that the requirement is applicable to the emergency port	Immediate
5.4.6.2.1.7 #1.o	Removed due to overlap with STIG requirement APP 3415	Immediate
5.4.6.2.1.7 #1.o.1	Removed due to overlap with STIG requirement NET 1624 NET 1639	Immediate
5.4.6.2.1.7 #1.o.2	Removed due to overlap with STIG requirement AC34.205	Immediate
5.4.6.2.1.7 #1.o.3	Removed due to overlap with STIG requirement APP 3415	Immediate
5.4.6.2.1.7 #1.p	Removed due to overlap with STIG requirement APP 3420	Immediate
5.4.6.2.1.7 #1.p.1	Removed due to overlap with STIG requirement APP 3430	Immediate
5.4.6.2.1.7 #1.p.2	Removed due to overlap with STIG requirement APP 3420	Immediate
5.4.6.2.1.7 #1.p.3	Removed due to overlap with STIG requirement APP 3405	Immediate
5.4.6.2.1.7 #1.q	Removed due to overlap with STIG requirement DSN18.14	Immediate
5.4.6.2.1.7 #1.r	Removed due to overlap with STIG requirement NET 1617	Immediate
5.4.6.2.1.7 #1.r.1	Removed due to overlap with STIG requirement NET 1617	Immediate
5.4.6.2.1.7 #1.r.2	Removed due to overlap with STIG requirement NET 1617	Immediate
5.4.6.2.1.7 #1.r.3	Removed due to overlap with STIG requirement APP 6250	Immediate
5.4.6.2.1.7 #1.r.4	Removed due to overlap with STIG requirement APP 3360	Immediate
5.4.6.2.1.7 #1.r.5	Removed due to overlap with STIG requirement APP 3450	Immediate
5.4.6.2.1.7 #1.s	Removed due to overlap with STIG requirement APP 3240	Immediate
5.4.6.2.2 #1.b.3	Removed due to overlap with STIG requirement APP 3510	Immediate
5.4.6.2.2 #1.b.6	Removed due to overlap with STIG requirement APP 3510	Immediate
5.4.6.2.2 #1.c.1	Removed due to overlap with STIG requirement APP 3130, APP 3140	Immediate
5.4.6.2.2 #1.e	The portion of the requirement specific to alarming for “critical errors” was removed because the requirement was too vague (no specific definition of the critical error) and not testable as written.	Immediate
5.4.6.2.2 #1.i	Removed due to overlap with STIG requirement APP 3150, APP 3260	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.2 #1.j	Removed due to overlap with STIG requirement APP 3130, APP 3550	Immediate
5.4.6.2.2 #1.j.1	Removed due to overlap with STIG requirement APP3130, APP6050, APP3550, APP3580, APP3570, APP3560, APP3590	Immediate
5.4.6.2.2 #1.l	Removed due to overlap with STIG requirement APP 3360	Immediate
5.4.6.2.3 #1.c.2.k	Moved from Section 5.4 to Section 5.3.4	Immediate
5.4.6.2.3 #1.c.2.k.i	Moved from Section 5.4 to Section 5.3.4	Immediate
5.4.6.2.3 #1.c.2.k.ii	Moved from Section 5.4 to Section 5.3.4	Immediate
5.4.6.2.3 #1.h.2	Minor wording change with no substantive impact to the requirement.	Immediate
5.4.6.2.3 #1.i	Removed due to overlap with STIG requirement APP 3360, APP 3450, APP 3460	Immediate
5.4.6.2.3 #1.j	Removed due to overlap with STIG requirement NET 1638, NET 1637	Immediate
5.4.6.2.3 #1.j.1	Removed due to overlap with STIG requirement NET 1637	Immediate
5.4.6.2.3 #1.j.2	Removed due to overlap with STIG requirement NET 1002	Immediate
5.4.6.2.4 #1.a	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.1	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.2	Removed due to overlap with STIG requirement APP 3690	Immediate
5.4.6.2.4 #1.b.2.a	Removed due to overlap with STIG requirement APP 3690	Immediate
5.4.6.2.4 #1.b.2.b	Removed due to overlap with STIG requirement APP 3690	Immediate
5.4.6.2.4 #1.b.3.a	Removed due to overlap with STIG requirement APP 3650	Immediate
5.4.6.2.4 #1.b.6.a	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.b	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.e	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.i	Removed due to overlap with STIG requirement APP 3680	Immediate

SECTION(S)	CORRECTION	EFFECTIVE DATE
5.4.6.2.4 #1.b.6.k	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.l	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.l.i	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.l.ii	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.l.iii	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.l.iv	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.m	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.6.q	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7.a	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7.b	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7.c	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7.d	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.4 #1.b.7.e	Removed due to overlap with STIG requirement APP 3680	Immediate
5.4.6.2.3 #1.g.3.b.i	Changed to require support for certain key types defined in RFC 6187 instead of the older draft RFC.	18 months
5.4.6.2.3 #1.g.3.b.ii	Changed requirement to require the ability to prioritize a preferred key type in a configurable manner.	18 months
5.4.6.2.3 #1.g.3.b.iii	Changed requirement to require support for denial of SSH sessions when the preferred key type cannot be negotiated	18 months
5.4.6.2.3 #1.g.3.c.iii	Changed to require support for certain key types defined in RFC 6187 instead of the older draft RFC.	18 months
5.4.6.2.4 #1.e	Reworded to provide minor clarification as to what is required to be supported when the audit function initiates and shuts down	18 months
5.4.6.3	Requirements moved from Section 5.4 into new Section 5.3.6, Multifunction Mobile Devices. Changed UC_Smartphone_App to UC_MMD_App. Replaced ‘smartphone’ term with ‘Multifunction Mobile Device’. Replaced Smartphone Backend Support System with Multifunction Mobile Device Backend Support System.	Immediate

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

5.4 INFORMATION ASSURANCE REQUIREMENTS

5.4.1 Section Overview and Scope

Information Assurance is the practice of providing confidentiality, integrity, and availability for information transiting, processed, and stored within an information system. Historically, this UCR section had addressed the Information Assurance requirements for only the Unified Capabilities (UC) Voice and Video over IP (VVoIP) and UC federated collaboration/XMPP components. These components include but are not limited to softswitches (SSs), local session controllers (LSCs), edge boundary controllers (EBCs), and end instruments (EIs). While VVoIP Information Assurance remains a key focus area, over time this section has been expanded to incorporate the general Information Assurance requirements for additional UC APL products. This section of the UCR now incorporates the general information assurance requirements for a number of UC APL "Security Devices," generally considered to be "Information Assurance Products" in accordance with DoDD 8500.1, which include network based firewalls (FWs), intrusion prevention systems (IPSs), virtual private network (VPN) servers, and network access controllers (NACs). More information on Security Devices can be found in Section 5.8, Security Devices Requirements, which specifies the "security-device-unique" functional requirements for these products.

This revision of UCR Section 5.4 also removes a large number of requirements which were determined to overlap the information assurance requirements found in DISA FSO Security Technical Implementation Guides (STIGs) directly. In order to preserve the requirement mapping to test plans, each removed requirement has been replaced with "Reserved." Since both the UCR and STIGs are utilized during testing, the intent is to minimize redundancy in information assurance test procedures and reports. As a general rule, if in the future the UCR is found to duplicate STIG requirements (as STIGs are frequently updated faster than the UCR) during testing, Action Officers at the DoD approved test facilities in combination with the appropriate DISA Program Management Office (PMO) representatives will determine if the UCR requirement should remain applicable. This will be done on a case-by-case basis.

5.4.2 VVoIP Information Assurance Requirements Structured Process

This section provides an overview of the VVoIP Information Assurance design and specifies the VVoIP Information Assurance requirements using a defined, structured process in order to secure the VVoIP system. The process is called the Information Assurance Process, shown in Figure 5.4.2-1, because it applies to any Information Assurance design. A basic tenet of this process is that threats are the primary driver for all stages of the Information Assurance Process. However, it is recognized that these systems may be influenced by other drivers, such as political, time, and technical motivators. This section is structured to follow the Information Assurance Process in the development of the VVoIP Information Assurance design and requirements.

The first step in the Information Assurance process is to document the threats based on a preliminary understanding of how the system will be deployed and in conformance with the DoD high-level Information Assurance requirements. A summary of the threats is provided in this UCR section, but the details of the threats are found in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," Version 3.4, DoD RTS Information Assurance Working Group, 22 May 2009.

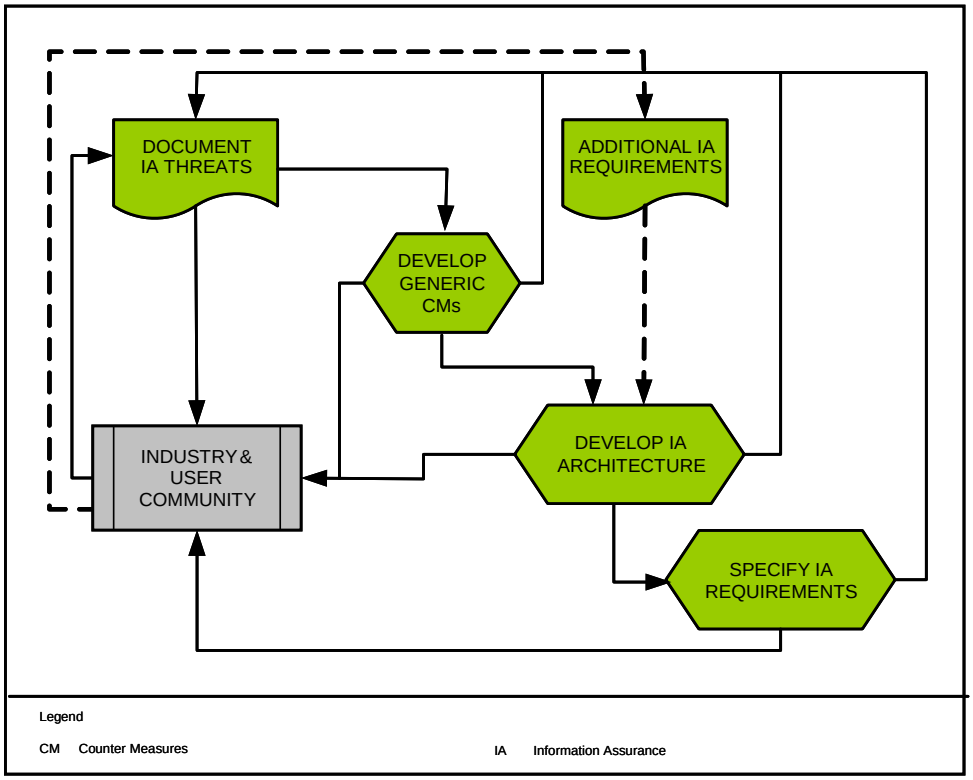

Figure 5.4.2-1. Information Assurance Process

In creating this section of the UCR, the threats were vetted with industry and the user community to get user buy-in and to ensure that all known threats were documented. An example of a threat is eavesdropping on the media stream of a telephone call to hear the contents of a conversation. After the threats were documented, the risks associated with each threat were classified based on the likelihood of a successful attack and the impact of a successful attack. The classification of the risks permitted the prioritization of resources to mitigate the risks during the development of the Information Assurance design.

Based on the threats, a set of generic countermeasures (CMs) was developed. A summary of the CMs is discussed in the main body of the UCR, but the details of the CMs are found in "DoD RTS Information Assurance Countermeasures," Version 0.7, DoD RTS Information Assurance Working Group, 29 March 2006. The reason generic CMs were developed, instead of specific

CMs, is that it allows for maximum flexibility in selecting an approach to implement the countermeasure. Encryption of the media stream is an example of a generic countermeasure, which would mitigate the threat associated with eavesdropping on the media stream. In defining the generic CMs, it is important to understand the interdependence of the CMs and document those interdependencies.

For example, confidentiality without authentication and authorization diminishes its benefit. In addition, it is important to map threats to CMs to ensure all threats are addressed. As with the threats, the generic CMs were vetted with industry and the user community to determine if they were feasible and to get user buy-in.

The next step was to develop an Information Assurance design based on the generic CMs and threats. The first step in the development of the Information Assurance design was to identify candidate mechanisms that satisfy the CMs and mitigate the threats. For example, confidentiality of the bearer stream could be achieved by implementing the SRTP, IPSec, or Type 1 point-to-point bulk encryption. The candidates were vetted with the user community and industry before selecting the default solution(s) for the Information Assurance design. Alternative solutions were allowed in specific cases, but a default solution was specified to ensure multivendor interoperability. In addition, although the threats and generic CMs were the primary driver of the Information Assurance design, political, time, and technical motivators also influenced the Information Assurance design and requirements, and they were incorporated into the Information Assurance design.

After the design was completed, the final step in the Information Assurance Process involved documenting the requirements necessary to achieve the Information Assurance design in a multivendor interoperable integrated environment that could be tested. An example of a requirement is that the system shall use SRTP for encrypting the media stream. As with the threats and CMs, the requirements were vetted with industry and the user community to ensure that the requirements were clear, concise, and achievable within the timeframe allocated.

The requirements are loosely grouped by their Information Assurance category. The Information Assurance categories are defined in DoDD 8500.1. The Information Assurance categories are similar to the Information Assurance services described in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," with one exception. The one exception is that unlike the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," DoDD 8500.1 does not have a separate category for authorization, and it includes the functions associated with authorization and access control in the authentication category. The "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment" is a reference document for the UCR and provides an Information Assurance analysis of the protocols, traceability of the DoD Information Assurance requirements, and a threat analysis of

the VVoIP design. This document does not provide that background information and instead focuses on the requirements with an overview of the threats.

Table 5.4.2-1, Mapping of Security Services to Security Categories and Goals, shows a mapping of the security services in the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and the security categories in DoDD 8500.1. For completeness, the table also maps the security services to the ETSI Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Protocols Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis, which provides a basis for the threat analysis used in this section and is discussed later.

Table 5.4.2-1. Mapping of Security Services to Security Categories and Goals

"ANALYSIS OF INFORMATION ASSURANCE REQUIREMENTS AND THREATS FOR THE DoD VVoIP ENVIRONMENT" SECURITY SERVICES	DoDD 8500.1 CATEGORIES	ETSI TS 102 165-1 GOALS
Authorization	Authentication (Includes Authorization and Access Control)	Accountability (Includes Non-Repudiation)
Authentication		
Non-Repudiation	Non-Repudiation	
Confidentiality	Confidentiality	Confidentiality
Integrity	Integrity	Integrity
Availability	Availability	Availability

This section concludes with a discussion of the threats and the extent to which they have been mitigated by enforcing the requirements and implementing the CMs. In addition, a brief discussion of the outstanding Information Assurance design issues is discussed. This section is a companion document to the STIGs, which are produced by the DISA FSO, and the intent is for this section to complement the STIGs. For instance, the UCR specifies the Information Assurance requirements that a VVoIP product must meet to be sold to DoD users. The STIGs specify the configurations that a DoD user must implement to ensure that the system is deployed in a secure manner.

5.4.3 Non-Mitigated Risks

The threat matrix used by the DISN IP VVoIP is based on the one developed by the ETSI TS 165-1. Where necessary it has been modified to reflect the threats that are unique to the DoD environment due to the issues raised in "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," which also provides a complete discussion of the threats associated with each protocol. The threat matrix was developed to permit a prioritization of the risks associated with those threats to target the most urgent threats. It was developed with the knowledge that it is impossible to prevent all attacks, but it is possible to limit the avenues of attack and to react to an attack in an expeditious manner.

The threats identified by the ETSI TIPHON work are focused on the nonphysical threats and do not address the physical threats to the system or all the threats that might arise from the interaction with ancillary equipment (i.e., equipment external to the system such as an external DHCP server).

The TIPHON threats are extracted from ETSI TS 101 165-1 and additional detail is provided in the following paragraphs. These threats are summarized in Table 5.4.3-1, TIPHON Threats. The "Xs" in Table 5.4.3-1 indicate that the threat affects the Information Assurance goal and must be mitigated to achieve that goal.

Table 5.4.3-1. TIPHON Threats

THREAT	GOALS			
	CONFIDENTIALITY	INTEGRITY	ACCOUNTABILITY	AVAILABILITY
Masquerading	X	X	X	X
Unauthorized Access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of Service				X
NOTE: The Xs indicate that the threat affects the Information Assurance goal and must be mitigated to achieve that goal.				

Masquerading or spoofing is the act of pretending to be someone you are not. This threat is often used to get information, deny a service, pervert a service, or misdirect a call. As shown in Table 5.4.3-1, TIPHON Threats, masquerading is a system threat to confidentiality, integrity, accountability, and availability. It is used also to introduce other threats to the system, such as unauthorized access or forgery, eavesdropping, and denial of service (DoS).

Unauthorized access is the act of someone accessing data or services in violation of the security policy. The threat with unauthorized access is that an attacker may access personal information, large amounts of sensitive or unclassified information, or classified information in a database, or an attacker may be able to make precedence calls causing unnecessary network preemptions. As shown in Table 5.4.3-1, TIPHON Threats, unauthorized access is a threat to both confidentiality and integrity if the action is from within a system. In addition, it is a threat to accountability and availability regardless of where the attacker is located. The principal resultant threats associated

with unauthorized access are DoS, masquerading as a real user, and eavesdropping on other users.

Eavesdropping is a breach of confidentiality caused by the unauthorized monitoring of a communication. Typically, it is associated with the monitoring of a telephone call. Eavesdropping is often used to determine call patterns, gain knowledge of personal information, and to acquire the information necessary to masquerade as another authorized user.

Loss or corruption of data is an attack that compromises the integrity of data. Typically, it involves unauthorized deletion, insertion, modification, reordering, replay, or delay. The goals that are affected by loss or corruption of data are integrity, accountability, and availability. The loss or corruption of data on a call will affect the integrity of the call and may make the call unintelligible. If the call detail records are destroyed, the accountability for the call will be affected. Finally, if the loss or corruption of data is significant enough, it could result in a DoS, which would affect the availability of the system.

Repudiation occurs when a user involved in a session subsequently denies that the session took place. Non-repudiation is required by the DISN to prevent subscription fraud and to determine responsibility for NM actions. The security service associated with this threat is accountability. In the DoD environment, this threat is not as significant as some of the other threats, but is still a concern.

Forgery is the act of fabricating information, and then claiming that the information was received from or sent to another caller. The security goals affected by this threat are integrity and accountability. One possible scenario for forgery is that an attacker may pretend to be a subscriber and receive calls intended for a legitimate subscriber with no intent to alert the caller, although they may falsely acknowledge that the request was completed. A different situation would involve a subscriber pretending to be the forged subscriber for issuing orders that may negatively affect the operational capabilities of the call recipient.

The final threat is a DoS attack, which is typically associated with an attacker causing enough congestion on the network that a subscriber's calls cannot be completed or are degraded. In the converged networks planned for the DoD, this may involve either data or VVoIP type attacks. Of particular concern is a VVoIP attack that involves a high number of illegitimate above ROUTINE precedence calls preventing access to the network for legitimate above ROUTINE precedence VVoIP calls. A DoS attack can occur at all three layers: signaling, bearer, or NM. The principal security goal affected by this type of attack is availability and this vulnerability is more likely to occur in a converged network.

The next step after identifying the threats is to perform a risk analysis of the threats. The method used in the ETSI TIPHON risk model is to score each threat in terms of its likelihood of occurrence and its potential effect. The Threat Risk Score is the product of the likelihood of

occurrence and the impact scores. Table 5.4.3-2, ETSI TIPHON Threat Likelihood Scoring Criteria, and Table 5.4.3-3, ETSI TIPHON Threat Impact Scoring Criteria, are extracted from ETSI TS 102 165-1 and designate the scores that should be used for assessing the system risks.

Table 5.4.3-2 describes the scores that should be used for the likelihood of a particular threat.

Table 5.4.3-2. ETSI TIPHON Threat Likelihood Scoring Criteria

SCORE	LIKELIHOOD	DESCRIPTION
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to start the threat, or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

Table 5.4.3-3 describes the scores that should be used to determine the effect of a particular threat.

Table 5.4.3-3. ETSI TIPHON Threat Impact Scoring Criteria

SCORE	IMPACT	DESCRIPTION
1	Low	The concerned party is not harmed very strongly; the possible damage is low.
2	Medium	The threat addresses the interests of providers and subscribers and cannot be neglected.
3	High	A basis of business is threatened and severe damage might occur in this context.

Following the ETSI TIPHON model, the risk associated with each threat is divided into three categories and all risks scoring a six or nine require CMs. Although risks scoring four do not require CMs, they are still considered major risks and should be mitigated.

NOTE: The risk cannot score 5, 7, or 8 due to basic mathematics. Figure 5.4.3-1, ETSI TIPHON Threat Risk Score, shows the result of likelihood and impact scores on the overall risk score.

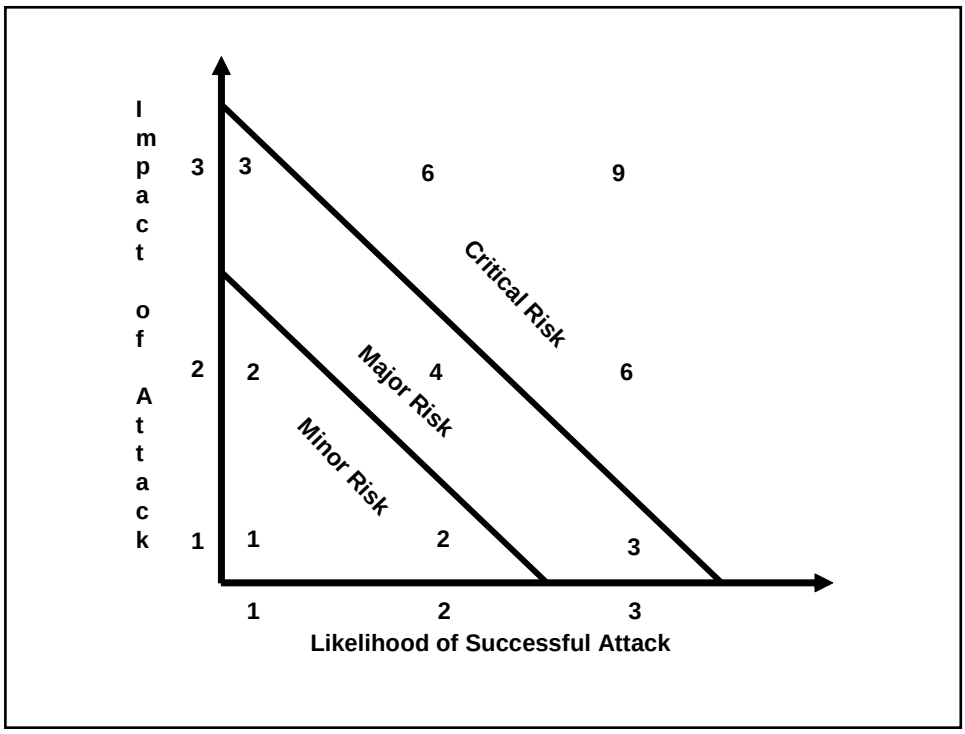

Figure 5.4.3-1. ETSI TIPHON Threat Risk Score

The UC Information Assurance team developed the initial scores and vetted the scores with the user community and industry. The scores are an average based on the feedback since every vendor's Information Assurance solution and every user's implementation is different.

Tables 5.4.3-4 through 5.4.3-12 are extracted from the "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," and summarize the risk assessments associated with the threats.

Table 5.4.3-4. General Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	2	2	4	Although the SBU voice service is a distinct network from the PSTN, most attacks do occur from inside the network. However, the effect is reduced due to the use of NSA certified devices for classified conversations and the use of encryption for all calls.
G2	Corruption of transport data	2	3	6	A user who can eavesdrop on the transport data can manipulate the data stream to issue false orders or to make the communication unintelligible.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	2	3	6	Encrypting all layers of the communication should reduce the likelihood. The ability to masquerade the telephone number makes the impact higher.
G4	Eavesdropping on the signaling data	2	3	6	SIP increases the likelihood of this attack. The information gained in this attack can be used to derive information for other attacks (e.g., a call teardown denial of service (DoS) attack). Call pattern tracking also allows for traffic analysis, which is an operations security (OPSEC) concern.
G5	Corruption of signaling data via malformed packets or protocol fuzzing	2	3	6	SIP increases the likelihood of this occurrence. The modification of the signaling data could be used to derive other types of attacks or for a DoS attack. Malformed messages are protocol messages with incorrect syntax; protocol fuzzing includes malicious messages with proper syntax. Protocol fuzzing interferes with message sequence, confusing the state machine. Unexpected protocol messages also can cause infinite loop parsing and system crashes, along with buffer overflows (see G22).
G6	Eavesdropping on NM traffic	2	1	2	The large number of tools available on the Internet makes this task easier, but the impact is minimal.
G7	Corruption of NM data	3	3	9	The closed loop approach to signaling involving the routers would make the impact of this attack high to the voice or video.
G8	Obtaining telephone number from VVoIP EI	3	2	6	This information could be used to discern the origination of calls, which can be used by enemies as intelligence.
G9	Denial of service	3	3	9	This is particularly important to voice or video due to the need for assured service for precedence calls. Examples include G11, G12, G21, G22, G23, and G30.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G10	Unauthorized access to data	1	3	3	The primary concern is unauthorized access to CDR. Nevertheless, the security in-depth approach used minimizes the likelihood of this occurring.
G11	Flooding the network	3	3	9	This item addresses flooding the network, which is an issue before, during, and after call setup. This is a type of DoS attack (see G9). See also valid/invalid registration flooding, valid/invalid call request flooding (see G21).
G12	Stolen terminals	3	3	9	In wartime and peacetime scenarios, it is likely that a terminal may be acquired by an enemy agent.
G13	Subscription and toll fraud	3	1	3	Since the DoD is a military organization, this is not as critical since the profit is not the only factor in the solution. This does not mean that it is not important as it relates to PSTN charges.
G14	Unauthorized access to NM or subscriber database	2	3	6	The prevention of the dissemination of the locations and sizes of units is critical to the safety of our forces.
G15	Unauthorized access to data in EIs	2	1	2	The EIs in the voice or video have limited usable data stored in them. If the EI stores private keys, then a possible threat is unauthorized access to the private key and additional related threats become possible.
G16	Masquerading as one legitimate subscriber or signaling device to another	3	3	9	In wartime and peacetime scenarios, it is likely that an enemy agent who gains access to the network will masquerade as a legitimate subscriber.
G17	Man-in-the-middle attack	3	3	9	Although this is an internal threat, the numerous shareware tools available to execute this attack make it likely and the impact is high due to the ability to redirect voice traffic and get access to user data.
G18	Repudiation of actions	2	2	4	The threat depends on the action taken and ability of the system to detect the action rapidly.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G19	Replay attack	1	2	2	This type of attack could be associated with command-related actions, such as "launch all aircraft." These attacks apply to NM, signaling, and bearer streams.
G20	SIP Parser attack	2	2	4	This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to create a poorly organized SIP message that is difficult to parse.
G21	SIP Registration or INVITE Flooding – DoS attack	3	3	9	Attacks include valid/invalid registration flooding, and valid/invalid call request flooding. This attack could occur if an unauthenticated EI or SIP signaling appliance was allowed to connect to the network. Another avenue would include the manipulation of the SIP application to generate repetitive registration or INVITEs.
G22	Buffer overflow attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	"Spam"over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install antivirus software on appliances that have applications.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G26	Exploitation of a "zero-day" vulnerability	3	3	9	System remains exposed until an approved fix is available. Close coordination with trusted vendors is needed, along with the ability to approve/implement fixes rapidly once available. Must address any CM, security approval, and implementation issues for expeditious turnaround.
G27	Disabling of security controls by authorized users	2	3	6	Various motivations (e.g., avoid complexity, concerns over agency monitoring) prompt authorized users to attempt turning off security mechanisms. Product features to prevent, detect, and/or respond to such circumvention should be included, along with having these features validated (APL).
G28	Exploitation of numerous vendor-specific VVoIP product vulnerabilities	3	3	9	The variety of products that comprise the DISN IP VVoIP introduces the potential for numerous vulnerabilities for exploitation by human threat sources. Although approved products are used, the components must be configured properly and patched on an ongoing basis.
G29	Exploitation of underlying (i.e., not VVoIP-specific) network and/or system vulnerabilities	3	3	9	This item is intended to address all threats considered "general" in the sense of DoDI 8510.01: "All DoD ISs shall be implemented using the baseline DoD information assurance controls IAW DoD Instruction 8500.2. The baseline DoD information assurance controls may be augmented if required to address localized threats or vulnerabilities (Section 4.5)." Integration and compliance with the DoDI 8500.2 baseline controls will largely mitigate this risk.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G30	Unintentional flooding	2	3	6	Unintended flooding due to simultaneous endpoint registration after a power outage, misconfigured endpoints (e.g., IP phones with too short a registration interval), legitimate flooding (e.g., following a disaster), or endpoint hardware, software, or firmware malfunctions that cause flooding.
G31	Security devices collectively impact QoS	2	2	4	Security defense-in-depth depends upon layers of safeguards, including technical components that have the potential to introduce delay (fws/NAT, IDS), packet loss and jitter (encryption solutions)—all challenges to VVoIP. Security requirements must be balanced carefully against performance needs.
G32	Components within the system from untrusted sources that could serve as future attack points, e.g., back doors, logic bombs	2	3	6	Example: usage of untrusted foreign actor-developed/supplied components, subassemblies, or software embedded within VVoIP, Information Assurance, and Information Assurance-enabled products.

Table 5.4.3-5. Data Deletion Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	3	1	3	To find the physical location of a user, an enemy may try to eavesdrop on an old address to determine where the terminal was. The likelihood is high due to the mobile nature of DoD subscribers. The risk is reduced by using non-global addressing.
D2	Masquerading as a subscriber to delete data	2	3	6	Once enemy agents gain access to the network they may, in addition to calling people, attempt to access the signaling data to disrupt the ability to place calls. However, the likelihood of this action is less than calling another subscriber.

Table 5.4.3-6. Subscriber Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.

Table 5.4.3-7. Subscriber De-Registration Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	Due to the use of TDM for the interface to the PSTN and other networks, the likelihood of this attack is minimal. The impact is also minimal since this would likely be detected very rapidly.
SD2	Subscriber does not allow de-registration by manipulating the EI	2	1	2	The impact is minimal since the subscriber should be isolated easily using FWs and other security mechanisms.
SD3	Subscriber does not allow de-registration by manipulating VVoIP server	2	3	6	This can inhibit the ability of the network to disable illegitimate users and is part of a DoS or flooding attack. SIP manipulation is possible using virus infection.

Table 5.4.3-8. Incoming Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	2	2	4	Since authentication is mandatory, the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken, it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear, making it difficult to obtain.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I4	Eavesdropping at the start of a communication on the EI	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers also are vulnerable to this due to the interval between a call transfer and the rekey.
I5	Modification of routing data	1	3	3	The impact is that data may be routed to bogus or enemy networks; legitimate entities also may be excluded. The likelihood is low due to the defense-in-depth strategy required.
I6	Message alteration: call black holing	1	3	3	Intermediary configured by an attacker to not pass essential protocol messages. This causes delays in call setup, dropped connections, and other errors.

Table 5.4.3-9. Outgoing Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
O1	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
O2	Masquerading using a subscriber's ID and authentication	1	3	3	Authentication would be obtained by methods described elsewhere in Section 5.4.4.3.
O3	Eavesdropping on the access interface by using a session key	1	2	2	Session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear, making it difficult to obtain.
O4	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.
O5	Eavesdropping on the start of a communication on the EI	2	1	2	This is possible if call setup is performed before the authentication is completed. Call transfers also are vulnerable to this due to the interval between a call transfer and the rekey.
O6	Eavesdropping on the phone number of a called party	2	1	2	This is possible if call setup is performed before the authentication is completed.

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
O7	Modification of the dialed number	2	3	6	This attack could result in a precedence call being forwarded to the wrong location.
O8	Masquerading using someone's ID	2	1	2	This is accomplished for placing a short call before authentication.

Table 5.4.3-10. Emergency and Precedence Call Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	3	1	3	An attacker would place a 911 or emergency call without reason to cause chaos during a crisis or attack. This is important if the authentication mechanisms are compromised or are not implemented for emergency calls. Normally, it would be associated with single sessions.
E2	Misuse of precedence calls	3	3	9	An attacker would place a precedence call without reason to a particular phone to deny that phone's access to other calls. This is important if the authentication mechanisms are compromised.
E3	Manipulation of emergency database information	2	3	6	This could cause calls to be improperly sent to emergency numbers; thereby tying up the circuits or sending the emergency calls to invalid destinations.
E4	Manipulation of precedence database information	2	3	6	The likelihood of this attack occurring is higher since this is a critical point of attack for an enemy agent.

Table 5.4.3-11. Survivability Threat Risk Assessment

ITEM	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	3	9	This is a situation very likely in the DoD environment.
S2	A device in the network is disabled or destroyed	3	3	9	Many times an attacker will be able to disable one device before the attacker is detected.

Table 5.4.3-12. Risk Summary

RISK LEVEL	NUMBER OF RISKS	RISK SCORE
Critical Risks	27	6,9
Major Risks	16	3,4
Minor Risks	15	1,2
Total	**58**	

As seen in Table 5.4.3-12, Risk Summary, approximately one half of the risks are categorized as critical and require CMs. Sixteen risks were categorized as major risks and the risk should be minimized. Although the other risks are minor, they are still risks that require mitigation and will need to be addressed in the Information Assurance design. This risk summary table is repeated at the end of this section as Table 5.4.8-9, Adjusted Risk Summary, and it shows the mitigated scores based on the full implementation of the VVoIP Information Assurance design.

NOTE: The risk scores are preference scores, which indicate multiple values that are relatively greater or lesser than the other values. These measures are ordinal. A risk with a score of two is considered to be a greater risk than a risk with a score of one; however, a risk of two is not necessarily twice as great as a risk of one. With ordinal measures, the magnitude of the difference between two and one is not known. In tables such as Table 5.4.3-4, General Threat Risk Assessment, scores are treated like interval data. A likelihood score of two is multiplied by an impact score of two to produce a product of four, which is called a risk score. Under certain conditions, ordinal data may be treated as interval data. In general, the nature of the distribution is the primary consideration.

5.4.4 VVoIP Generic Countermeasures

In "Analysis of Information Assurance Requirements and Threats for the DoD Real-Time Services Environment," a set of threats and requirements for the DoD VVoIP environment was identified and these threats were summarized in the preceding paragraphs. A complete discussion of the CMs is provided in "DoD RTS Information Assurance CMs." This section describes the process used to develop the CMs required of the DoD VVoIP environments based on those threats and requirements, and it summarizes the generic CMs developed to mitigate the threats. The first step in the process is to develop an initial set of recommended CMs that tentatively mitigate the threat to an acceptable level.

5.4.4.1 Recommended Countermeasures

The recommended CMs were developed using an iterative process involving the vendor and DoD communities to mitigate the threats associated with a DoD VVoIP environment. The CMs are presented in a generic manner to ensure they do not mandate a technical solution, and are provided as part of the systems engineering process for developing the Information Assurance design. There is no intent to mandate a countermeasure on an appliance or system and they

should not be considered requirements. The system design, and its associated requirements, will define the technical solution for the system and its appliances and a specific countermeasure may or may not be used dependent on the design. The threats associated with ancillary services and TDM technologies have not been addressed completely. Therefore, the CMs described below do not address the threats associated with ancillary equipment and TDM technologies completely. Before discussing the CMs, it is important to define the terms used in the discussion.

1. Registrant. An appliance that is used to register with the network to seek and gain authority to invoke services or resources from the network. Registrants are typically associated with primary and alternate registrars. Examples of registrants are EIs, AS-SIP End Instruments (AEIs), EOs, PCs, and LSCs.

2. Registrar. The appliance that stores the location of a registrant and its profile. The profile is used to define the services to which a registrant is authorized (or a user via the registrant). In the DoD VVoIP environment, examples of the registrar include LSCs, AEI and DoD approved Public Key Infrastructure (PKI) servers. A registrar may reside on the same appliance and be integrated with a Service Point of Attachment (SpoA).

3. Service Point of Attachment. An SpoA is an appliance to which a registrant establishes a session over the IP network or TDM network. The session may be established to pass signaling or network management traffic. In the DoD VVoIP environment, examples of an SpoA are LSCs, MFSSs, SSs, directory servers, or gateways.

4. Transport Point of Attachment (TpoA). A TpoA is an appliance that is used to provide transport of a session over a network. Examples of transport appliances in the DoD VVoIP environment include routers, LAN switches, firewalls, EBCs, MFSS, and gateways.

Figure 5.4.4-1, Interaction between VVoIP Information Assurance Components, shows the interactions between the different countermeasure elements.

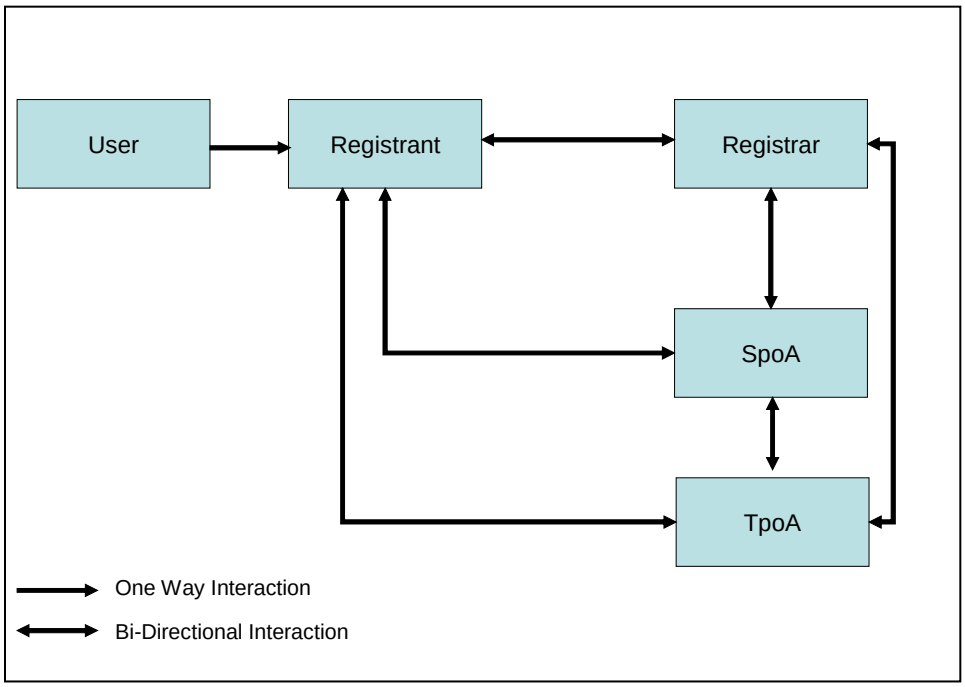

Figure 5.4.4-1. Interaction between VVoIP Information Assurance Components

5.4.4.2 Access Control Countermeasures

1. C1 – Access Control to Services. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to services.

2. C2 – Access Control to Database. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to a database.

3. C3 – Access Control to Sensitive Information in EI and AEI. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to sensitive information stored on an EI or on an AEI.

4. C4 – Access Control to System Software. The system should validate, based on prior authentication, the privileges to which a user has authorization before granting access to the system software. This software includes the software needed to provide VVoIP as well as the operating system software.

5. C5 – Access Control to System Hardware. The system should control access to the use of system hardware from users who are not authenticated.

6. C6 – Access Control to System Resources. The system should protect system resources from users who are not authenticated.

7. C7 – Access Control between Network Resources. The system should protect one network resource from another network resource unless there is a defined requirement for those resources to interact.

5.4.4.3 Authentication Countermeasures

1. A1 – Authentication of the EI and the AEI by the Registrar. The EI and AEI should contain a unique identity that identifies the EI and the AEI to the registrar, and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar, the EI, and the AEI, or by the use of a public key cryptosystem. This countermeasure is the corollary of A2.

2. A2 – Authentication of the Registrar by the EI and the AEI. The Registrar should contain a unique identity that identifies the registrar to the EI and the AEI, and authentication should confirm this identity through proof of knowledge of a secret shared by the registrar and the EI and the AEI, or by the use of a public key cryptosystem. This countermeasure is the corollary of A1.

3. A3 – Authentication of the EI and the AEI by the SpoA. Before providing service to the SpoA, the SpoA should authenticate the EI and the AEI. This countermeasure is the corollary of A4.

4. A4 – Authentication of the SpoA by the EI and the AEI. Before transmitting to a SpoA, the EI and the AEI should authenticate the SpoA to ensure that it is the actual SpoA assigned by the registrar. This countermeasure is the corollary of A3.

5. A5 – Authentication of the SpoA by the Registrar. The registrar should authenticate the SpoA before directing an EI and AEI to use that SpoA. This authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is the corollary of A6.

6. A6 – Authentication of the Registrar by the SpoA. The SpoA should authenticate the registrar requesting service before granting that service. The authentication should be based upon a secret shared by the registrar and the SpoA. This countermeasure is a corollary to A5.

7. A7 – Authentication of the User to the Appliance. The user should authenticate to the appliance to protect against misuse. This countermeasure does not have a corollary.

8. A8 – Authentication of the SpoA by the TpoA. Before transmitting to a SpoA, the TpoA should authenticate the SpoA to ensure that it is the actual SpoA to which it is assigned. This countermeasure is the corollary of A9.

9. A9 – Authentication of the TpoA by the SpoA. Before transmitting to a TpoA, the SpoA should authenticate the TpoA to ensure that it is the actual TpoA to which it intends to transmit. This countermeasure is the corollary of A8.

10. A10 – Authentication between SpoAs. Before transmitting to a SpoA, the SpoA should authenticate the other SpoA to ensure that it is the actual SpoA to which intends to transmit. This countermeasure does not have a corollary.

11. A11 – Authentication between TpoAs. Before transmitting to a TpoA, the TpoA should authenticate the other TpoA to ensure that it is the actual TpoA to which intends to transmit. This countermeasure does not have a corollary.

5.4.4.4 Non-Repudiation Countermeasures

N1 – Non-Repudiation of User Modifications to Appliance Resources. The appliances should ensure that non-repudiation is associated with any modifications made to an appliance's resources to include the operating system, files, applications, or databases.

5.4.4.5 Data Confidentiality Countermeasures

1. E1 – Confidentiality of User Communication on the EI and the AEI. The system should provide confidentiality for bearer stream at the EI and the AEI for originating and terminating sessions.

2. E2 – Confidentiality of Signaling on the EI and the AEI. The system should provide confidentiality for the signaling stream at the EI and the AEI for all originating and terminating sessions.

3. E3 – Confidentiality of Signaling between SpoAs. The system should provide confidentiality for the signaling between SpoAs. Signaling may include session keys, call-forwarding numbers, network management traffic, and personal data.

4. E4 – Confidentiality of Signaling between SpoA and TpoA. The system should provide confidentiality for sessions between the SpoA and the TpoA. The signaling may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

5. E5 – Confidentiality of Communication between TpoAs. The system should provide confidentiality for sessions between TpoAs. The communication between TpoAs may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

6. E6 – Confidentiality of Communication between SpoA and Registrar. The system should provide confidentiality for sessions between SpoAs and registrars. The communication may consist of signaling or network management traffic. This may be accomplished using physical protection or cryptographic protections.

7. E7 – Confidentiality between User and Appliance. The system should provide confidentiality for sessions between an authenticated and authorized user and an appliance for network management purposes.

8. E8 – Confidentiality of Data at Rest. The system should provide confidentiality for data at rest. The data may be stored in a file or a database.

9. E9 – Confidentiality between the Registrar and the Registrant. The system should provide confidentiality for registration and de-registration of appliances to the network.

5.4.4.6 Data Integrity Countermeasures

1. I1 – Signaling Integrity. The system should ensure integrity for signaling messages. Types of signaling messages include SIP, H.323, and routing updates.

2. I2 – Bulk Data Transfer Data Integrity. The system should ensure integrity for bulk data transfers. Bulk data transfers include call detail records (CDRs).

3. I3 – Appliance Data Integrity. The system should ensure the integrity of data written, read, or stored on an appliance.

4. I4 – Appliance System Integrity. The system should ensure the integrity of the operating system and the applications on the appliance. This shall include unauthorized operating system or application modifications.

5. I5 – End Instrument Transport Integrity. The system should ensure the integrity of the bearer packets transmitted between the end instruments.

5.4.4.7 Survivability/Availability Countermeasures

1. S1 – Diversity of Network Connections. The system should ensure high availability using diverse geographical distinct connections for designated locations throughout the network.

In addition, the connections should be diverse from both physical and logical perspectives. Sites that require diverse geographic distinct connections are typically C2 sites. However, non-C2 sites sometimes require diverse connectivity dependent on the mission and network topology.

2. S2 – Redundancy of Hardware and Software. The system should have sufficient redundancy in hardware and software to ensure that the required availability is achievable based on the computed failure rates for the hardware and software.

3. S3 – Out-of-Band Network Management Capability. The system should have an out-of-band network management capability for use during network outages or for when network resources are not reachable during Information Assurance attacks.

4. S4 – System Power Redundancy. The system should have sufficient backup power for use during power failures based on its usage and user requirements.

5.4.4.8 Miscellaneous Countermeasures

Some CMs overlap many assurance categories; these are classified as miscellaneous CMs. Each of the assurance categories are subject to newly-discovered ("zero-day") vulnerabilities. Miscellaneous CMs contribute to a layered, defense-in-depth design for zero-day addressing and other vulnerabilities.

Product Assurance: VVoIP components should be purchased from reputable vendors that, at a minimum, conduct internal pre-release reviews and provide vulnerability fix support for their products. Details of these provisions should be documented as part of the vendor warranty to the Government that addresses product defects.

5.4.4.9 Privacy Countermeasures

1. P1 – Physical Security. The system infrastructure should be placed in a secure facility that only permits access by authenticated and authorized personnel.

2. P2 – Personal Data Security. Personally Identifiable Information (PII), especially Social Security numbers, in the system infrastructure should be minimized to the maximum extent possible. Where present, the PII should be protected IAW DoD information assurance and privacy policy and guidelines.

5.4.4.10 Network Management Countermeasures

M1 – Threshold Exception Management System Notification. The system should notify a designated network management system when predefined thresholds are exceeded. A threshold

may consist of a single event (e.g., an audit log failure) or multiple events (e.g., multiple failed login attempts).

After developing the CMs, the next step in the Information Assurance Process was to develop a VVoIP Information Assurance design that implements these CMs. Based on that, design a set of requirements was derived. An iterative process was used due to the many interdependencies involved.

5.4.5 Information Assurance Design

5.4.5.1 Physical Security

Physical security for systems specified in this UCR is the responsibility of the installing B/P/C/S. Essentially, two sets of requirements are associated with a complete UC system. The EIs have one set of physical security requirements while the network (LAN switches and routers), signaling products (i.e., LSC, MFSS, SS, MG), and security devices require another set of requirements. A full definition of physical security requirements is beyond the scope of this section of the UCR.

The physical security for the UC product network infrastructure and signaling appliances must limit physical access to all the associated appliances and cable terminations. Physical security safeguards shall be in place regardless of the sensitivity and/or classification of the product. However, products processing information of a higher sensitivity or classification level generally will require more rigorous physical safeguards than those products that do not. This means that the supporting infrastructure for the total product must reside, minimally, behind locked doors. This however, may be provided minimally by a lock on a cabinet housing a LAN switch in the open (i.e., an unsecured area). With the EI and the AEIs, typically this is afforded by the facility in which the equipment or infrastructure is housed (e.g., locks and/or access control on doors of rooms and closets housing the equipment).

Facility security requirements fall under the purview of "DoD Traditional Security." A subset of these requirements is provided in the VVoIP STIG and other related DISA STIGs.

Vendors must support their customer's need to comply with the DoD system physical security requirements for UC products. This support is to be provided in the form of locking kits for any equipment that the vendor normally provides in a cabinet. If a cabinet lock is not provided normally in the vendor's commercial offering, optional locking kits must be made available that work well with the vendor's cabinet. All cabinet locking mechanisms must be robust enough to resist prying the cabinet open.

5.4.5.2 Security Design

The UC product security design uses a defense-in-depth approach that is based on best commercial practices. The product security defenses are categorized as follows and discussed in the following paragraphs:

- User Roles
- Hardened Operating Systems
- Auditing
- Application Security
- Redundant Systems

Additional defenses may be added dependent on the specific threats associated with a product.

5.4.5.2.1 User Roles

In general, three types of users are related to a UC product, which are segmented into two different categories: users of the system services, and administrative users of the product. This becomes confusing due to the unqualified and repeated use of the word "user." One must be aware of and remember what area of the product is being discussed (i.e., its services or its administration, configuration, or maintenance) in order to be sure of the context of the word.

Essentially, a user of product services has one role. He or she uses the services that the product provides and they are referred to in this UCR section as "application users." Such a user may be a "privileged application user" who has permission to use certain restricted services, such as the ability to initiate a FLASH precedence session. Such a user may be required to authenticate to the product in some fashion (such as entering a personal identification number (PIN) code to identify the user (called User ID) and a different PIN (called password) to authenticate the user) in order to receive access to their "privileged" service. There may be multiple levels of privileged service, which might be considered "service user roles" by some readers.

Administrative users are those users that are tasked with the configuration, operation, or maintenance of the system. These users are usually referred to as system administrators. System administrators fulfill different roles based on their duties, responsibilities, or job description/function. DoD policy requires that system administrators receive only those system privileges or access to commands that are required to perform their duties (i.e., role-based access). System administrators who are limited to selected applications on the system are designated application administrators.

System administrators receive their privileges or access to commands based upon Discretionary Access Control (DAC), which provides authorization control. Discretionary Access Control is a role-based feature that grants a system administrator specific permission to perform various

functions when accessing the product. Such permissions are established IAW the job functions and responsibilities (role) of the individual. Permissions are established by the responsible security officer (i.e., the Information Assurance Officer (IAO) or system security administrator), and stored in the system memory or its configuration files. The security officer also establishes the relationship in the system between authorized command class(es) or group(s).
Products that are developed with various levels of authorization or command access must support DAC requirements. This can be achieved by user privileges or group privileges. The methods to access resources may vary depending on hardware and software products.

Examples of system administration roles are as follows; however, more information on DoD-specific designated Information Assurance roles can be found in DoDD 8570:

1. Tier III Engineer (Troubleshooter – Initial Support). This role may only have privileges and access to commands that allow him/her to view operational statistics, alarms, and some specific level of appliance or system configuration. This role may not have the ability to change any configuration settings. This could be considered Tier III support.

2. Tier II Engineer. This role would have all the capabilities of the troubleshooter role with the added privileges and access to certain commands that allow him or her to make some but not all configuration changes.

3. Tier I Engineer. This role would have privileges and access to all commands for troubleshooting and system configuration.

4. Provisioner/Administrator. This role may only have privileges and access to commands that allow him/her to provision circuits, configure end instruments and/or features. This role may have the ability to troubleshoot some aspects of the system.

Another scenario is the case of a database administrator or application administrator role that only has rights to access the database or an application that they manage but does not have rights to access the administration of the operating system on the platform that support one or more databases or applications.

Similar roles or levels of privilege and DAC to those described above are required for DoD information systems. These equate to the normal system administrator roles. The granularity of DAC provided is dependent on the capabilities of the specific system being managed.

The third type of user required for DoD systems is the Auditor, which is short for Security Auditor. This role has none of the normal system administrator privileges or access. The normal system administrator role does not have access to auditor level commands. The auditor role only has access to commands related to the security or audit logs, and is associated with the system security administrator.

5.4.5.2.2 Hardened Operating Systems

Multipurpose or general-use operating systems are delivered without, or with a minimal number of security features enabled. Access to critical areas of the operating system as well as application and data files is sometimes unrestricted. Additionally, some of these operating systems are delivered with inherent security vulnerabilities, both known and undiscovered. The process of "hardening" an operating system is the process of restricting access to those system areas and functions that could be detrimental to the security of the system and mitigating the known and/or discovered security vulnerabilities. The implementation guidelines associated with common operating systems are found in the STIGs developed for the operating system and are different for every operating system.

5.4.5.2.3 Auditing

Auditing refers to the logging and analysis of security-related events. Auditing and recording the events occurring to or within an appliance of the APL product is critical to maintaining accountability. This is accomplished by tracking security- and configuration-related changes, which provides the system security administrator or Information Assurance manager vital information to reconstruct what may have occurred before a system crash or other situation. Security auditing is necessary for the reconstruction of system events that have led to a security incident in support of disciplinary action or prosecution. This information also may allow the system manager to restore a system to its correct configuration and to determine the cause of the problem. The term "history file" may or may not relate only to security. Some systems, such as telecommunications appliances, record every transaction performed by the appliance. History files may or may not contain auditable security events. A determination must be made for each appliance about the location of the security audits. Appropriate security record events must be captured, recorded, retrieved, protected, reviewed, and archived on a regular basis.

The DoDI 8500.2 is the primary driver of auditing requirements. The DoDI 8500.2 Information Assurance control Enclave and Computing Environment Audit Trail Protection-1 (ECTP-1) states:

> "The contents of audit trails are protected against unauthorized access, modification or deletion."

DoD requirements also state that all systems perform security auditing and that auditing records are placed in an unalterable audit or history file that is available only to those individuals authorized to analyze system or network appliance access and configuration activity. This implies that the audit log must be separate from any other system logs. Some devices in the network may not maintain audit logs directly themselves (for example, EI); however the servers and systems to which these devices connect (for example, LSCs) will generate and store audit content based on the activity of the connected device.

The DoDI 8500.2 states the following about audit record content:

Audit records include:

Enclave and Computing Environment Audit Record Content-1 (ECAR-1): Base level for information sensitivity = public

- User ID
- Successful and unsuccessful attempts to access security files
- Date and time of the event
- Type of event

Enclave and Computing Environment Audit Record Content-2 (ECAR-2): Adds items for information sensitivity = sensitive

- Success or failure of event
- Successful and unsuccessful log-ons
- Denial of access resulting from excessive number of logon attempts
- Blocking or blacklisting a user ID, terminal or access port, and the reason for the action
- Activities that might modify, bypass, or negate safeguards controlled by the system

Enclave and Computing Environment Audit Record Content-3 (ECAR-3): Adds items for information sensitivity = classified

- Data required to audit the possible use of covert channel mechanisms
- Privileged activities and other system-level access
- Starting and ending time for access to the system
- Security-relevant actions associated with periods processing or the changing of security labels or categories of information

The above DoDI 8500.2 requirements are mapped, interpreted, and augmented with best practice, as shown in the following paragraph.

At a minimum, the following events are to be audited on the system and network devices:

- Logons and logouts
  - Starting and ending time for access to the system
- Excessive logon attempts or failures
  - Denial of access resulting from excessive number of logon attempts
  - Blocking or blacklisting a user ID, terminal, or access port, and the reason for the action
- Remote system access
- Change in privileges or security attributes
  - Activities that might modify, bypass, or negate safeguards controlled by the system
- Change of security levels or categories of information
  - Security-relevant actions associated with periods processing or the changing of security labels or categories of information
- Failed attempts to access restricted system privilege levels or data files
- Audit file access
- Password changes (not the passwords)
- Device configuration changes
  - Privileged activities and other system-level access
- Other
  - Data required to audit the possible use of covert channel mechanisms

At a minimum, the following information is recorded in the audit log for each event that is audited:

- Date and time of the event
- Origin of the request (e.g., terminal/workstation ID, port ID, IP address)
- Unique ID of the user who initiated the event
- Type of event
- Success or failure
  - Success or failure of event
  - Successful and unsuccessful logons
  - Successful and unsuccessful attempts to access security files
- Description of modification to configurations

NOTE: A vendor's system, appliance, or product should support the audit requirements for classified products so that they can be purchased for use in classified systems. There may be additional requirements that it will need to meet.

DoDI 8500.2 also requires that audit logs be:

"…regularly reviewed for indications of inappropriate or unusual activity" (ECAT-1) on MAC-3 and/or systems processing sensitive and public information.

Additionally, for MAC 1 and 2 and/or systems processing classified information it states:

"An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential information assurance implications, and with a user-configurable capability to automatically disable the system if serious information assurance violations are detected (ECAT-2). These requirements indicate that they are to be reviewed regularly and additionally for classified and/or mission critical systems, auditing should generate alarms to 'immediately alert personnel' of security issues."

The process of auditing security events can generate large volumes of data on busy systems. For this reason, audit logs are to be retrieved or removed from the system on a regular basis. Since audit logs contain information that may be required in support of administrative or prosecutorial actions, they must be protected. In some cases (i.e., Microsoft Windows-based systems), audit log protection is provided by halting the system operation if the audit capability fails.

DoDI 8500.2 ECRG-1 states:

> "Tools are available for the review of audit records and for report generation from audit records."

The tools that are referenced are software tools provided by the vendor that can interpret the vendor's audit log file format to allow offline viewing and analysis of the logs, as well as the generation of reports from the data contained therein.

5.4.5.2.4 Application Security

DoD application security requirements are based on and are implemented IAW DoD Information Assurance policy requirements. These requirements are detailed in the DoD "Application Security Checklist" and DoD "Application Development STIG." Basic application security requires that the application must not negatively alter the security posture of the supporting operating system or other applications on the platform. In addition, applications must not change operating system files. Applications may rely on the operating system for some Information Assurance functions or may include some or all Information Assurance enablement features in the application. Applications that provide management capabilities of a system should be Information Assurance enabled. These applications should provide, at a minimum, for identification, authorization, roles/command classes, and auditing IAW the documents mentioned previously in this section.

5.4.5.2.5 Redundant Systems

Products that support critical services, such as voice communications or security services should be designed with enough redundancy to prevent single point of failure issues that could affect more than a threshold number of endpoints. This is partially driven by the percentage of "uptime" that is targeted for the overall system. Every critical product function should have a backup. This includes power distribution, signaling appliances, other critical servers, core LAN hardware (routers and switches), boundary hardware (EBCs and CE Routers), and data links. A certain level of redundancy is appropriate. The core and distribution segments of a LAN, for example, should be redundant. The uplinks to the access segment switches should be redundant also. Redundancy for access segment switches and the distribution cabling to the endpoints does not make sense. One design concern is that if the access segment switch supports more than the threshold number of voice endpoints, which is typically driven by the Telcordia Technologies GR-512-CORE reliability requirements, then it is recommended that the endpoints be split among different switches. If this cannot be done, the switch should have redundant processors and power supplies.

It is beyond the scope of this section to define every item that needs to be redundant. This determination must be made based on good design criteria and best commercial practices. Nevertheless, System Quality Factors (see Section 5.3.3.12) of this UCR specifies many

requirements associated with redundancy, and these should be used as a requirement baseline for the systems to which the documents apply.

5.4.5.3 UC Component Interactions

One of the principal tenets of any Information Assurance design is the separation of components (i.e., traffic, appliances, and users) and/or services from each other based on their characteristics. Still, a converged network requires the opposite in that appliances within a converged network may service the voice, data, and video applications. As a result of this conflict, the interactions between the various component segments must be controlled to ensure that an attacker that gains access to one segment neither gains access to, nor can affect, the other segments. In addition, interaction control between various segments is used to prevent configuration or user errors in one segment from affecting other segments. The actions of normal users of converged network services must not affect the other services—more specifically the voice service. The principal mechanisms that are used within this design for segmenting the network are VLANs, segmented IP address space or subnets, and VPNs, and they are used in combination with filters, access control lists (ACLs), and stateful packet inspection firewalls (VVoIP Stateful Firewalls) to control the flow of traffic between the VLANs and VPNs.

Figure 5.4.5-1, Notional Example of Voice and Data ASLAN Segmentation, presents the simplest type of converged LAN with only voice and data applications. Those readers familiar with the framework defined in the DISA "Enclave STIG" will recognize many similarities between Figure 5.4.5-1 and the recommended framework defined in the "Enclave STIG." Separate VLANs are established between voice and data applications and the Layer 3 switches are responsible for providing access control between the different VLANs using filtering techniques, such as ACLs. In this type of deployment, appliances are classified as VVoIP appliances or data appliances and it may be possible to avoid deploying appliances that service both VVoIP and data appliances. At the CE Router, separate VPNs may be established, if necessary, to segment the voice traffic from the data traffic as the packets transit the DISN WAN. In addition, VPNs may be used to extend the local enclave to remote offices of the same organization, telecommuters, and travelers. Also, the VVoIP traffic is routed from the CE Router to the PE Router along the same path as the non-VVoIP traffic. The only connection to the PSTN is through a TDM interface using PRI or CAS signaling so there is not interaction between the VVoIP system and commercial VVoIP IP networks. Moreover, it is important to note that the LSC has two separate interfaces, one for signaling and bearer traffic, and one for NM traffic.

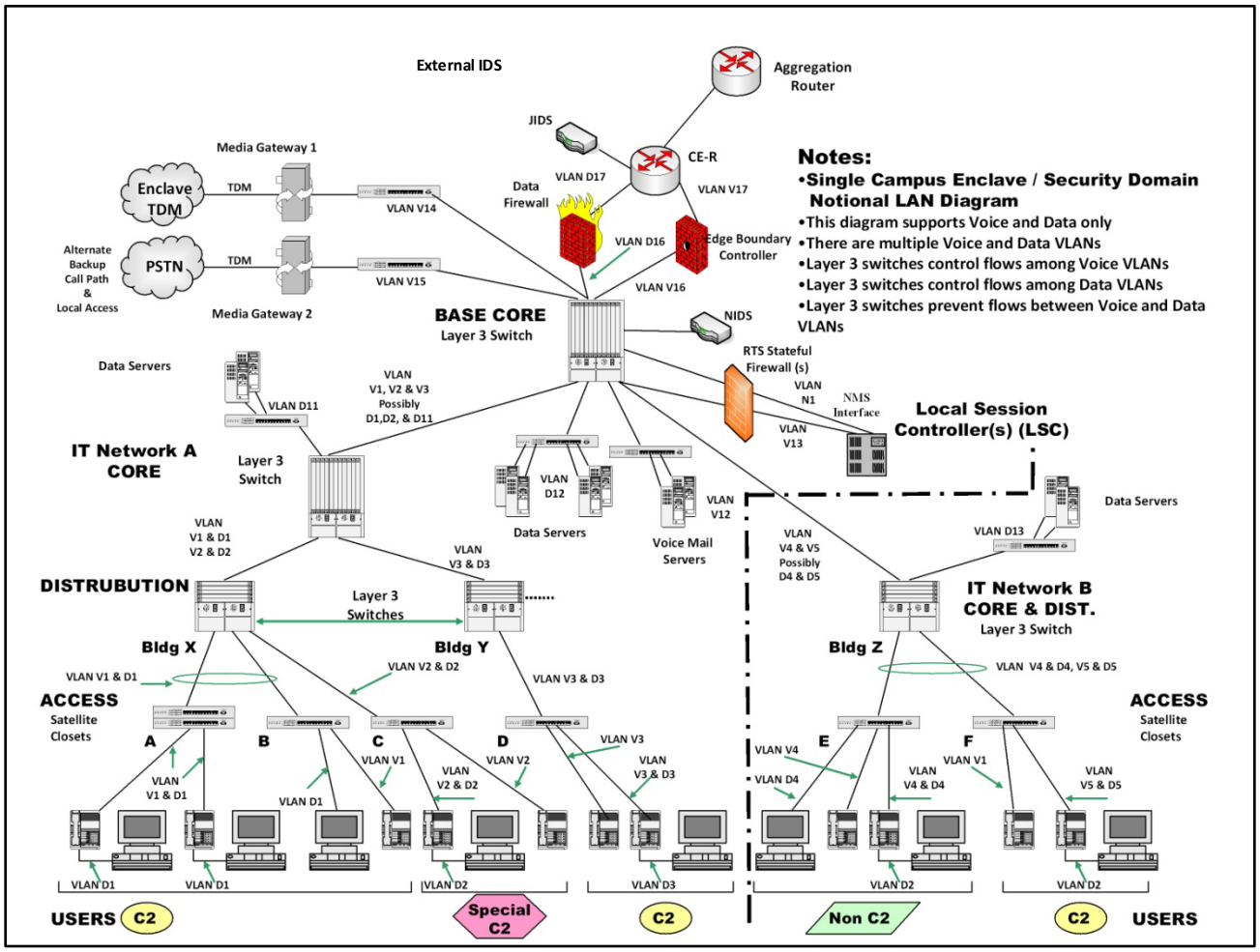

Figure 5.4.5-1. Notional Example of Voice and Data ASLAN Segmentation

The 802.1Q VLAN tagging of the packet for the appropriate VLAN should occur at the appliance, but may occur at the first LAN switch if the appliance is not capable of 802.1Q VLAN tagging. To comply with this, the ASLAN permits port-based and MAC-based VLAN tagging. If an EI or an AEI supports a subtended data computer OR workstation, it must perform several unique functions. The first function is that it should be capable of VLAN tagging the data traffic with a different VLAN tag than the voice traffic. In addition, it must be capable of routing the VVoIP traffic and the data traffic to the appropriate VLAN. This function's objective is to ensure that the data applications on the workstation do not have visibility to the voice-related packets.

A more complex and complete design involves appliances that support multiple types of applications like softphones (running on PCs), UC VVoIP applications running on Multifunction Mobile Devices (e.g., smartphones, wireless tablets, Personal Digital Assistants (PDAs)), and videophones. Figure 5.4.5-2, Notional Example of Voice, Video, Softphone, Multifunction Mobile Device, Videophone, and Data ASLAN Segmentation, shows the VLAN segmentation

associated with this complex design. This figure also shows additional components that can be used to augment the security posture of the network such as NACs, VVoIP IDSs that monitor decrypted media and signaling at the EBC, and backend supporting services for remotely connected Multifunction Mobile Devices. Because this is an example deployment, actual deployments may not contain or use all the components shown. Additionally, some components may be deployed in different locations within the system depending on the requirements of the operational environment.

The figure illustrates that all voice, video, and data sessions associated with a VTC are VLAN tagged as a video session. In the case of videophones, the videophone may be used for voice or video applications. In this case, the audio and video traffic from the videophone may reside in the voice VLAN(s). The VTC only systems, desktop or room size, should have their own VLAN and addressing structure.

Demilitarized zones are created for appliances that must service multiple segments of the converged network. An example is the LSC that must service voice, video, videophone, and softphone appliances. Another example is the Multifunction Mobile Devices Backend Support System (MBSS) that serves remote devices connected via external networks while simultaneously providing access to internal servers. When the number of VLAN types increases, access control between the various VLANs becomes significantly more complex. Filtering at switches and routers alone is not adequate, and thus VVoIP stateful firewalls are used as an added defense to ensure that only authorized packets are able to transit the VLAN boundaries. In some cases, the stateful firewall may have the complete functionality of an EBC, but this is not required.

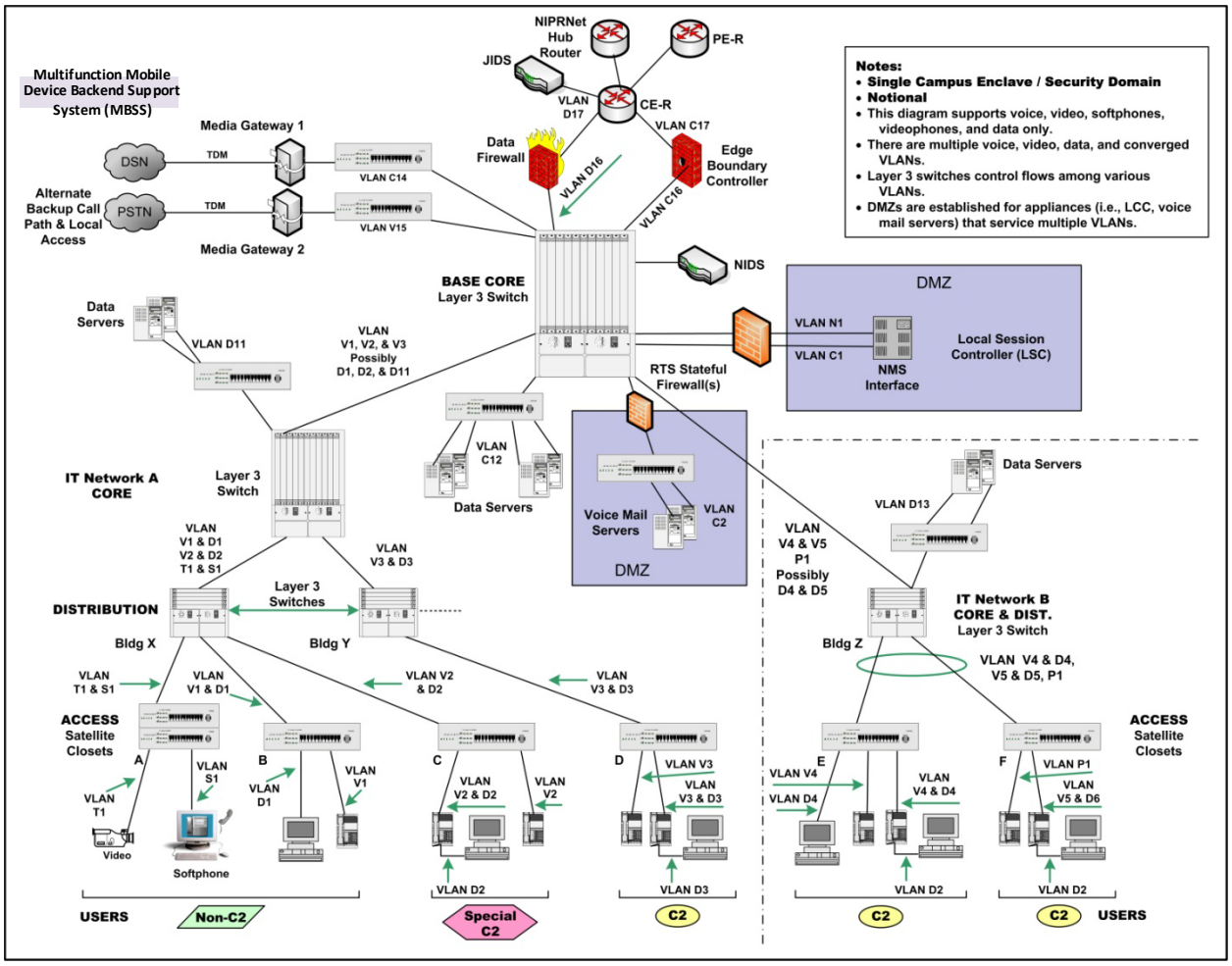

Figure 5.4.5-2. Notional Example of Voice, Video, Softphone, Multifunction Mobile Device, Videophone, and Data ASLAN Segmentation

In addition, if softphones are used in remote connectivity situations, such as for a long local for a Tactical Deployed system, the system must be capable of supporting a VPN for VVoIP traffic from the PC to the LSC. It is essential that the data and VVoIP traffic must be separated into the appropriate VLAN at the earliest point in the path. In the long-local scenario for a Tactical user, this separation would likely occur at the Teleport facility. For Multifunction Mobile Devices that support connectivity to UC VVoIP services, such as the LSC, the MBSS should perform this VLAN separation function if possible (if the traffic is not already separated by the edge device itself) so that VVoIP and XMPP-based media is separated from Multifunction Mobile Device data (e.g., e-mail, file transfer). Traffic from the MBSS should be placed into a separate VLAN dedicated to incoming Multifunction Mobile Device users, at a minimum, even if the voice and data traffic cannot be separated easily.

Finally, an alternative not shown in the figures involves an LSC that has separate interfaces for the H.323, AS-SIP, and NM traffic. In this scenario, the ASLAN should have an H.323 VLAN,

an AS-SIP VLAN, a data VLAN, and an NM VLAN as a minimum. Each network typically will have unique requirements and topology, and the VLANs implemented will depend on the local network needs.

Each of the following represents a separate VLAN (NOTE: Items marked with an asterisk (*) are currently required in the VoIP STIG.):

1. VoIP EIs and AEIs (multiple VLANs recommended for large sites)*

2. VoIP LSCs, SSs, and configuration servers*

3. Separate VLANs for other voice/VVoIP related servers

    a. Voice mail or unified messaging (voice mail and e-mail)*
    b. Computer Telephony Integration (CTI)
    c. Automatic Attendant/Call Director (ACD)
    d. Call center or operator's systems
    e. Emergency messaging system servers
    f. Multipoint controllers for conferencing: VTC and/or audio only
    g. Streaming video servers (video streams share the data VLANs)

4. Media Gateways*

    a. VoIP EIs that are part of a CTI, ACD, or call center/operator's system

5. VoIP EIs that have an integrated VTC capability

    a. VoIP and VTC video can share the same VLAN
    b. Multiple VLANs recommended for larger sites

6. Stand-alone desktop VTC units

    a. Units associated with and/or controlled by the VoIP LSC can reside in the VoIP EI VLAN(s)

    b. Workstations running softphone applications (DAA Approved)*

    c. Workstations running desktop VTC applications (DAA Approved)

7. Collaboration tools: The VTC portion should use the appropriate VVoIP VLAN(s) if technically feasible while the data applications (e.g., whiteboard, file sharing) must use the data VLAN(s).

8. Remote Multifunction Mobile Device users entering the network through the MBSS are placed into a separate VLAN upon entrance into the network. The UC VVoIP and data traffic ideally are placed into separate VLANs at this point. (DAA Approved)

Figure 5.4.5-3, Component Interaction Flow Diagram, provides a different depiction of the interactions between various VLANs within a B/P/C/S. The illustrations in this section are notional and address the scenario where ancillary services are internal to the system. The information is only provided as reference material and each B/P/C/S will determine its VLAN needs and boundaries based on its tailored requirements and security profile.

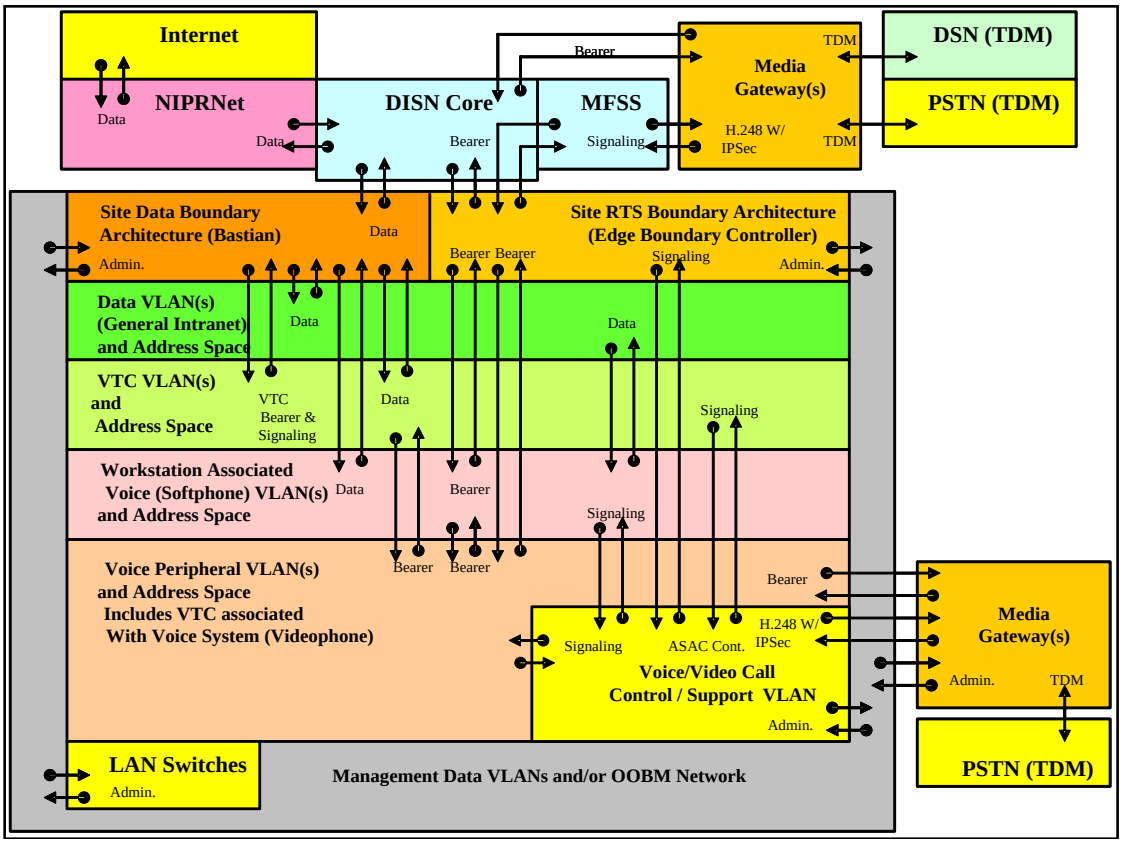

Figure 5.4.5-3. Component Interaction Flow Diagram

5.4.5.4 VVoIP Protocol Design

5.4.5.4.1 Overview

The VVoIP protocol design consists of a combination of standards-based protocols and proprietary-based protocols. Within an APL product the vendor is allowed to implement proprietary protocols for signaling (e.g., between the EI and the LSC or between the LSC and the MG), but standards-based protocols are required for interfaces to external NM, signaling and

transport appliances. Although EIs may use proprietary protocols, AEIs may not. The AEIs are required to use AS-SIP for signaling. Every proprietary protocol must be secured so that it is at least as secure as can be achieved using a standardized protocol. For instance, the VVoIP design mandates the use of TLS with AS-SIP to provide confidentiality and integrity. The AS-SIP, in combination with TLS, could be used for the signaling between the EI and the LSC, but is not required (AEIs require AS-SIP). Since every proprietary protocol must be secured so that it is at least as secure as can be achieved using a standardized protocol, if a vendor chooses to use a proprietary protocol for that interface, it must be as secure as that which can be achieved by using AS-SIP with TLS. Figure 5.4.5-4 presents the different protocols that are allowed in the VVoIP system and discriminates between interfaces that permit proprietary protocols and ones that require standardized protocols.

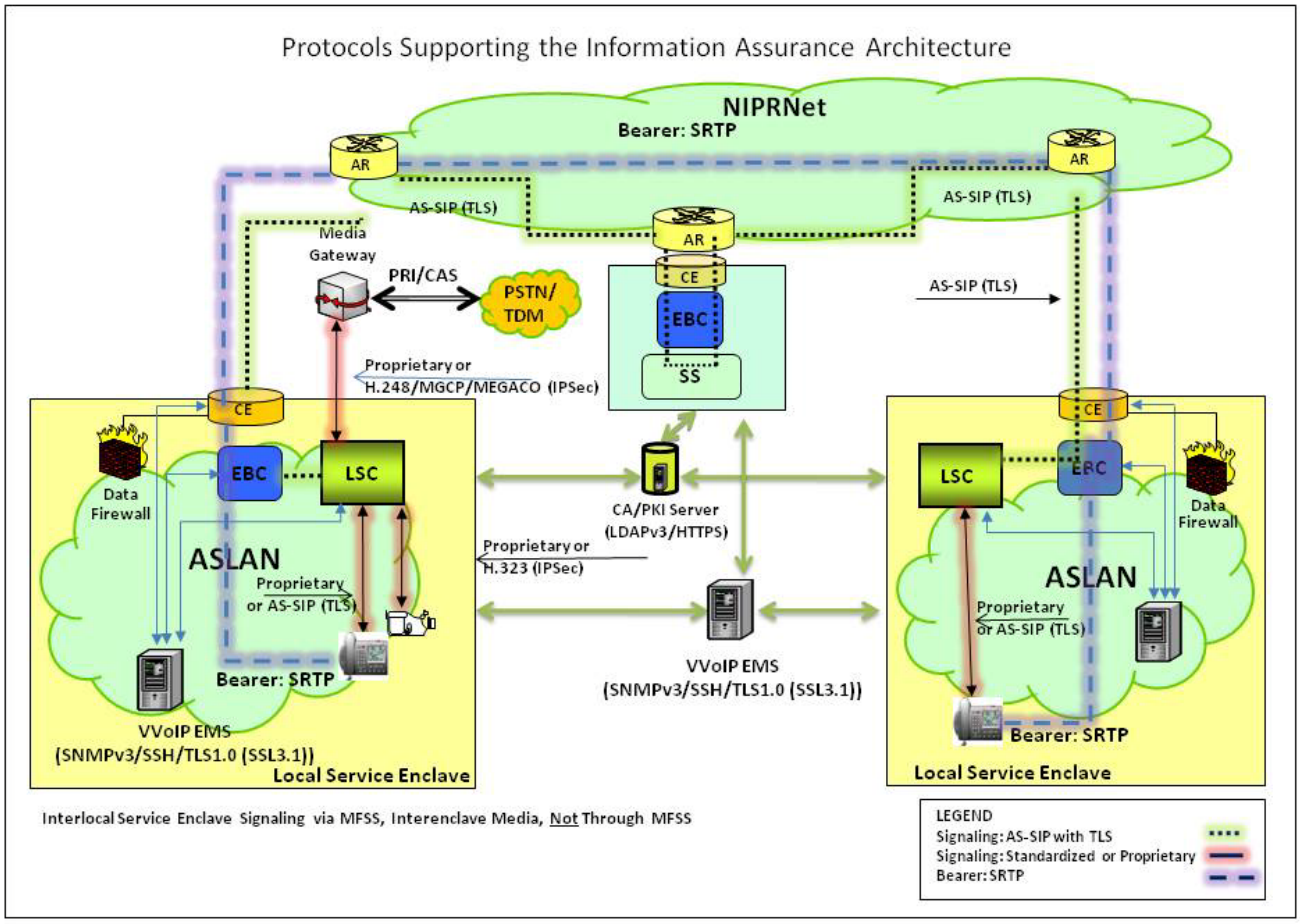

Figure 5.4.5-4. VVoIP Proprietary-Based and Standards-Based Protocols

Independent of the protocol or cryptographic algorithm used, many common Information Assurance mechanisms are required of all appliances. For example, every VVoIP signaling appliance that performs a cryptographic function must use a cryptographic module that is Federal Information Processing Standard (FIPS) 140-2 level 1 compliant in a FIPS-approved

configuration (with limited exceptions for certain widely used protocols that are not yet FIPS compliant). In addition, the default encryption algorithm for the VVoIP system is the Advanced Encryption Standard (AES) algorithm with 128-bit encryption unless the protocol does not support AES, in which case the encryption algorithm selected must use 128-bit encryption as a minimum. The default hash is the Secure Hash Algorithm (SHA) 1 or SHA-1, which is supported on every protocol used in this system. However, given the NIST directives to migrate to SHA-256 for digital signatures and the direction DoD-approved PKIs are heading with respect to SHA-256, all UC devices will need to minimally support SHA-256 when validating signatures on objects generated by DoD-approved PKI. In compliance with DoD requirements and policies, all VVoIP appliances also are required to be Public Key Enabled (PKE) so that they may interoperate with the DoD-approved PKIs, with the exception of EIs where this requirement is Conditional.

5.4.5.4.2 EI and AEI Authentication and Registration

The first step in the VVoIP protocol design is the registration of the appliance to the network and its receipt of an E.164 telephone number if it is an EI or an AEI. During the initial installation of an appliance either it will be configured with a static IP address (i.e., LSC, SS, MG, MFSS, AEI, and EI) or will receive its (EI or AEI) IP address from a DHCP server. The first step is for the EI or AEI to authenticate itself to the LAN switch to which it is physically connected using the 802.1X protocol. If DHCP is used, when the EI or AEI authenticates itself to the DHCP server to get its IP address it also will obtain the registration information necessary to locate the LSC. If an EI uses static IP addresses, it will be preconfigured by the system administrator with the location information of the LSC. NOTE: The DHCP server must be physically separate from the routers and LAN switches. Then the EI or AEI will authenticate itself to the LSC using its assigned E.164 number, and the LSC shall update its user database and local directory to reflect the active status of the EI or AEI with its associated profile. In addition, the LSC shall authenticate itself to the EI or AEI. The mutual authentication between the EI and the LSC shall use TLS or its equivalent for authentication, as a minimum, and more sophisticated authentication mechanisms, such as a PKI certificate assigned to the EI, are encouraged. The mutual authentication between the AEI and the LSC also shall use device certificates issued from a DoD-approved PKI, but only in conjunction with TLS. Each AEI (and conditionally each EI) shall be issued a device DoD PKI certificate that will contain a unique Common Name in the X.509v3 Subject field. Any exchanged X.509v3 certificates are validated against an Online Certificate Status Protocol (OCSP) responder or Certificate Revocation List (CRL) and validated against loaded trust anchors (Certificate Authorities or CAs). At this point, the EI or AEI is able to support VVoIP sessions at the ROUTINE precedence level. NOTE: The exact approach used for proprietary EIs to mutually authenticate with their LSC using PKI certificates is beyond the scope of this document. Figure 5.4.5-5, AEI Registration Process (DHCP), shows the AEI registration process if DHCP is used for obtaining its IP address. The figure simplifies the TLS authentication process for ease of understanding the sequence, but Figure 5.4.5-7, AS-SIP TLS Authentication Process, provides a detailed description of the TLS negotiation process.

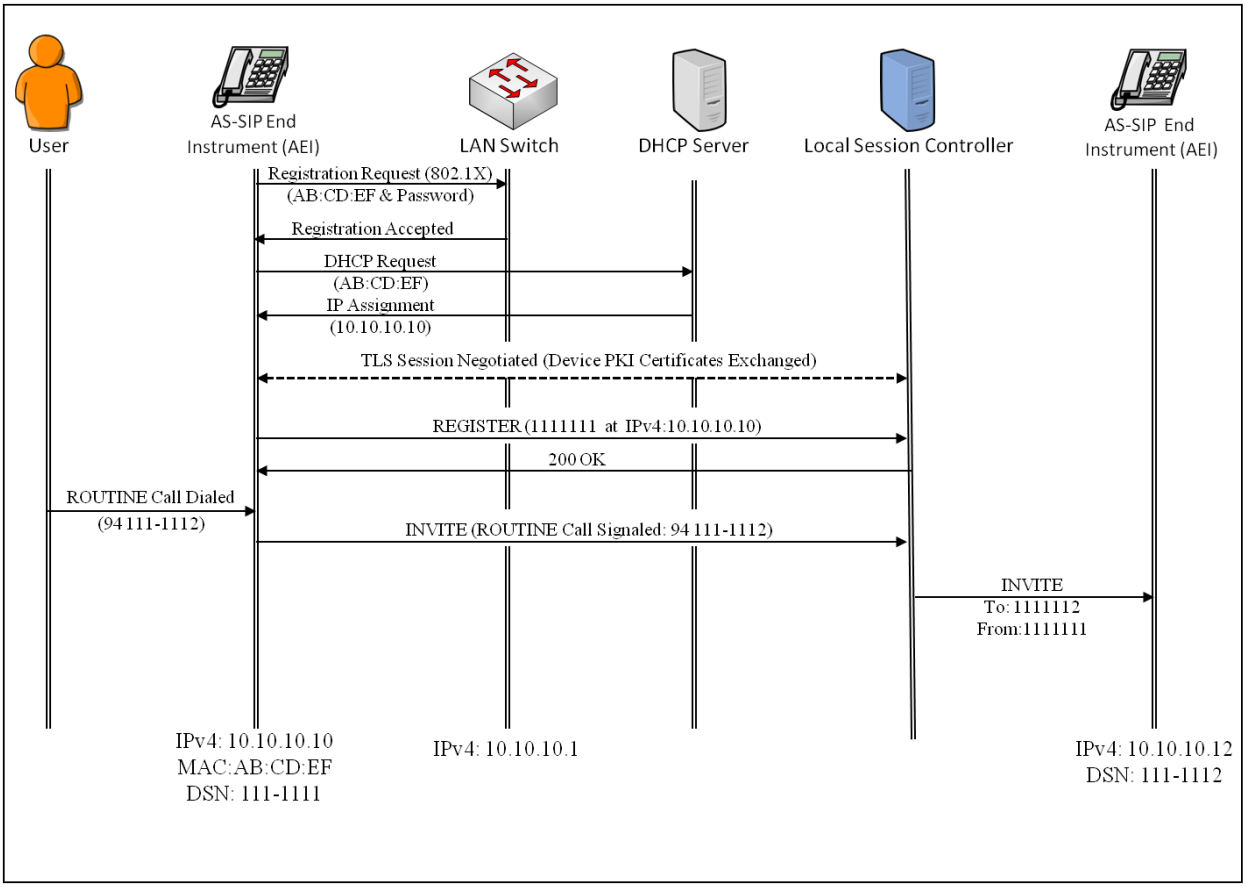

Figure 5.4.5-5. AEI Registration Process (DHCP)

5.4.5.4.3 User Authentication and Authorization

For a ROUTINE precedence VVoIP session, the system does not require user authentication. However, VVoIP sessions above ROUTINE precedence may require user authentication depending on the site configuration and that authentication may be provided using a User ID (PIN) with an associated numeric password (PIN), or using user certificates issued from a DoD-approved PKI. If the EI is a softphone, the EI must support the ability to pass the user credential provided by the CAC or other DoD-approved token to the LSC for user authentication. If a DoD-approved X.509v3 certificate is used, then the certificate path should be authenticated up to the trust point (or anchor point). Alternatively, if no other intermediate trust point is established, the certificate path shall be authenticated to the root certificate or Certificate/Certification Authority (CA). Limiting the authentication of a user to sessions with precedence above ROUTINE also limits the effect that authentication has on the post-dial delay, since the validation of a DoD PKI certificate can take up to 4 seconds to complete. If the user certificate cannot be validated due to inaccessibility to an online revocation status checking system, such an

OCSP responder, the session setup shall continue, but the event shall be logged and an alarm shall be sent to the Network Management System (NMS).

Based on the user authentication and the profile associated with that user, the LSC will make a decision on whether to allow the session setup to continue.

Figure 5.4.5-6, Precedence Session User Authentication and Authorization, shows the user authentication and authorization process for session requests above the ROUTINE precedence level when the user enters a User ID and PIN to authenticate to the LSC via an AS-SIP EI.

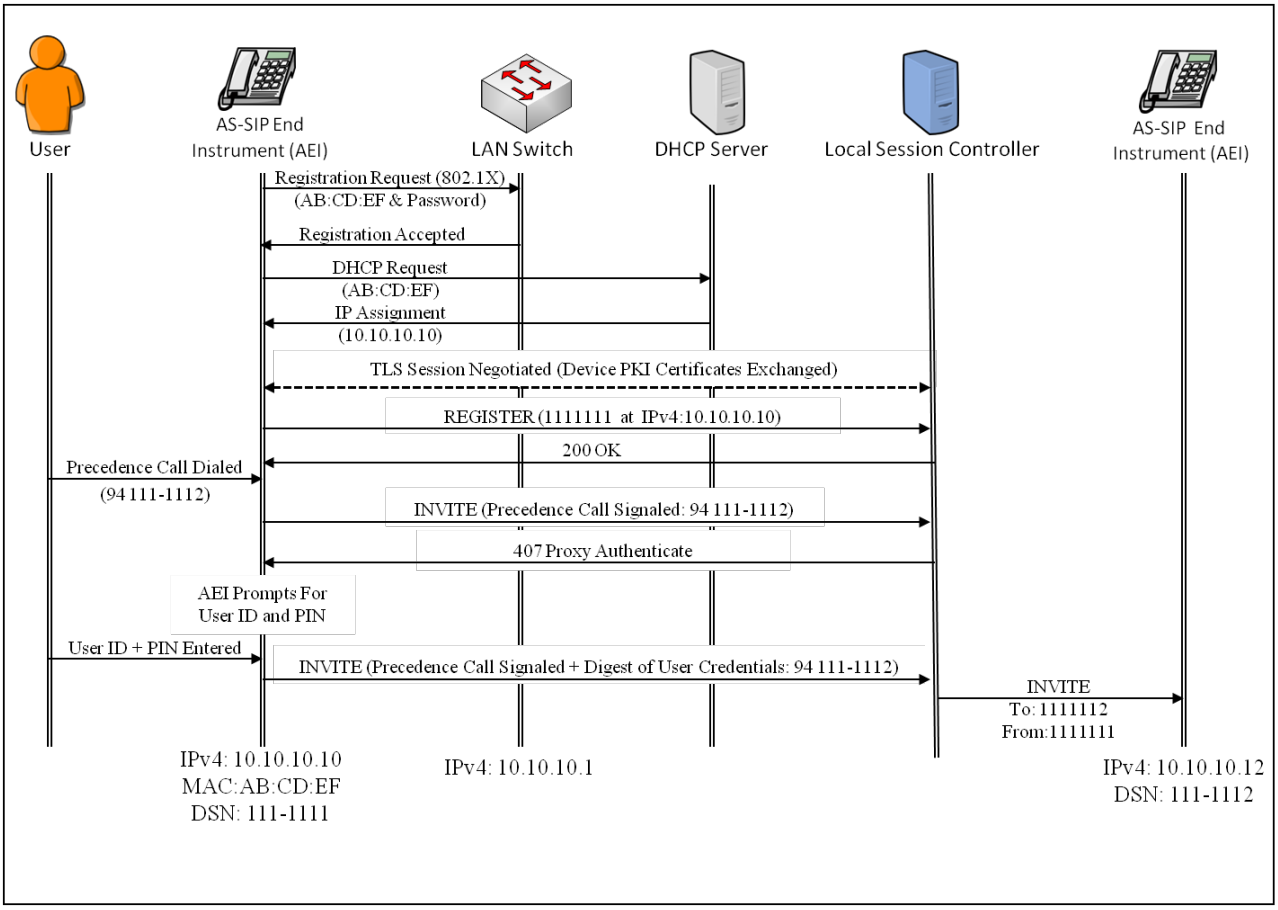

Figure 5.4.5-6. Precedence Session User Authentication and Authorization

5.4.5.4.4 Signaling Appliance Authentication and Authorization

5.4.5.4.4.1 AS-SIP

In addition to user authentication and appliance authentication, the signaling appliances must mutually authenticate to each other using a DoD-approved PKI. Since all signaling appliances support AS-SIP, the authentication mechanisms must be integrated with AS-SIP to provide

interoperability. Unfortunately, the SIP is not intended to be a secure protocol and must rely on other security protocols for its security. Since the AS-SIP model chosen is a hierarchical signaling model, TLS was chosen as the Information Assurance protocol to secure AS-SIP since its hop-by-hop security model integrated nicely with the hierarchical signaling model. Fortunately, all AS-SIP signaling appliances are required to be DoD PKE and support the interoperability with a DoD-approved PKI. Currently, the process for obtaining a DoD-approved X.509v3 certificate is a manual process and has to be completed before or during the initial installation. Use of a certificate from a DoD-approved PKI, in combination with TLS, provides a secure process for signaling appliances to authenticate to each other, and the process must be completed before transmitting an AS-SIP signaling session to the remote AS-SIP signaling appliance. This UCR contains requirements that detail how this validation process, using certificates and AS-SIP signaling messages, must occur.

Figure 5.4.5-7 shows the process that must be completed before AS-SIP signaling is transmitted between AS-SIP signaling appliances.

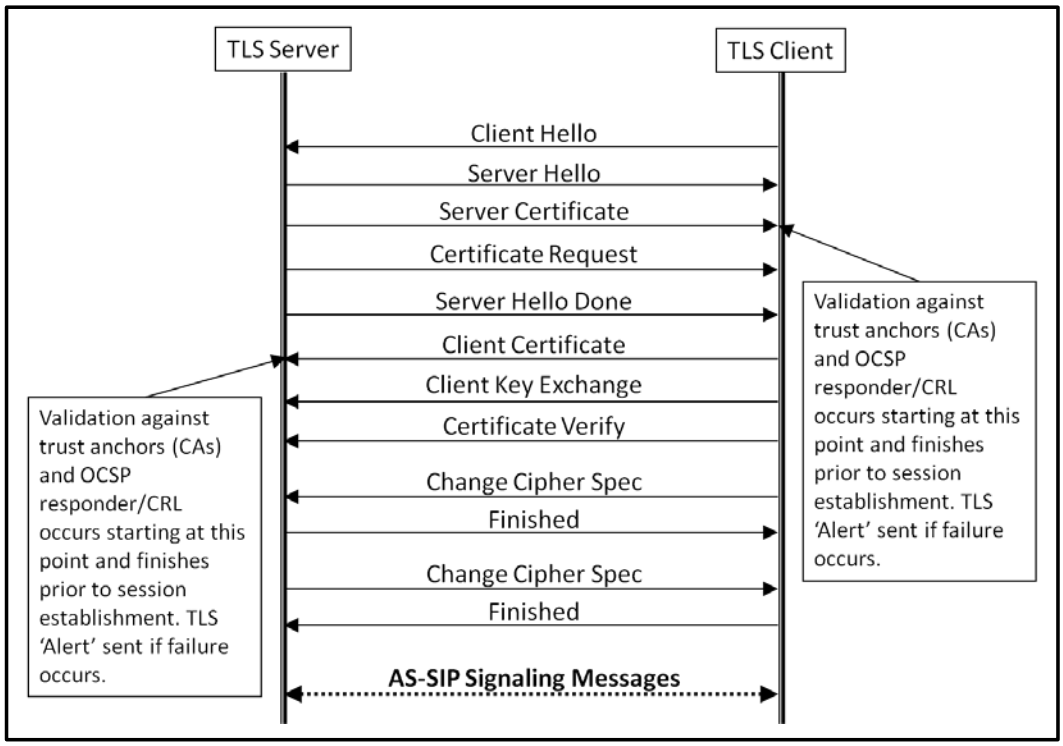

Figure 5.4.5-7. AS-SIP TLS Authentication Process

After a TLS session is established between the AS-SIP signaling appliances, the AS-SIP signaling messages are allowed to transit between the appliances if the appliance profile permits. Every signaling appliance in the path of a AS-SIP signaling session (with the exception of the EI, where it is Conditional) is responsible for receiving the AS-SIP packet, decrypting the packet, verifying the integrity of the packet, processing the packet IAW the AS-SIP specification, and

then encrypting the packet before transmitting it to the next hop. Figure 5.4.5-8, AS-SIP Signaling Appliance Packet Processing, shows this process.

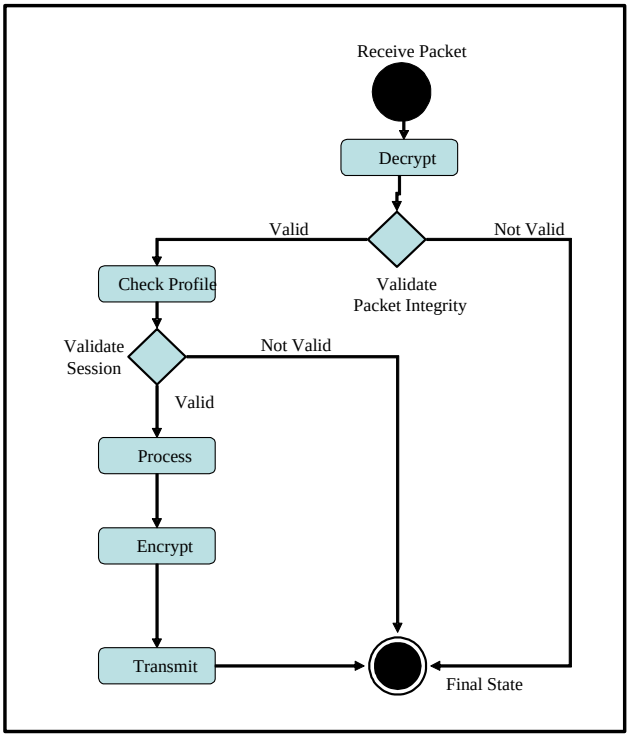

Figure 5.4.5-8. AS-SIP Signaling Appliance Packet Processing

5.4.5.4.4.2 H.323 and H.248

Several legacy protocols must be supported until the UCR 2012 timeframe. They include H.323, which is primarily used to support video sessions, and H.248, which is primarily used to communicate between an MGC and an MG. The LSC may interpret H.323 and H.248 for line-side connections (within a local domain or to the PSTN), but will translate the signaling to AS-SIP for trunk-side (WAN) signaling. If H.323 is used for trunk (WAN)-side signaling, it will involve a point-to-point signaling session that will bypass the LSC and extend directly to the remote EI or Multipoint Control Unit (MCU). The TLS can be used to secure H.245 channels within the H.323 protocols because it uses TCP. However, H.323 also is composed of H.225.0 and RAS protocols, and these protocols are not compatible with TLS if they are implemented with User Datagram Protocol (UDP) since TLS requires a reliable protocol (TCP or SCTP). As a result, IPSec was chosen as the protocol to secure H.323 and H.248 and this is IAW the DISA FSO "VVoIP STIG Checklist."

The mechanism used for H.323 authentication and key exchange is the Internet Key Exchange (IKE) protocol. The IKE is a standards-based approach developed by the IETF to support IPSec. It defines a method for establishing a security association (SA) that authenticates users,

negotiates the encryption method, and exchanges the secret key. The IKE is derived from the ISAKMP framework for key exchange and the Oakley key exchange technique. In addition, it is designed to support a PKI-like infrastructure, such as the DoD PKI.

5.4.5.4.4.3 Secure Bearer Path

In addition to securing the VVoIP signaling path, the VVoIP bearer path for EIs is also secured using the SRTP to provide confidentiality and integrity. Since the E2E signaling path was authenticated using TLS and the EIs are the origination and termination points for that path, the EIs authentication will be achieved via that hop-by-hop authentication. It is understood that a limitation of hop-by-hop authentication model is that it is only as strong as the weakest link. To understand the effect of this approach, an analysis was conducted that weighed the risk of a hop-by-hop security model with the benefit of reducing post-dial delay by eliminating the point-to-point authentication process between the EIs using the authentication provided by the TLS process. The result of the analysis was that the benefits outweighed the risks. Given that additional authentication is not required, the next concern is to reduce the delay associated with exchanging encryption keys.

This was accomplished by embedding the SRTP encryption key for the session in the AS-SIP INVITE message as part of the SDP within the AS-SIP packet IAW RFC 4568. H.248 is also capable of distributing the SRTP encryption key in the SDP portion of the H.248 using the same parameter. H.323 distributes the session key in the same manner using the H.235 key distribution mechanisms instead of using SDP. Since the AS-SIP messages are mutually authenticated, encrypted, and checked for integrity, the inclusion of the SRTP encryption key in the AS-SIP message provides a secure method for key exchange. In addition to providing a secure method for transport of the session key, it also allows the encrypted bearer stream to be transmitted as soon as the session setup is complete–critical for command and control (C2) as well as Tactical operations. The SRTP is used for both confidentiality and integrity of the bearer path. In determining the size of the hash needed to provide SRTP integrity, a cost benefit analysis was conducted that weighed the cost for each SRTP packet to process the hash and the IP overhead associated with the hash with the risk mitigated by a applying a larger secure hash. The analysis showed that a small hash (32-bit) was adequate to mitigate the risk given the large number of packets and the documented threats.

5.4.5.4.5 Network Management

Network management protocols are the final category of protocols that must be secured within the VVoIP environment. Since the Information Assurance framework leverages the DoD PKI for authentication, it is expected that all EMS personnel will be assigned a CAC or other DoD approved token and will use this credential for authenticating to the system. Once authenticated to the system using PKI, it is expected that the credentials from the token will be passed to the system to provide role-based access to the EMS based on the privileges assigned to the EMS

personnel (in other words, no secondary username or password should be required for authorization purposes). Network management protocols, for the purposes of this discussion, are separated into two categories dependent on whether they support traditional FCAPS (Fault, Configuration, Accounting, Performance, and Security)-related functions or directory services-type functions. At this time, the VVoIP Information Assurance design has not identified a requirement for the VVoIP systems (i.e., LSC, SS, MFSS, EBC, and CE Router) to interface the EMS using XML-based web services, and this UCR does not address the mechanisms that would be used to secure those services. Although the VVoIP systems do not use XML-based web services, the EMSs managing the VVoIP systems do use XML-based services for Information Sharing and have secure ways of providing the service. The Information Assurance approach used for the Information Sharing is not within the scope of this UCR. Appliances performing NM functions (i.e., LSC, SS, MFSS, MG, ADIMSS, and ARDIMSS) will use static IP addresses and they will not be assigned IP addresses by a DHCP server. Since the IP address can be published to the FCAPS personnel in advance, the session initiator will use the appropriate IP address (either IPv6 or IPv4) in their request, and IPv4 or IPv6 translation is not required between the terminal and the appliance.

The VVoIP Information Assurance design requires that every LSC and MFSS support a minimum of two Ethernet interfaces (to include redundancy on each interface). The two Ethernet interfaces are used to support 1) signaling and bearer traffic and, 2) the EMS. Using Information Sharing, the EMS (local or RTS EMS) will share FCAPS information with other EMSs to provide E2E management. Since there are multiple interfaces, the appliance must ensure that traffic transiting from one Ethernet interface to a different Ethernet interface is limited to authenticated and authorized traffic. For example, the LSC appliance must ensure that a user who has access to the signaling and bearer interface to establish a session is not allowed access to the local EMS network. An instance of transiting between interfaces occurs when an authenticated and authorized systems administrator logs in to an LSC to perform call tracing functions as part of a troubleshooting sequence. In this case, the system administrator entered the system through the EMS interface, but transmitted the traffic through the signaling and bearer interface. The external Ethernet interfaces are assigned to distinct VLANs IAW the types of traffic they support. Figure 5.4.5-9, VVoIP Product External Ethernet Interfaces, shows an example of the Ethernet interfaces found on an LSC and the access controls that may be configured to control traffic between the interfaces.

The first category of protocols is the protocols that support FCAPS. These have been defined as the SNMPv3, the SSHv2, and Secure Sockets Layer (SSL) Protocol version 3.1 (SSL3.1). The SNMPv3 builds on earlier versions of SNMP, but adds additional security mechanisms that are integrated into the protocol. Primarily, SNMP is used for minor configuration changes and for providing real-time status on the VVoIP appliances. The VVoIP Information Assurance design requires the use of SNMPv3 as a threshold requirement due to its significant improvement in the Information Assurance area over previous versions. However, it is understood that due to its newness, some solutions may have to use earlier versions of SNMP with the mitigations of the

appropriate patches, IPSec, and an upgrade plan for migrating to SNMPv3 due to their development cycles. The VVoIP Information Assurance design will use the SNMPv3 user-based security model.

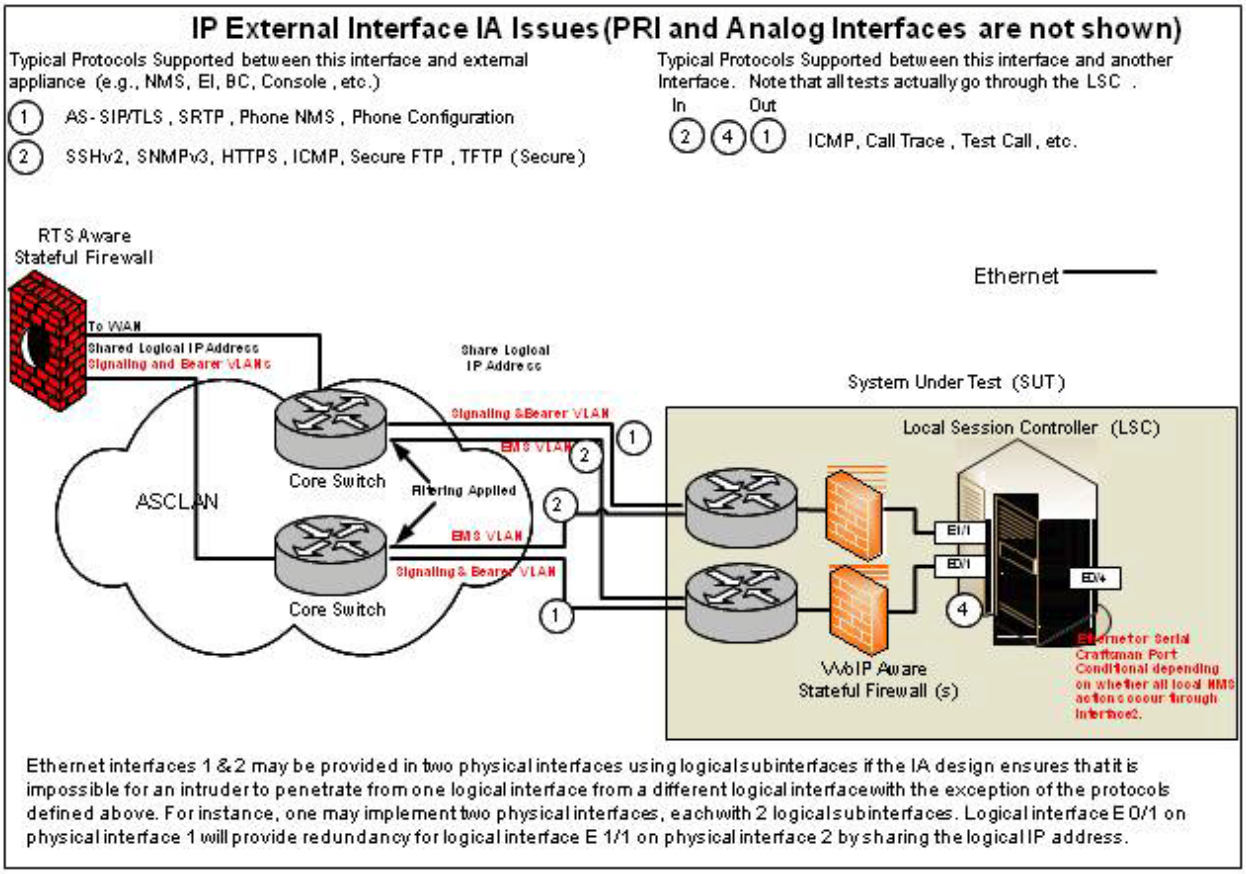

Figure 5.4.5-9. VVoIP Product External Ethernet Interfaces

Secure Shell version 2 is defined in RFC 4251 as a protocol for secure remote log-in and other secure network services over an insecure network. Primarily, SSHv2 is in the DoD VVoIP environment as a secure configuration and control protocol used by network engineers to access network elements to configure the appliances. NOTE: The EIs and AEIs will disable remote manual configuration after the initial installation is completed and should not allow remote manual configuration after the initial installation. In addition, all EI and AEI non-automatic processes shall be performed locally. The SSH protocol consists of the following three major components: the Transport Layer Protocol, User Authentication Protocol, and Connection Protocol. The Transport Layer Protocol provides server authentication, confidentiality, and integrity. The User Authentication Protocol authenticates the client to the server, and the Connection Protocol multiplexes the encrypted tunnel into several logical channels. The SSHv2 implementations must support the transmission of full X.509v3 certificates conditionally during session establishment.

The final protocol is the TLS, version 1.0 or higher, which for the purposes of this design is considered interchangeable with SSL3.1, unless TLS is identified specifically for interoperability purposes. The TLS is used within the NMS as an alternative to SSHv2 and is associated primarily with web-based NM GUIs. It provides a secure manner for authorized and authenticated network engineers to access VVoIP appliances to perform NM functions.

The second category of NM protocols is associated with location services. Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), is the protocol that will be used to interface between the RTS routing database and the LSC and SS. In addition to directory services, LDAPv3 may be used to interface with portions of the DoD PKI and is designed to provide access to directories supporting the X.500 models, while limiting the resource requirements associated with other protocols. The LDAP is nothing more than an access protocol and does not require the underlying directory database to be based on any particular technology. In addition, LDAPv3 is designed to integrate with TLS in a similar manner to AS-SIP. The TLS is used with LDAP to provide confidentiality, integrity, and authentication for information in transit in combination with the use of the DoD-approved PKI certificates. NOTE: The use of TLS does not provide or ensure confidentiality and/or non-repudiation of the data housed by an LDAP-based directory server, and it does not secure the data from inspection by the server administrators.

5.4.5.4.6 AS-SIP End Instruments

End instruments can be placed into two broad categories on the basis of the signaling protocols that are used to communicate with the LSC to set up the call. These categories are “vendor proprietary” and “AS-SIP.”

Vendor proprietary EIs are EIs that use vendor-proprietary signaling interfaces between the LSCs and itself. Both ITU H.323 and IETF SIP (commercial SIP, not DISA-specified AS-SIP) also are considered vendor-proprietary EI to LSC protocols in this UCR. They are treated as vendor-proprietary protocols because one EI vendor’s implementation of H.323 or SIP is not guaranteed to interoperate with another LSC vendor’s implementation of H.323 or SIP.

The AS-SIP EIs are EIs that use AS-SIP between the LSCs and the AEI itself. The AEIs from any AEI vendor operate on any LSC vendor’s product, using the AS-SIP-based LSC-to-AEI interface.

5.4.5.4.6.1 Secure VVoIP End Instruments

Secure EIs are NSA Type-1 certified VVoIP terminals that support the E2E transmission of classified VVoIP media traffic. In addition, Secure EIs can be placed into “vendor proprietary”

and "AS-SIP" categories on the basis of the signaling protocols that are used to communicate with the LSC to set up the call.

Currently, the Secure EI is designed to rely on the SCIP standard (the FNBDT standard was renamed SCIP in 2004), which allows for E2E secure communications regardless of whether the terminal is on an IP (DISN), DSN, PSTN, ISDN, cellular wireless, or radio network. The Secure EI relies on SCIP transported over either V.150.1 or SRTP within to transmit classified voice and data across DoD IP networks. Per NSA mandates, Secure EIs operating within the UC VVoIP environment are expected to adopt the AS-SIP protocol as the default VVoIP signaling protocol.

5.4.5.4.7 Edge Boundary Control Appliances

The VVoIP Information Assurance design uses two appliances to defend the boundary between the Customer Edge Segment and the Network Edge Segment. The first appliance is called the EBC and its function is to act as a VVoIP aware firewall, performing functions similar to those identified in RFC 5853 "Requirements from Session Initiation Protocol (SIP) Session Border Controller (SBC) Deployments." The second appliance is called the CE Router, and its primary functions are associated with QoS and perimeter defense. Figure 5.4.5-4, VVoIP Proprietary and Standards Based Protocols, shows the location of the EBC and the CE Router. Both appliances must be highly reliable (i.e., 99.999 percent available) and IPv6 capable using a dual stack.

The CE Router is responsible for providing traffic conditioning (policing and shaping) on inbound and outbound traffic to ensure that the performance requirements are met for both the Network Edge Segment and the Customer Edge Segment. This is one of the defense-in-depth mechanisms used to prevent a DoS attack by ensuring that only a predetermined number of signaling or VVoIP sessions may transit the CE Router at a particular instance of time. It is understood that this only prevents the Customer Edge Network from being affected by a DoS attack and that the external connectivity may be affected. The granularity of the traffic conditioning is to the level of the granular service class, such as voice or video. Currently, the configuration changes associated with traffic conditioning will be a manual process. However, it is hoped that the Fiscal Year (FY) 2012 design will incorporate dynamic traffic conditioning based on policy. To achieve this vision, an interface must be defined for communication between the AS-SIP signaling appliance (i.e., LSC or SS) and the CE Router to ensure that the AS-SIP signaling appliance budgets are consistent with the CE Router traffic conditioning parameters. In addition, the CE Router must have the capability to provide QoS for VVoIP by supporting the per-hop behaviors (PHBs) based on the DSCP markings that will be defined by the QoS Working Group.

Primarily, the EBC is focused on perimeter defense. Real time services suffer from certain difficulties with traditional perimeter defense mechanisms, such as NAT and data firewall behavior. Many protocols designed by the IETF used within the VVoIP environment, such as SIP, are designed as E2E protocols. The E2E model is broken by the presence of firewalls and

NAT appliances. In large deployments of VVoIP, such as the DISN, a specialized appliance is needed to facilitate the coexistence of VVoIP and perimeter defense mechanisms. The DoD VVoIP Information Assurance design has labeled this specialized appliance as an EBC to distinguish it from similar commercial appliances that do not have unique DoD requirements. Before describing the requirements and functions associated with the EBC, it is important to explain the difficulties that VVoIP protocols experience crossing network boundary devices and to explain the common types of solutions available in the commercial market that leverage commercial standards. Following this discussion, a general discussion of the requirements associated with an EBC will be provided.

As mentioned previously, the use of NAT introduces several problems to an E2E protocol security model. The use of NAT is required at the WAN boundary by the DISA FSO "VVoIP STIG" and the DISA FSO "Network Infrastructure STIG." In a traditional NAT employment, the NAT is conducted at the Network Layer (Layer 3) of the Open Systems Interconnect (OSI) model (Network Address Port Translation (NAPT) is conducted at Layer 4). However, the DoD VVoIP environment requires that the EBC perform NAT at a higher layer to process the AS-SIP messages properly. The common scenario provided for NAT is the use of private addressing in two remote enclaves, with a public address space in the interconnecting WAN.

During the initial AS-SIP offer/answer exchange, both the originating and terminating AS-SIP User Agents (UAs) will specify in the SDP payload the desired IP address and port combination for the caller and called party to receive the associated media stream and to direct the signaling stream properly. The AS-SIP UAs within the Customer Edge Segment may use private addressing for topology hiding reasons. A problem occurs when private addressing is used within the SDP payload since the private address is not resolvable from the WAN side of the NAT. A traditional NAT device will change the IP source address and/or port combination at packet header level, but not the IP address within the SDP payload. Consequently, the called party, or UA in the remote enclave, will not have the correct IP address to respond to from a signaling perspective and the call setup will fail. Even if the call is established from a signaling perspective, the bearer stream would be sent to the wrong address or port and the session would not be established.

An additional problem is that the signaling and bearer paths are different IP sessions and the NAT bindings in a traditional NAT appliance are finite in nature (not correlated). A scenario may result where a VVoIP session may continue for many minutes with active Real Time Protocol (RTP) streams, but no signaling messages. Since there is no signaling, the signaling NAT binding could time out, and the session would not be able to end properly.

Difficulties experienced by AS-SIP signaling and RTP/Real Time Control Protocol (RTCP) media protocols passing through firewalls stem mainly from bearer stream port numbers that are selected dynamically for each call from a large pool of potential port numbers. Allowing this large range (typically around 20,000 UDP ports for a large MILDEP) of potential port numbers

to be open at the enclave boundary is unacceptable. The EBC needs to know which ports to open temporarily, when to open them, and when to close them. Placing this functionality (essentially an Application Level Gateway) into data firewalls carries with it some disadvantages, for example, having the firewall perform actions it is not supposed to handle.

Solutions for these issues have evolved slowly within the standards bodies and major equipment vendors. A myriad of suggestions have been offered from both communities. Efforts have included work from the IETF's Middlebox Communication (MIDCOM) Working Group, which closed in March 2008. The envisioned MIDCOM design provided for a protocol link between the LSC and the boundary device, a firewall or NAT device, called a middlebox, for opening and closing pinholes in the middlebox. The MIDCOM Working Group never completely achieved its goal, but certain pre-MIDCOM solutions, such as Simple Tunneling of UDP through NAT (STUN) and Interactive Connectivity Establishment (ICE), have been implemented in freeware projects and in some products. Widespread deployment of technologies such as STUN, Traversal Using Relay NAT (TURN), and ICE has not happened as of this writing, though a number of RFCs have emerged that may improve more standardized, widespread usage. Also, other developments within the IETF include RFC 5853, completed in April 2010, which specifies high-level functions and issues for SIP Session Border Controller (SBC) deployments. In the interim, some vendors have developed limited solutions for their products to allow functionality, and several have acquired EBC functionality to enhance their product lines; however, no clear solution to achieve multivendor interoperability has come out of the major vendor arena. As a result, interoperability problems often occur between different vendor solutions due to the proprietary nature of the vendor-unique solutions.

Some of the difficulty with solutions coming from the standards arena is an aversion to dealing with middleboxes at all. Originally NAT was meant to be a short-term solution to the IP address depletion problem. Many application protocols are designed to be E2E in nature, and firewalls and NAT devices break this E2E nature of many protocols. Other arguments say that middleboxes prevent application layer protocols from protecting themselves by breaking the E2E security model. Standardization of NAT behavior has not occurred and has resulted in NAT implementations that behave differently from vendor to vendor. Another IETF working group, the Behavior Engineering for Hindrance Avoidance (BEHAVE) working group, was formed to identify, classify, and understand these behaviors to bring some standardization to them but the end state of a standardized behavior has not been achieved.

In response to a need for a solution to various problems with VVoIP in the areas of firewall/NAT traversal, topology hiding, and lawful intercept, a large number of startup companies have produced a solution that has come to be known as SBC. These products may provide functionality in one or more areas, but there is no standardization among the producers of these products, and currently, they do not meet the DoD-unique requirements associated with the processing of AS-SIP, so it is necessary for the DoD to specify precisely the functionality required in these solutions.

The result of this situation is that the DoD has defined an EBC system that is placed at the boundary between the Edge segment and the Access segment to provide four critical functions: topology hiding, "pinholing," filtering, and VVoIP IPS traffic monitoring.

Topology hiding is accomplished by processing the AS-SIP messages and performing the appropriate IP address and port translations within the IP header and the SDP payload. Figure 5.4.5-10, Typical End-to-End AS-SIP Call Flow, shows the typical call flow associated establishing an AS-SIP session. The diagram shows how the media is bidirectionally anchored by the EBC to ensure that topology hiding is provided IAW the DoD requirements.

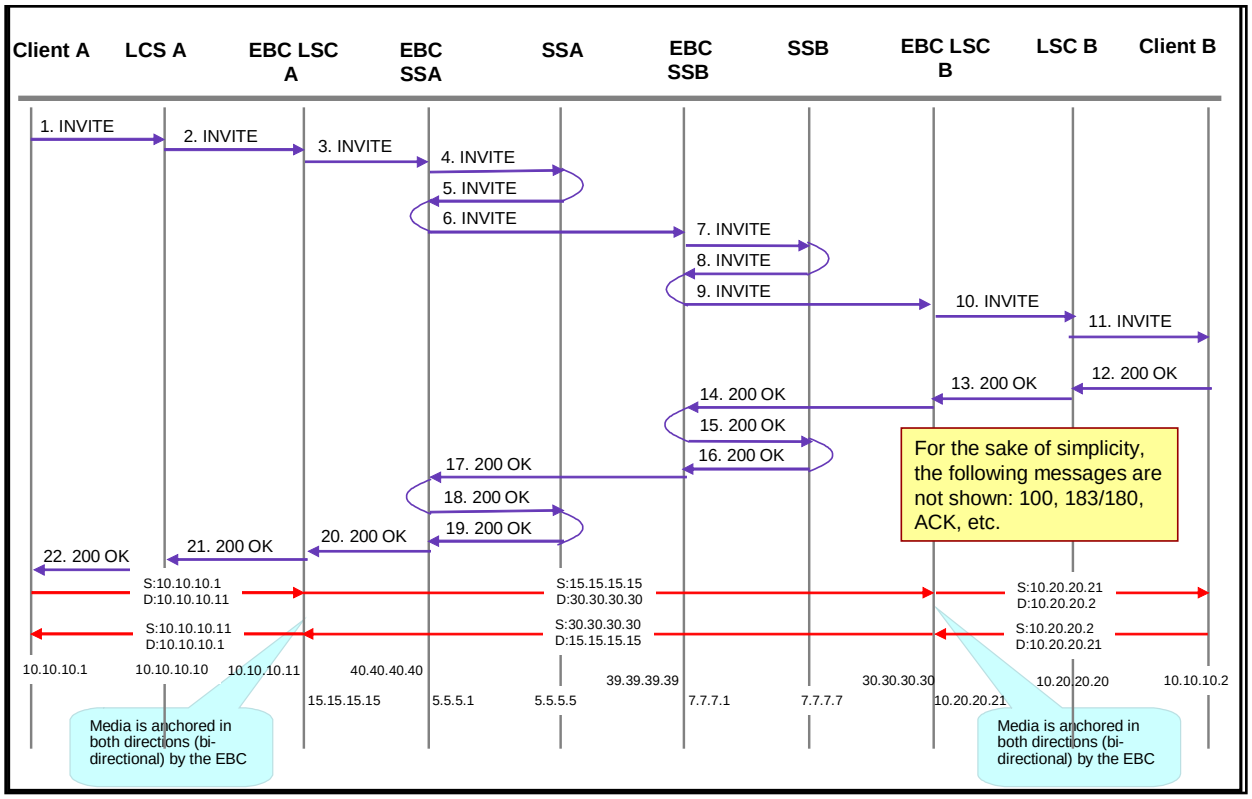

Figure 5.4.5-10. Typical End-to-End AS-SIP Call Flow

Several issues are encountered by EBCs in attempting to meet the topology hiding requirements due to the VVoIP signaling hierarchy and by the requirement to allow call forwarding and call transfer. The first issue is found in EBCs that front an SS component of an MFSS. Upon receipt of an AS-SIP INVITE, the EBC does not know whether that session terminates within the enclave, or will be forwarded to another enclave (after processing by the SS). Due to the uncertainty, the EBC must anchor the media stream bidirectionally. If the SS returns the INVITE to the EBC for forwarding to the next hop, the EBC must restore the original IP address and port number so that it is no longer involved in the media stream associated with that session.

Figure 5.4.5-11, Media Anchoring for Transitive SIP Signaling, shows the process associated with transitive SIP signaling for an EBC that fronts the SS component of the MFSS.

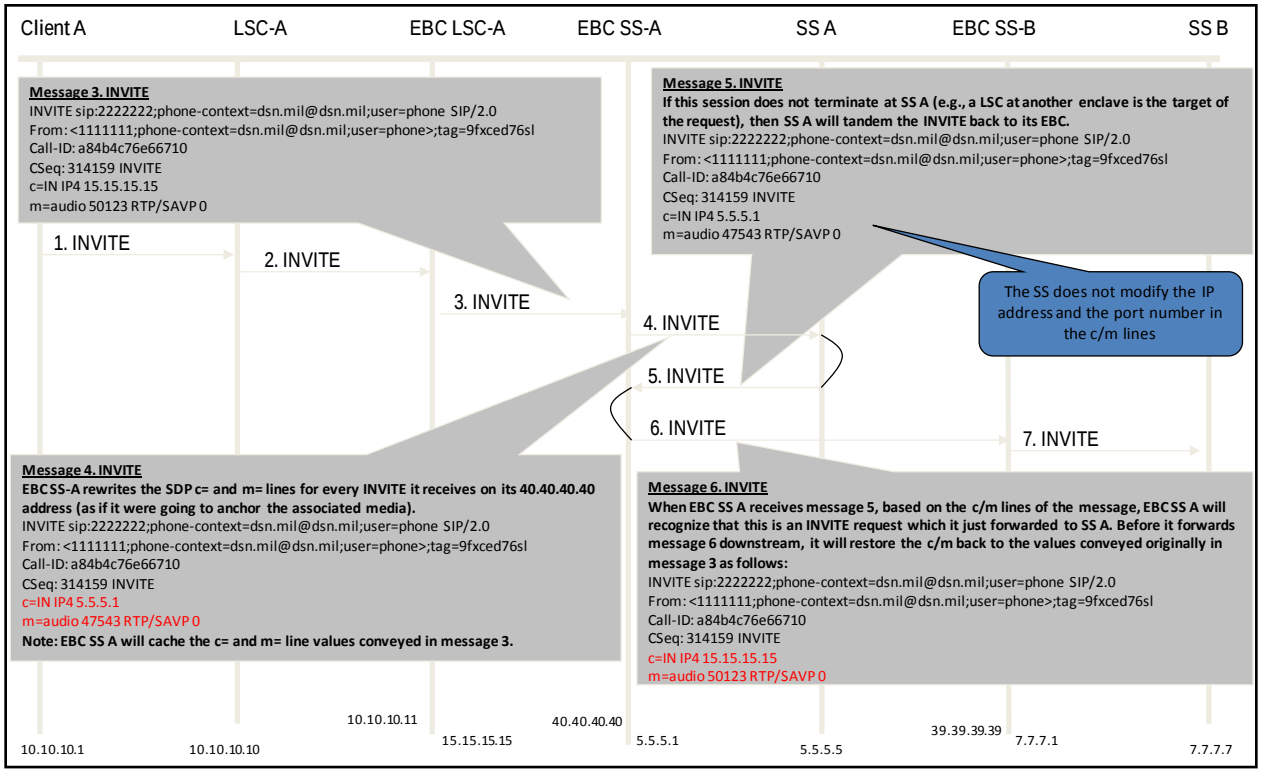

Figure 5.4.5-11. Media Anchoring for Transitive SIP Signaling

The second issue associated with topology hiding is related to call forwarding and call transfer scenarios where the session no longer terminates within the enclave. Upon notification that a session is being forwarded or transferred, the EBC associated with the forwarding or transferring party must restore the original IP address and port number associated with that session to ensure that the media is not anchored improperly at the enclave since the session is no longer associated with the enclave. The process used is similar to the process described in Figure 5.4.5-11, Media Anchoring for Transitive SIP Signaling.

The next issue concerns the ability of the EBC to determine the appropriate next hop for signaling. For an EBC fronting an LSC, the EBC has only a primary and secondary TLS path in which to forward the AS-SIP messages. The primary TLS path is to the EBC fronting the primary MFSS for the LSC and the secondary path is to the EBC fronting the secondary MFSS for the LSC. However, for an EBC fronting the SS component of the MFSS, it has many TLS sessions associated with the subtended LSCs of the MFSS and with the other primary and secondary MFSSs for all the remote LSCs. Since the EBC does not have its own location service, it must rely on the SS component of the MFSS to inform it of the appropriate next hop. The SS informs the EBC of the next hop using the Route header construct defined in the RFC

3261. NOTE: This issue is not relevant to INVITEs arriving from the WAN, since the EBC is associated with one and only one AS-SIP signaling system on the line side and always forwards INVITEs arriving from the WAN to its associated AS-SIP signaling system (i.e., LSC or MFSS). In addition to performing topology hiding, the EBC provides several other functions to include "pinholing."

"Pinholing" is accomplished by opening and closing "pinholes" that only allow approved sessions to transit the EBC based on the AS-SIP messages. The coupling of the signaling and bearer stream requires that both streams must transit the EBC. If H.323 video is transiting the EBC too, the pinholes may be associated with the H.323 messages also. In addition, the EBC must have a timer associated with each pinhole to ensure that pinholes do not remain open indefinitely if a signaling message is not received to close the pinhole. If the EBC closes the pinhole, it must send a BYE message in each direction to notify the next hop signaling appliances that the session has been terminated.

Filtering is accomplished by allowing targeted IP flows to transit the EBC based on their "6 tuple," which in VVoIP consists of the:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- DSCP
- Protocol identifier

Compared to pinholes, filtering is a manual process and is not dynamic in nature. A type of traffic flow associated with filtering is an SNMPv3 session from the EMS to an LSC that is active all the time and is well defined. If the EBC detects an anomalous condition (e.g., DoS attack, abnormal number of invalid AS-SIP requests), it must have the ability to notify the appropriate EMS of the event.

The EBC is required to provide either an onboard VVoIP-specific IDS/IPS capability or an interface to external VVoIP IDS/IPS, which can monitor the VVoIP signaling and media traffic for potential threats. The EBC represents the ideal location for such a capability, because generally the EBC is the only place in the system, other than the endpoints, where signaling and media traffic transit the same component. The VVoIP IDS/IPS does not have to be a separate, independent component from the data IDS/IPS already in use at the site provided that the existing IDS/IPS provides the required VVoIP monitoring capabilities. If an external IDS/IPS interface is provided by the EBC, the interface must be secure and must minimally meet the security profiles defined for IPSec and TLS in this UCR.

5.4.5.4.8 RTS Stateful Firewall

The role of the RTS stateful firewall (RSF) is to protect an LSC, SS, or MFSS from attacks that originate from inside the enclave. The placement of the RSF within the LAN is displayed in Figure 5.4.5-2, Notional Example of Voice, Video, Softphone, Multifunction Mobile Device, Videophone, and Data ASLAN Segmentation. In most deployment scenarios the LSC, MFSS, and WAN SS provide a sufficient Information Assurance posture to be deployed without an RSF. Therefore, the use of the RSF is not a mandatory requirement. However, some MILDEPs may determine that additional protection is required because of the risks associated with their unique scenario (i.e., a large regional MAN). When this occurs, the RSF may be deployed to provide additional protection. The RSF is similar to an EBC and may be an EBC. However, the RSF is only required to support a subset of the EBC requirements. For example, the RSF is not required to support NAT and NAPT and is not required to support Route headers to support failover scenarios. The primary requirement that is added to an RSF that is not applicable to an EBC is the support of both TLS dual path and reuse methods. The RSF needs to support both methods since it will be involved in the SIP dialogues between the LSC and the AEIs and the LSC and proprietary SIP EIs. Since proprietary EIs have an option to implement both TLS methods, the RSF needs to support both methods. The EBC is not involved in TLS sessions between the LSC and EIs and only needs to support AS-SIP TLS sessions, which use the dual path method.

5.4.5.5 Security Devices

A detailed discussion of UC security devices and their functionality occurs in Section 5.8, Security Devices Requirements, of this UCR and will not be repeated here. This section of this UCR contains the "general" Information Assurance requirements for the security devices defined in Section 5.8. However, functional requirements for security devices or non-generic Information Assurance requirements specific to only a certain security device are captured in Section 5.8.

5.4.6 Requirements

5.4.6.1 Introduction

For the components comprising the UC Information Assurance design, a set of derived requirements were developed based on the analyzed threats and countermeasures. Different vendors combine different functions into their appliances to meet the requirements of a particular type of product. The requirements are levied on the individual appliance, as applicable, to secure the entire product. In many cases, the system is composed of multiple appliances. For example, typically an LSC is composed of a Call Connection Agent, a media server, a configuration server, a voicemail server, and other servers. Due to the wide variation in vendor products, it is impossible to break out the requirements for each component of a system and the reader should

apply the higher level requirements to that component unless specifically stated. An example is that the LSC requirements apply to a media server since it is not specifically called out. However, MG and EI requirements are called out specifically; therefore, the LSC requirements do not apply to them. The Information Assurance design provides a high-level description of how the security services are applied to the appliance and how the appliances interact in a secure manner. In addition, the appropriate STIGs will further clarify how the Information Assurance design and requirements are implemented on the appliance.

During information assurance testing at approval DoD laboratories, UC APL products are testing against the UCR requirements in this section and information assurance requirements found in other Sections of the UCR (e.g., 5.3.5, 5.8), as applicable, in addition to the STIGs. For all products not directly addressed within Section 5.4 or other UCR sections from an information assurance perspective, information assurance testing for the product will include testing against all applicable STIGs.

The requirement key words (i.e., Required, Conditional) are defined elsewhere in this UCR. Failure to satisfy a requirement will result in a UCR Category I, II, or III finding.

Finally, the requirements that follow do not include all administrative requirements (nontechnical) associated with policy and the STIGs. For instance, if someone is required to document something administratively (e.g., waiver, pilot request) as part of site accreditation, that requirement is not included. Table 5.4.6-1, Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

This section of the UCR generally does not address IPv6 related requirements. Section 5.3.5 shall be used for IPv6 requirements for all components unless otherwise stated within this section.

5.4.6.1.1 The [Alarm] Tag: Generation of Alarms

When the **[Alarm]** tag appears after a requirement's applicability statement (e.g., Required and Conditional), this indicates that the product must support, at a minimum, the capability to perform the following functions in addition to complying with the specified requirement:

1. Generate an alarm to the NMS based on the alarmable actions identified in the requirement using the configured alarm transmission mechanism (e.g., SNMP, syslog, e-mail, pager).

2. Record an entry in the product's system and audit logs indicating that the event occurred.

Table 5.4.6-1. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MFSS	Multifunction Softswitch
SS	Softswitch
LSC	Local Session Controller
MG	Media Gateway
EBC	Edge Boundary Controller
RSF	RTS Stateful Firewall
EI	End Instrument (Including Multipoint Conference Units (MCUs) and other devices which provide EI-equivalent functionality on their respective interfaces)
AEI	AS-SIP End Instrument (including MCUs and other devices which provide AEI-equivalent functionality on their respective interfaces)
LS	LAN Switch
R	Router
FW	Data Firewall
VPN	Virtual Private Network Concentrator and Termination
IPS	Intrusion Detection/Prevention System
NAC	Network Access Controller

This tag is intended to facilitate rapid identification of all those requirements that result in alarm conditions by automated requirement management tools.

5.4.6.2 General and VVoIP Component Requirements

1. **[Required: MFSS, SS, LSC, MG, EBC, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall conform to the following requirements:

   a. Reserved.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC, R, LS]** The appliance shall only have applications or routines that are necessary to support its designated function.

   NOTE: The disabling or deletion of applications or routines via hardware or software mechanisms shall satisfy this requirement. For example, in the case of a VVoIP appliance, if an appliance by default is installed with a web browser and the web browser is not needed to support VVoIP, then the application shall be removed from the appliance. Another example is if a feature is part of the application, but is not needed in the DoD environment that feature shall be disabled via hardware or software mechanisms.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** The product shall not contain unauthorized compilers, editors, and other program development tools within its operational system boundary.

c. Reserved.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product is designed to accept automatic software updates, the product shall only accept automatic software updates if they are cryptographically signed by the software vendor and the system validates the signature before installing.

NOTE: It is assumed that manual updates will be validated by an authorized administrator before installation.

NOTE: For JITC testing purposes, the vendor must provide a mock software update server to verify compliance with this requirement.

d. **[Required: FW, IPS, VPN, NAC]** The product shall be National Information Assurance Partnership (NIAP) validated against the NIAP validated process for that technology.

NOTE: The NIAP program office determines whether Common Criteria (CC) mutual recognition can be used to satisfy this requirement. Protection profiles or a NIAP approved security target, if no protection profile exists, will be used during the product's evaluation.

NOTE: Evaluations completed against retired protection profiles/security targets will be accepted if the NIAP PMO deemed the protection profile/security target acceptable at the time the product entered the NIAP validation process.

(1) Reserved.

2. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If the product uses public domain software, unsupported software, or other software, it shall be covered under that system's warranty.

NOTE: If a vendor covers in its warranty all software, regardless of its source, within their product then this requirement is met. An example of unsupported software is Windows NT, which is no longer supported by Microsoft and it is unlikely that a vendor would support this operating system as part of its system.

a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** The products shall only use open source software if all licensing requirements are met.

NOTE: It is anticipated that the Government will accept an LOC from a vendor as a means of satisfying this requirement. Open source software refers to software that is copyrighted and distributed under a license that provides everyone the right to use, modify, and redistribute the source code of the software. Open source licenses impose certain obligations on users who exercise these rights. Some examples include publishing a copyright notice and placing a disclaimer of warranty on distributed copies.

3. Reserved.

4. **[Conditional: EI, AEI]** If the softphones are used in remote connectivity situations, the product shall be capable of supporting a VPN for VVoIP traffic from the PC to the Enclave VPN access router or node.

NOTE: The data from the PC and VVoIP traffic from the PC softphone must be separated into the appropriate VLANs at the earliest point in the path.

5. Reserved.

a. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** If the BIOS settings are configurable, the product shall be capable of enabling password protection of BIOS settings.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** The product shall be capable of disabling the ability to boot from a removable media.

6. **[Conditional: EI, AEI]** If the product has a speakerphone, the system shall be capable of disabling the speakerphone microphone.

NOTE: Acceptable methods for meeting this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter.

7. **[Conditional: EI, AEI]** If the product is used in a sensitive area where NSS are used and/or within environments where national security information (NSI) is stored, processed, or transmitted, then the system shall be certified and accredited IAW the Telephone Security Standard (TSG) 6, which is prepared by the National Telecommunications Security Working Group (NTSWG).

8. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall be capable of using a static IP address.

9. Reserved.

10. Reserved.

11. **[Required: MFSS, SS, LSC, EBC, MG, AEI, EI]** When the system assigns the port numbers to a session, the system shall assign the SRTP port ranges within a configurable range between 2048 and 65535 with the default between 16384 to 32764.

12. **[Required: MFSS, SS, MG, LS, EBC, RSF, R, LSC, AEI, EI, FW, IPS, VPN, NAC]** The product by default shall disable any "call home" features or features that would result in unauthorized transfer of information to an external network.

5.4.6.2.1 Authentication (Includes Authorization and Access Control)

5.4.6.2.1.1 Banners

1. Reserved.

   a. Reserved.

   b. Reserved.

   c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product banner shall be capable of being configured by authenticated and authorized personnel.

   d. Reserved.

   e. Reserved.

      (1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** The product shall record the acknowledgement in the audit log in association with the administrator or user name.

      NOTE: If the acknowledgement is an essential step in the successful log-on process, then it is sufficient to only log the completion of a successful log-on.

   f. Reserved.

(1) Reserved.

(2) Reserved.

5.4.6.2.1.2 System User Names and Passwords

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** Every communicating system entity (i.e., persons, processes, or remote systems) shall be identified by an entity identifier that is unique within the domain of the appliance or application to which the system entity is connected.

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing a primary access control method that is stronger than assigning passwords to specific actions (e.g., operations-related commands) although assigning passwords may be used to augment access control.

      NOTE: If such a password is assigned, it loses its confidentiality because it has to be shared among all authorized users.

   b. Reserved.

      (1) Reserved.

      (2) Reserved.

         (a) Reserved.

      (3) Reserved.

      (4) Reserved.

         (a) Reserved.

         (b) Reserved.

      (5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** After a password is assigned to a human user, when that user establishes a session for the first time, the product shall be capable of prompting the user to change the password and deny the session if the user does not comply.

(6) Reserved.

(a) Reserved.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of setting the password aging interval on a "per-user ID basis."

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall notify the user a specified period of time before the password expiration.

ii. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall notify the user upon password expiration, but allow a specified additional number of subsequent log-ons within a specified time period before requiring a new password.

A. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The default for the number of subsequent log-ons shall not be greater than three.

B. Reserved.

iii. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall not hard code the notification mechanism for password expiration to allow for variation in variables such as "early warning period," "grace period," and subsequent log-on after password expiration.

(7) Reserved.

(a) Reserved.

(8) Reserved.

(a) Reserved.

(b) Reserved.

(c) Reserved.

(d) Reserved.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall be capable of ensuring that a "null" password is not possible.

(f) Reserved.

(9) Reserved.

(a) Reserved.

(b) Reserved.

(c) Reserved.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** The product shall ensure that it does not prevent a user from choosing (e.g., unknowingly) a password that is already associated with another user ID (Otherwise, an existing password may be divulged).

(11) Reserved.

(12) Reserved.

(13) Reserved.

(14) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If PINs are used for passwords, the product shall have a configurable parameter for the PIN length and the range shall be between four and twenty characters with a default of four characters.

NOTE: All password requirements defined in this section apply to PINs when used as passwords.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If PINs are used for passwords, the product shall ensure that only numbers are allowed (i.e., no "#" or "*").

c. Reserved.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If PINs (user IDs) are used for user identification, the product shall have a configurable length between six and twenty characters and the default shall be six characters.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If PINs (user IDs) are used for user identification, the system shall only use numbers (i.e., no "#" or "*") when assigning the PIN (user ID).

NOTE: The uniqueness rules for the PIN (user ID) are the same as for any user ID as described in the following requirements.

d. Reserved.

(1) Reserved.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** At any given instance of time, the product shall be capable of internally maintaining the identity of all user IDs logged on at that time.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of associating a process that is invoked by a user or customer with the user ID of that user.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of associating a process that is invoked by another process, with the ID of the invoking process.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of associating autonomous processes (i.e., processes running without user or customer invocation) with an identification code (e.g., "system ownership").

NOTE: An example of this would be a daemon on a UNIX workstation.

f. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** A product shall have the capability to deny access to a user ID after a configurable specified time interval, if that user ID has never been used during that time interval.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** This capability shall be either an autonomous disabling of the user ID by the product along with an alarm/alert to notify the appropriate

administrator, or an alarm/alert generated by the product for an appropriate administrator who then, depending on the policy, may disable or delete the user ID by using appropriate commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** A disabled or deleted log-on ID shall not be re-enabled by the user or another application user.

(3) Reserved.

g. Reserved.

h. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** An attempt for a specified user (e.g., administrator) to log on to the network a configurable number of times shall cause an alarm to be sent to the NMS unless an exception is granted per site policy.

NOTE: Example: If a user should only be logged on once to the network, but the user attempts to log on while an active session for the same user is ongoing, this case could indicate a compromise of the user's credentials. Therefore, an alert must be sent to the appropriate administrators if configured.

i. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** The product shall be capable of immediately notifying the user of a failed log-on (i.e., "Login Failed"). The error feedback generated by the system after the user authentication procedure shall provide no information other than "invalid," (i.e., it shall not reveal which part of the user-entered information (user ID and/or authenticator) is incorrect). Information such as "invalid user ID" or "invalid password" shall not be reported.

NOTE: It is acceptable to return a generic message such as "Account Locked" or "Account Disabled."

(2) Reserved.

(a) Reserved.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC] [Alarm]** The product shall be capable of providing a mechanism to immediately notify (in real time–within 30 seconds) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.

(4) Reserved.

j. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If the system supports the capability to create temporary or emergency accounts, the system shall provide the capability to automatically terminate these accounts after a configurable time period.

5.4.6.2.1.3 User Roles

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall be capable of having different types of user's roles and using Role-Based Access Control (RBAC) in the local and remote administration of all device functions and operations.

NOTE: Section 5.4.5.2.1, User Roles, defines an example set of user roles. A vendor may rename the user roles as long as the requirements are met. The user roles are used for originating VVoIP sessions and for NM functions.

a. **[Required: MFSS, SS, LSC]** The product shall be capable of having at least five types of user roles: a system security administrator (e.g., auditor), a system administrator, an application administrator, a privileged application user, and an application user.

b. **[Required: R, LS, EBC, RSF, MG]** The product shall be capable of having at least three types of user roles: a system security administrator (e.g., auditor), a system administrator, and an application administrator.

c. **[Required: EI, AEI]** The product shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user.

NOTE: The product demonstrates the ability to support a privileged application user by being able to dial precedence digits to signal the LSC the precedence of the session.

d. **[Required: EI, AEI]** The product shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.

e. **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product default user role shall be an application user.

f. **[Required: R, LS, EBC, RSF]** The product default user role shall be an application administrator.

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall be capable of working properly without Super User access privileges for any user application roles (system security administrator, a system administrator, an application administrator, and application user).

h. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The security functions performed by an appropriate administrator shall be identified and documented.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the ability to enable or disable the administrator's account is an option of a product, the products shall not require that the account be enabled or activated during normal operation.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions:

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Display all users currently logged on to the product.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Monitor the activities of a specific terminal, port, or network address of the system in real time.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Authorize users.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Revoke Users.

(f) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Lock out and restore a specific system port or interface and shut down unused interfaces.

(g) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Identify all resources accessible to any specific user along with the associated privileges required to access them.

NOTE: Resources (e.g., files, applications, processes) should be denied to users unless specifically authorized access.

(h) Reserved.

(i) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Disable or allow manual deletion of a user ID after a specific period during which the user ID has not been used.

(j) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Reinstate a disabled user ID.

(k) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Delete a disabled user ID.

(l) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Create or modify a password associated with a user ID.

(m) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Delete a user ID along with its password.

(n) Reserved.

(o) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define a password aging interval.

(p) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the interval during which an expired password of a user shall be denied reusing a password.

(q) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.

(r) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the duration of session lockout, which occurs when the threshold on the number of incorrect log-ons is exceeded.

(s) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Specify a customized advisory warning banner that is displayed upon valid system entry.

(t) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the duration of the time-out interval.

(u) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the privilege of a user to access a resource.

(v) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Define the privilege of an interface or port to be used to access a resource.

(w) Reserved.

(x) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Permit the retrieval, copying, printing, or uploading of the security log.

(y) Reserved.

(z) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Provide a mechanism to specify the condition that would necessitate uploading the security log to avoid an overwrite in the buffer.

(aa) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Provide a capability to validate the correct operation of the system.

(bb) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Provide a capability to monitor the system resources and their availabilities.

(cc) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Provide a capability to detect communication errors above an administrator-defined threshold. The types of communications errors that must be detected include abnormally large numbers of received packets that fail decryption and/or fail to pass integrity checks (e.g., failed CRC or hash function computations).

(dd) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** View the configuration of the product during operation.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product implements SNMP, the product shall minimally support the capability for the appropriate administrator to configure the following SNMP traps:

(a) Link Disconnect ("Link Down")
(b) Link Reconnect ("Link Up")
(c) Power Cycle ("Cold") Restart
(d) Software ("Warm") Restart

NOTE: Additional SNMP traps for certain devices are defined in Section 5.3, IP-Based Capabilities and Features.

i. Reserved.

j. Reserved.

k. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the system provides remote access, the system shall be capable of limiting user access based on a time of day interval (i.e., duty hours).

NOTE: Even during the times where remote access is restricted, local access is still permissible for emergency situations.

l. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Products providing remote access shall be capable of limiting user access based on IP address and/or MAC address as appropriate.

m. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The device shall associate all user security attributes with an authorized user.

n. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The device shall allow and maintain the following list of security attributes for an authorized user:

(1) User identifier(s)
(2) Roles (e.g., system administrator)
(3) Any security attributes related to a user identifier (e.g., associated certificate)

o. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The device shall immediately enforce:

(1) Revocation of a user's role
(2) Revocation of a user's authority to use an authenticated proxy
(3) Changes to the information flow policy rule set when applied
(4) Disabling of service available to unauthenticated users

p. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The device shall ensure all roles can perform their administrative roles on the device locally.

q. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The device shall ensure all roles can perform their administrative roles on the security device remotely.

r. **[Required: FW, IPS, VPN, NAC]** The product shall support at least four roles: Cryptographic Administrator (CAdmin), Audit Administrator (AAdmin), System Administrator, User.

NOTE: The CAdmin and AAdmin roles are defined in NIAP publications.

(1) **[Required: FW, IPS, VPN, NAC]** The ability to perform the following functions shall be restricted to the System Administrator role:

(a) **[Required: FW, IPS, VPN, NAC]** Modify security functions.

(b) **[Required: FW, IPS, VPN, NAC]** Enable or disable security alarm functions.

(c) **[Required: FW, IPS, VPN, NAC]** Enable or disable the Internet Control Message Protocol (ICMP) and destination unreachable notification on external interfaces (in an IP-based network), or other appropriate network connectivity tool (for a non-IP-based network).

(d) **[Required: FW, IPS, VPN, NAC]** Determine the administrator-specified period for any policy.

(e) **[Required: FW, IPS, VPN, NAC]** Set the time/date used for timestamps.

(f) **[Required: FW, IPS, VPN, NAC]** Query, modify, delete, and/or create the information flow policy rule set.

(g) Reserved.

(h) **[Required: FW, IPS, VPN, NAC]** Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the security device.

(2) **[Required: FW, IPS, VPN, NAC]** The ability to enable, disable, determine, and/or modify the functions of the security audit or the security audit Analysis shall be restricted to the AAdmin role.

(3) **[Required: FW, IPS, VPN, NAC]** The ability to perform the following functions shall be restricted to the CAdmin role:

(a) **[Required: FW, IPS, VPN, NAC]** Enable and/or disable the cryptographic functions.

(b) Reserved.

(c) **[Required: FW, IPS, VPN, NAC]** Modify the cryptographic security data.

(4) **[Required: FW, IPS, VPN, NAC]** The device shall restrict the ability to determine the administrator-specified network identifier.

5.4.6.2.1.4 Ancillary Equipment

1. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use ancillary Authentication, Authorization, and Accounting (AAA) and syslog services shall do so in a secure manner.

   a. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use external AAA services provided by the Diameter Base Protocol shall do so IAW RFC 3588.

      (1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Systems that act as Diameter agents shall be capable of being configured as proxy agents.

         (a) [Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC] Systems that act as proxy agents shall maintain session state.

      (2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.

      (3) **[Conditional: MFSS, SS, LSC, MG, EBC, R, LS, EI, AEI, FW, IPS, VPN, NAC]** All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539.

      (4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services.

      NOTE: Unlike previous UCR revisions where RADIUS was a Conditional requirement, RADIUS is now a capability that is Required when supporting AAA services.

      (1) [Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC] Products that use the EAP within RADIUS shall do so IAW RFC 3579.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the products support RADIUS based accounting, the system shall do so IAW RFC 2866.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product supports RADIUS, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product supports RADIUS and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

c. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later).

NOTE: The intent is to use the most current TACACS+ specification.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product supports TACACS+, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product supports TACACS+ and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR (Section 5.4.6, Requirements).

d. **[Conditional: EI, AEI]** Products that use external address assignment services provided by the DHCP shall do so IAW RFC 2131.

NOTE: An external address assignment service is a service that extends beyond the boundary of the system.

(1) **[Conditional: EI, AEI]** Products that act as DHCP clients upon receipt of a new IP address shall probe (e.g., with ARP) the network with the newly received address to ensure the address is not already in use.

NOTE: The actions to take if a duplicate address is detected are found in RFC 2131.

(2) **[Conditional: EI, AEI]** Products that act as DHCP clients upon receipt of a new IP address shall broadcast an ARP reply to announce the client's new IP address and clear outdated ARP cache entries in hosts on the client's subnet.

e. **[Conditional: R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use external AAA services provided by port based network access control mechanisms shall do so IAW IEEE 802.1X-2010 in combination with PEAP and EAP-TLS support, at a minimum, plus any other desired secure EAP types (e.g., EAP-Tunneled Transport Layer Security (TTLS)).

(1) **[Conditional: R, LS, EI, AEI, FW, IPS, VPN, NAC]** Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.

(a) Reserved.

f. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Products that use external syslog services shall support the capability to do so IAW RFC 3164.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Products that support syslog over UDP IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product supports syslog, the product shall support the capability to transmit messages in the format defined by RFC 3164.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product supports syslog, the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the originally formed message has a TIMESTAMP in the HEADER part, then it shall support the capability to specify this field's value in the local time of the device within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT).

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If products use TCP for the delivery of syslog events, then the system shall support the capability to do so IAW the RAW profile defined in RFC 3195.

2. **[Required: EBC]** The product shall either support an onboard VVoIP IDS/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form, or support the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

a. **[Required: EBC] [Alarm]** The VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 5.8, Security Devices Requirements, of this UCR. The product shall support the capability to generate and transmit an alarm to the NMS when these threats are identified.

b. **[Conditional: EBC]** If the product provides the capability to transmit decrypted media and signaling to an external VVoIP IDS/IPS platform, the product shall at a minimum provide FIPS-compliant confidentiality and integrity for this information in a manner that conforms to the cryptographic profiles specified for TLS and IPSec in this UCR.

c. **[Conditional: EBC]** If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, this interface shall use publicly accessible specifications and standards.

NOTE: The intent of this requirement is to ensure that third party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.

5.4.6.2.1.5 Authentication Practices

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall be capable of authenticating users and appliances.

   a. Reserved.

      (1) Reserved.

      (2) Reserved.

         (a) Reserved.

         (b) **[Required: MFSS, SS, LSC, MG, EBC, R, LS, FW, IPS, VPN, NAC]** Identification and Authentication management mechanisms shall include, in the case of communication between two or more systems (e.g., client server), bidirectional authentication between the two systems.

      (3) **[Required: LSC]** The product shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) and/or with PKI certificates issued from a DoD approved PKI.

         NOTE: This assumes the EI is served directly by the appliance.

      (4) **[Required: LSC]** The product shall be capable of authenticating the AEI using TLS with PKI certificates issued from a DoD-approved PKI.

      (5) **[Required: EI]** The product shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) and/or with PKI certificates issued from a DoD-approved PKI.

      (6) **[Required: AEI]** The product shall be capable of authenticating the LSC using TLS with PKI certificates issued from a DoD-approved PKI.

      (7) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product must, at a minimum, support the ability to perform authentication via a configurable mechanism internal to the product (local authentication) even when authentication via an external AAA service is supported.

NOTE: When an authentication server is used, the Network Infrastructure STIG requires only one account or console account to be configured locally for use in an emergency (i.e., authentication server or connection to the device is down).

b. Reserved.

(1) Reserved.

(2) Reserved.

c. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** If a CAC or other PKI token approved by the DoD PKI PMO (e.g., PIV) is used for authentication purposes, the user's credentials from the CAC or token shall be passed by the authentication mechanism (i.e., local authentication, RADIUS, DIAMETER, TACACS+, etc.) to the product's management and configuration applications for providing role-based access control.

NOTE: For example, this means that the product should not have to require a second authentication, such as a username and password, to occur for authorization purposes after the CAC or other approved token-based authentication has completed successfully.

d. Reserved.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** The product shall perform the entire user authentication procedure even if the user ID that is entered is not valid.

NOTE: The notification requirements associated with a failed log-on are covered in other requirements in this section of the UCR.

f. Reserved.

g. **[Required: EI, AEI]** The product shall be capable of allowing users to place ROUTINE precedence calls without authenticating.

(1) **[Required: EI, AEI]** The product shall be capable of allowing users to place emergency calls without authenticating.

h. **[Required: EI, AEI]** The product shall only allow authenticated users to access the product for services above the ROUTINE precedence.

(1) **[Conditional: LSC, EI, AEI]** If the product uses SIP or AS-SIP, the system shall, at a minimum, support the use of SIP digest authentication as specified in RFC 3261 when authenticating users. The product may support the ability to authenticate users via PKI certificates when authenticating user credentials to the LSC via the EI or the AEI using proprietary mechanisms.

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

(a) **[Required: LSC, EI, AEI]** The product shall use the procedures and algorithms specified in RFC 3261, Section 22.4, to execute SIP digest authentication for user authentication. The user ID entered by the user shall be used for the value of the "username" field and the PIN entered by the user shall be used as the value for "secret" in the digest calculation.

(b) **[Required: EI, AEI]** The device shall support the capability to provide audible and/or visible notification to the user, which, in a human understandable manner, prompts them to enter their assigned User-ID and PIN when a precedence level above ROUTINE is requested.

(2) **[Required: LSC, EI, AEI]** The user authentication mechanism shall be software enabled or disabled.

NOTE: In certain deployments, the user does not have the time to input authentication credentials and the EI or AEI is located in a secure environment where credentials are not necessary due to the mission. By default this capability will be disabled to allow users to place calls without authenticating.

(a) **[Conditional: EI, AEI, (Softphone)]** If the product is a softphone, the product shall support the capability to provide user authentication by presenting the user credentials extracted from the CAC or other DoD PKI PMO approved PKI token to the LSC.

NOTE: The mechanism for AEIs and EIs to authenticate the User CAC or approved token credentials is permitted to occur via proprietary means. However, authentication of users via User ID and PIN authentication has been standardized for AEIs in this UCR.

i. **[Required: EI, AEI]** The product shall allow only an authenticated system administrator to perform configuration functions.

NOTE: This requirement is focused on network and LSC configuration items and is not meant to preclude users from personalizing the phone through configuration items like volume control (to include mute), speakerphone enable/disable (if originally enabled by the system administrator), headset enable/disable, LCD contrast, voice mail features, speed dial and call forwarding features.

i. **[Required: EI, AEI]** The product shall not display configuration information without proper authentication.

NOTE: The minimum requirement for authentication is defined in Section 5.4.6.2.1.5, Authentication Practices, of the UCR.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of ensuring that all ports on a system that support operations related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the device supports SNMP, the device shall support the capability to configure SNMP so that read-only access is provided.

k. Reserved.

l. **[Required: EI, AEI]** The product shall operate properly when auto-registration is disabled.

NOTE: Typically, auto-registration is used during initial installation of large numbers of EIs. It involves the automatic registration of EIs to the LSC, automatic assignment of IP assignment of IP addresses and user IDs, and automatic download of application files. Typically, auto-registration is disabled after installation and manual changes are made.

m. Reserved.

5.4.6.2.1.6 Public Key Infrastructure

1. Reserved.

a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of generating asymmetric (public and private) key pairs and symmetric keys.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of generating asymmetric keys whose length is at least 2048 for RSA.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS, FW, IPS, VPN, NAC]** The product shall be capable of generating symmetric keys whose length is at least 128 bits.

(a) Reserved.

(3) Reserved.

b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of storing key pairs and their related certificates.

(1) Reserved.

(2) Reserved.

(a) Reserved.

(b) Reserved.

(c) Reserved.

(d) Reserved.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall operate with DoD-approved trust points (e.g., public keys and the associated

certificates the relying party deems as reliable and trustworthy, typically root CAs).

NOTE: Trust points are further defined in Appendix A of this UCR, Definitions, Abbreviations and Acronyms, and References.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall authenticate individual certificates up to a trusted DoD-approved CA (intermediate or root).

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, LS, EI, FW, IPS, VPN, NAC]** If a trust point is not established, the product shall authenticate individual certificates from the issuer specified on the individual certificate up to the root CA.

c. Reserved.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the "DoD PKI Functional Interface Specification."

(1) Reserved.

e. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of using the LDAPv3, HTTP, or HTTPS as appropriate when communicating with DoD-approved PKIs.

(2) Reserved.

(3) Reserved.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If CRLs are used, the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.

i. Reserved.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If CRLs are used, the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is Objective.

NOTE: This requirement does not prevent the product from supporting the ability to use manually configured, local CDPs which differ from the CDP provided in the certificate.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If OCSP is used, the product shall support the capability to use both the Delegated Trust Model (DTM), whereby the OCSP responder's signing certificates are signed by DoD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DoD PKI PMO guidance.

NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DoD PKI OCSP responders. Products should expect these certificates to change regularly (approximately every 30 days).

NOTE: RFC 2560 describes both the Trust Responder and Delegated Trust (termed "Authorized Responder" within RFC 2560) models. Though DoD PKI-specific implementation details can only be found in DoD PKI PMO publications.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If OCSP is used, the OCSP responder shall be contacted based on the following information:

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** The OCSP responder preconfigured in the application or toolkit; and

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** The OCSP responder location

identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If both of the above are available, the product shall be configurable to provide preference for one over the other.

iv. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.

(4) **[Conditional: EI]** If the EI is PKI enabled, the EI shall support a mechanism for verifying the status of an LSC certificate using a Certificate Trust List (CTL), CRLs, or an online status check (OCSP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

(5) **[Conditional: LSC]** If the EI is PKI enabled, the LSC shall verify the status of an EI certificate using the CTL, CRLs, or an online status check (OCSP in the case of the DoD PKI).

NOTE: It is understood that the system administrator must ensure that the CTL is current to ensure that the status is accurate.

NOTE: When implemented the CRL and OCSP implementation must conform to the CRL and OCSP requirements specified previously and later in this section.

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall support all of the applicable requirements in the latest DoD PKE Application Requirements specification published by the DoD PKI PMO.

NOTE: At the time of this UCR's writing, the “DoD Class 3 Public Key

Infrastructure Public Key-Enabled Application Requirements" document from July 13, 2000 is the latest version of this document.

f. Reserved.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of producing SHA digests of messages to support verification of DoD PKI signed objects.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm.

NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.

(2) Reserved.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, FW, IPS, VPN, NAC, LS]** The product shall log when a session is rejected due to a revoked certificate.

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of supporting the development of a certificate path and be able to process the path.

NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust point. The process terminates when either the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path.

(1) Reserved.

(2) Reserved.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The path process shall fail when a problem that prohibits the validation of a path occurs.

(4) Reserved.

(a) Reserved.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI] [Alarm]** During VVoIP session establishment, if the product uses an online status check to validate a certificate and the product cannot contact the online status check responder (OSCR) (in the case of the DoD PKI, this will be an RFC 2560 OCSP responder) and backup OSCRs, the product will establish the VVoIP session (e.g., shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions. This requirement is not applicable to scenarios related to non-VVoIP-session related functions such as logging on to administrative interfaces. The intent of this requirement is to prevent phone or video calls from being denied due to connectivity issues with the OCSP responder.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI] [Alarm]** During VVoIP session establishment, if the product uses CRLs to validate a certificate and the product cannot reach the CDP or any backup CDPs, the product will continue the process (e.g., shall not terminate the session), but will log the event and send an alarm to the NMS.

NOTE: This requirement applies only to the establishment of VVoIP sessions (see the note on the preceding requirement).

(b) Reserved.

(c) Reserved.

(d) Reserved.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, FW, IPS, VPN, NAC, LS]** The product shall log an event if the certificate is rejected due to a status check.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of ensuring that

the intended use of the certificate is consistent with the DoD-approved PKI extensions.

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of ensuring that the digital signature bit is set for authentication uses.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** The product shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.

(c) Reserved.

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI]** Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired.

NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check (see Section 5.4.6.2.1.6, Public Key Infrastructure, Paragraphs 1.g(4)(a)i and 1.g(4)(a)ii).

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If the system supports manual loading of a CRL or CTLs configured by an administrator, the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If the system supports automated retrieval of a CRL from a CDP, the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL.

(a) Reserved.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If the system supports automated retrieval of a

CRL from a CDP, the system shall support the ability to configure the interval in which the CRL is retrieved periodically.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, IPS, VPN, NAC, LS]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, the device shall query the online status check responder every 24 hours for as long as the session remains active.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, FW, VPN, IPS, NAC, LS]** If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI] [Alarm]** The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration.

NOTE: Since EIs and AEIs are not expected to have direct access to the NMS, the LSC, MFSS, or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or AEIs. However, EIs and AEIs should also alert their users via the EI or AEI user interface when certificates are nearing expiration.

NOTE: There is no expectation for vendors to develop a proprietary protocol for this purpose. It is sufficient for an MFSS, SS, or LSC to inspect the certificate of a served EI or AEI during registration time and periodically thereafter for the duration of the signaling session. Some products may also store the certificate associated with their subscribing EIs and AEIs so as to enable this check to be performed even when the EIs and AEIs are offline.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, FW, IPS, VPN, NAC, LS – Conditional: EI] [Alarm]** By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.

j. **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI, FW, IPS, VPN, NAC – Conditional: EI]** The product shall support the capability to verify that the identity claimed in an X.509v3 certificate Subject Common Name, used to establish an authenticated and secure channel, correctly maps to the identity claimed in signaling messages transmitted within the same secure channel.

NOTE: At this time, the identity claimed in an X.509v3 certificate Subject Common Name may be a FQDN, IPv4, or IPv6 address.

(1) **[Required: MFSS, SS, LSC, MG, EBC, FW, IPS, VPN, NAC] [Alarm]** The product shall support the capability to generate and transmit an alarm to the NMS when it detects a mismatch between the identity claimed in an X.509v3 certificate used to establish a secure channel at a lower layer, and the identity claimed in messages within the established secure session. Furthermore, the product shall deny the operation requested by the message containing the mismatched identity.

NOTE: Examples include cases where a device attempts to use a phone number not assigned to the identity claimed in the X.509v3 certificate presented by the device. Another example includes cases where the domain in the SIP URI of a Route header unexpectedly does not match the identity in the X.509v3 certificate.

(2) **[Required: MFSS, SS, LSC, MG, EBC, EI, AEI – Conditional: EI]** The product shall support the capability to examine the identity claimed by the X.509v3 Subject Common Name field and compare it to the identity claimed within signaling messages regardless of whether the claimed identity contains an FQDN, IPv4 address, or IPv6 address.

(3) **[Required: MFSS, SS, LSC, MG, EBC, AEI]** The product shall adhere to the requirements in RFC 5922 Section 7.2 "Comparing SIP Identities" when comparing the domains extracted from X.509v3 certificates with AS-SIP identities contained in signaling messages.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** The product shall support the capability to statically map the FQDNs contained in X.509v3

certificate Subject Common Names to IP addresses via a configurable lookup table.

NOTE: Use of DNS to map X.509v3 Subject Common name fields to IP addresses may be optionally supported in addition to this requirement. However, using DNS in this manner is not required because all MILDEP sites will not be configured to populate certificates with only DNS associated X.509 Subject Common Name FQDNs.

(5) **[Conditional: MFSS, SS, LSC]** If the system support AEIs that use the sip.instance media feature tag (RFC 5626), the system shall ensure that the identity claimed in the AEI's X.509 certificate Subject Common Name presented during TLS session establishment maps to the AS-SIP Address of Record (AOR) and sip.instance values specified in AS-SIP signaling messages.

NOTE: This requirement is meant to ensure that the identity claimed by a registering AEI in AS-SIP is authorized based on its presented X.509 certificate.

5.4.6.2.1.7 Authorization

1. Reserved.

a. Reserved.

b. Reserved.

(1) **[Required: LSC, MFSS, SS]** The product shall only forward a signaling message when the forwarding destination is authorized.

NOTE: This is to ensure that sessions are not forwarded to an unauthorized destination. This includes on-net and off-net destinations.

c. Reserved.

d. **[Required: R, LS, EBC, RSF]** The product shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for the authenticated users and EIs.

NOTE: Proxies and screened subnets are provided by using border controllers,

ACLs, FWs, and VLANs. Network service classes are defined by the QoS WG, and they may consist of voice, video, and data service classes.

(1) **[Required: R, LS, EBC, RSF]** The product shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, DSCP, and protocol identifier ("6 tuple").

(a) **[Required: EBC, RSF]** The product shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6 tuple") based on the information contained within the SDP body of the AS-SIP messages.

i. **[Required: EBC, RSF]** The product shall have the capability to close a "gate/pinhole" based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP signaling appliances (lost BYE scenario).

NOTE: The inactivity timer is based on the inactivity of the media stream.

A. **[Required: EBC, RSF]** The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes.

(b) **[Required: R, EBC, RSF]** The product shall have the capability of permitting the configuration of filters that will permit or deny IP packets on the basis of the values of the packet's source address, destination address, protocol, source port, and destination port in the packets header. These filters shall have the capability of using any one value, all values, or any combination of values. Filters using source ports and destination ports shall have the capability to be configured to use ranges of values defined by the operators (1) equal to, (2) greater than, (3) less than, (4) greater than or equal to and (5) less than or equal to.

(2) Reserved.

(a) **[Required: R, LS]** The product shall be capable of supporting a minimum of five distinct VLANs for VVoIP.

(b) **[Required: LS, R]** The product shall be capable of ensuring that EIs (that do not contain a multiport switch) and VVoIP appliances are connected only to switch ports with access to the VVoIP VLAN(s).

NOTE: This requirement is not applicable to an EI with an embedded multiport switch.

(c) **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be capable of supporting 802.1Q trunking to separate VVoIP and data traffic, or it shall have a separate Network Interface Card (NIC) for the data and the VVoIP.

NOTE: The intent of this requirement is to prevent the workstation from accessing or viewing the voice traffic as well as to prevent the workstation from accessing the EI and AEI for configuration purposes.

i. Reserved.

ii. **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be capable of routing the VVoIP and data traffic to the appropriate VLAN.

NOTE: This requirement differs from the previous requirement in that the previous requirement involves marking the packet and this requirement is focused on what action to take based on the marking or the output NIC.

iii. **[Conditional: EI, AEI]** If the product supports a data workstation, then the system shall be able to disable the switchport that allows access for the data workstation when the data workstation is not connected.

(d) Reserved.

i. **[Required: LS – Conditional: R] [Alarm]** The product shall be capable of notifying the NMS when the MAC address tables threshold is reached to avoid an overflow.

ii. Reserved.

(e) Reserved.

(f) Reserved.

(g) Reserved.

(h) Reserved.

(3) Reserved.

(a) **[Required: EBC]** The product shall be capable of using NAT and NAPT on all VVoIP enclave-to-WAN connections.

i. **[Required: R, EBC, RSF]** The product shall have the capability to deploy using private address space IAW RFC 1918.

ii. **[Required: EBC]** The EBC shall be an AS-SIP intermediary in all WAN signaling sessions.

A. **[Required: EBC]** To enable the application of NAT and NAPT, the EBC shall be able to inspect and modify the SDP body (i.e., the SDP "c=" and the "m=" lines) of the corresponding AS-SIP message.

iii. **[Conditional: EBC]** If the system supports H.323 video sessions, the EBC shall be capable of supporting H.323 NAT and NAPT.

(b) Reserved.

(c) Reserved.

(4) Reserved.

(5) Reserved.

(a) **[Conditional: R, LS, EI, AEI]** If DHCP is used, the product shall be capable of using 802.1X in combination with a secure EAP type (defined within this UCR and the STIGs) residing on the authentication server and within the operating system or application software of the EI and AEI to authenticate to the LAN.

i. Reserved.

ii. Reserved.

(6) **[Required: RSF]** The product shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled so that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services.

(7) **[Required: EBC, RSF]** The product shall have the capability to deploy VVoIP aware FWs at all VVoIP security boundaries (internal and external).

(a) **[Required: EBC, RSF]** The product FWs deployed at the boundaries of the VVoIP enclave shall have the capability to use stateful packet inspection.

(b) Reserved.

e. Reserved.

(1) Reserved.

f. Reserved.

(1) Reserved.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Assigning passwords to specific actions (e.g., operations-related commands) shall not be used as a primary access control method (though passwords may be used to augment other access control(s).

NOTE: When passwords are used as the primary access control method, confidentiality is lost because of password sharing among authorized users.

(2) Reserved.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** Depending on the application, if the product is to be accessed by administrative users who need to keep this access (including the fact that an access is being made) confidential from other administrative users, such as unauthorized B/P/C/S Director of Information Management (DOIM) employees (i.e., CALEA type requirements), the product shall be

capable of providing a separate interface/port for such confidential access. It shall be capable of ensuring that messages (including log-on requests) at this "special" interface/port are kept confidential from users logged on at other interfaces/ports.

NOTE: It is acceptable to implement the CALEA logging functions in a separate security log on a different appliance than the normal security log.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, VPN, IPS, NAC]** The product shall be capable of controlling access to resources over a given interface/port on the basis of privileges and policies assigned to that interface/port.

(c) **[Conditional: EBC, RSF]** If the product supports CALEA functions, those functions shall be disabled by default.

g. Reserved.

h. **[Required: MFSS, SS, LSC, MG]** The product shall have the capability to provide a secure method for allowing automatic interconnections.

NOTE: Automatic interconnection is allowed only between an incoming long-distance SBU voice call and the local commercial system (off-netting).

(1) **[Required: MFSS, SS, LSC, MG]** Automatic interconnection between DoD IP VVoIP calls and local commercial systems shall be permitted only with proper authorization.

NOTE: The authorization is granted based on successful authentication in combination with an acceptable profile allowing the interconnection.

(2) **[Required: MFSS, SS, LSC, MG]** The product shall have the capability of identifying all calls made through the automatic interconnection.

(3) **[Required: MFSS, SS, LSC, MG]** The product shall be capable of ensuring that all automatic calls are verified periodically by the user.

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes around-the-clock to all

DoD IP VVoIP database tables (excluding tables associated with non-DISA controlled devices).

NOTE: The intent of this requirement is to ensure that authenticated and authorized NMS personnel have limited capability to resolve issues in the event that a problem occurs and there are no on-site maintenance personnel available.

j. Reserved.

k. **[Required: MFSS, SS, LSC, EBC, RSF]** The product shall have the capability to deny system access to all session requests (i.e., disable the points of ingress) in response to appropriate messages received from the NMS.

NOTE: Sessions in this context are associated with NMS sessions, such as a SSH session.

l. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product provides an emergency entry port (Emergency Action Interface) with system access control, the product shall have the capability to meet the following requirements (note that an emergency port is defined to be a port that is infrequently used; and so it is not used for regular maintenance):

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** On its emergency entry port, the product shall be capable of minimally using a username with a strong password that meets the complexity and character diversity requirements specified in this UCR and the STIGs.

(2) [Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] The product shall log all access attempts in an audit log.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of ensuring at least one, and not more than two, system security administrator accounts cannot be locked out due to log-on failures.

m. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product provides an emergency entry port without system access control then the following requirements shall be met.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product emergency entry port shall recognize only those

commands that perform system restoration (for example, from a disk) and no other operations commands.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** The product shall generate a real-time alarm/alert when this port is used to gain access to the system and transmit that alarm to the appropriate NOC.

n. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall have the capability to deny the establishment of any session via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a log-on request, the system shall not respond.

o. Reserved.

(1) Reserved.

(2) Reserved.

(3) Reserved.

p. Reserved.

(1) Reserved.

(2) Reserved.

(3) Reserved.

q. Reserved.

r. Reserved.

(1) Reserved.

(2) Reserved.

(3) Reserved.

(4) Reserved.

(5) Reserved.

s. Reserved.

t. Reserved.

u. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing a level of granularity so that, for any specified resource controlled by the system (to include precedence calls), it shall be possible to do the following:

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Grant access rights to a specified user/customer or group of users/customers.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Deny access rights to a specified user/customer or a group of users/customers.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Grant access rights to a specified interface/port or a group of interfaces/port.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Deny access rights to a specified interface/port or a group of interfaces/ports.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional.

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Deny an interface/port access to potentially damaging processes and transactions that the interface/port does not have to access to be functional.

(7) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Deny a user (as well as an interface/port) access to data files and/or tables unless the user (as well as the interface/port) is authorized for it.

(8) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the system has its operations database structured based on commands, views, records, and fields, the system shall restrict, based on user

ID as well as interface/port, the execution of any specifiable command on any specifiable view, record, or field.

5.4.6.2.2 Integrity

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, AEI, EI, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing data and system integrity using industry-accepted integrity mechanisms (e.g. parity checks, cyclic redundancy checks, message authentication codes, hashing).

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** The product shall be capable of ensuring the integrity of VVoIP signaling messages.

      (1) **[Required: MFSS, SS, LSC, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using TLS for providing integrity of AS-SIP messages.

      NOTE: The condition for the EI is the support of AS-SIP.

      (a) **[Required: MFSS, SS, LSC, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using HMAC-SHA1-160 with 160 bit keys.

      (2) **[Conditional: MFSS, SS, LSC, EI, AEI]** If the product uses H.323, the product shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160 bit keys.

   b. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** The products shall be capable of protecting data integrity by performing integrity checks and/or data updates. Examples include:

      (1) [Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC] Proper rule checking on data update.

      (2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** Adequate alert messages (e.g., "Do you really mean it?") in response to potentially damaging commands before executing them, so that involuntary human errors may be reduced.

      (3) Reserved.

(4) [Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC] Checking return status.

(5) [Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC] Checking intermediate results.

(6) Reserved.

(7) [Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC] Proper serialization of update transactions.

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC] [Alarm]** The product shall be capable of providing strong integrity mechanisms (e.g. integrity locks, encryption) that can be used to periodically validate the correct operation of its stored data, software, firmware, and hardware (such as proper functioning of the security log, proper functioning of various trigger mechanisms, etc.). The product shall alert the NMS when anomalous operation is detected.

(1) Reserved.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues).

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** The product shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold.

NOTE: The types of communications errors that must be detected include abnormally large numbers of received packets that fail decryption and/or fail to pass integrity checks (e.g., failed CRC or hash function computations).

f. **[Required: MFSS, SS, LSC, EBC, RSF, FW, IPS, VPN, NAC]** The product shall be capable of providing a mechanism to monitor the integrity of the system (data, software, firmware, hardware) and generate a status report detailing the values of all parameters and flags that affect the secure operation of the system.

NOTE: The vendor shall document parameters and flags that affect the secure operation of the product and the Information Assurance test team at the appropriate DoD laboratory will validate these parameters and provide technical advisement to the DISN Security Accreditation Working Group (DSAWG) about its adequacy.

(1) **[Required: MFSS, SS, LSC, EBC, RSF, FW, IPS, VPN, NAC] [Alarm]** The system shall support the capability to generate an alarm to the NMS when it detects that the integrity of the system is such that it is no longer operating in an approved or secure state. (For example, a failed signature check on the currently loaded software would cause this type of alarm.)

g. **[Required: MFSS, SS, LSC, MG, EBC, RSF, FW, IPS, VPN, NAC]** The product shall be capable of automatically running file or disk integrity checking utilities by vendor-supplied software.

h. **[Required: EI, AEI, MG, MFSS]** The product shall be capable of providing data integrity of the SRTP bearer (transport) packets.

(1) **[Required: EI, AEI, MG, MFSS]** The product shall be capable of using HMAC-SHA1-32 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTP packets.

(2) **[Required: EI, AEI, MG, MFSS]** The product shall be capable of using HMAC-SHA1-80 for the authentication tag with 160 bit key length as the default integrity mechanism for SRTCP.

NOTE: The ability to process received SRTCP messages is optional, but the capability to transmit SRTCP messages is required.

i. Reserved.

j. Reserved.

(1) Reserved.

k. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, EI, AEI, LS, FW, IPS, VPN, NAC]** The product shall be capable of ensuring that default user IDs and passwords, previously modified by the administrator, do not revert to the vendor delivered default user IDs and passwords when the system is restarted unless configured to do so by an appropriate administrator.

l. Reserved.

m. **[Conditional: MFSS, SS, LSC, MG, FW, IPS, VPN, NAC]** If the product uses IPSec, the product shall be capable of using HMAC-SHA (class value 2) as the default IKE integrity mechanism as defined in RFC 2409.

n. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160 bit key length by default.

o. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSHv2, the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.

p. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, FW, IPS, VPN, NAC]** If the product uses TLS, the product shall be capable of using TLS (SSL v3.1 or higher) in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.

5.4.6.2.3 Confidentiality

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** Products providing encryption services shall be capable of providing data and signaling confidentiality. (This includes confidentiality protection for all VVoIP signaling and media traffic.)

   a. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** The product shall at a minimum implement FIPS 140-2 Level 1 validated cryptographic hardware modules or software toolkits and operate this module in a FIPS 140-2 approved mode for all cryptographic operations.

      NOTE: FIPS 140-2 addresses many aspects of the cryptographic module to include the encryptor and the random number generator. The application does not have to be FIPS 140-2 compliant, but the cryptographic module within the application must be compliant. It is expected that a vendor either will purchase an approved FIPS 140-2 cryptographic module for its application or will submit its developed cryptographic module to an approved FIPS 140-2 certification laboratory before submitting its solution to the Government for testing. It is anticipated that the Government will accept a letter of compliance (LOC) from a vendor as a means of satisfying this requirement.

      (1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** The product shall be capable of generating all keys (asymmetric and symmetric) using a random source algorithm that conforms to NIST randomization requirements and is validated IAW NIST guidelines.

         NOTE: At the time of this document's writing, NIST draft SP 800-131 specifies the following:

(a) Use FIPS 186 if the product's randomizer is approved by NIST before and including 2010.

(b) Use NIST SP 800-90 if the product's randomizer is approved by NIST after 2010.

Also, the draft NIST SP 800-131 fully deprecates FIPS 186 randomizers after the year 2015.

b. **[Required: EI, AEI, MG]** The product shall be capable of providing confidentiality for media streams using SRTP with either the AES_CM_128 encryption algorithm as the default.

(1) Reserved.

(2) **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages IAW RFC 4568.

(3) **[Required: MFSS, SS, LSC, MG, EI, AEI]** The product shall be capable of distributing the Master Key and the Salt Key in concatenated form.

(4) **[Required: EI, AEI, MG]** The product shall use a Master Key of 128 bits to support 128-bit AES encryption.

NOTE: This implies that the Master Salt Key may be null.

(5) **[Required: EI, AEI, MG]** The Master Key and a random Master Salt Key shall be supported for SRTP sessions.

c. **[Required: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI]** The product shall be capable of providing confidentiality for VVoIP signaling messages using TLS or IPSec (or its equivalent) using the AES 128-bit algorithm.

(1) **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If H.323, MGCP, or H.248 (MEGACO) is used, the product shall be capable of using IPSec to provide confidentiality.

(a) **[Conditional: MFSS, SS, LSC, MG]** If the product uses H.248 (MEGACO), the product shall be capable of distributing the SRTP

Master Key and Salt Key in the SDP "k =" crypto field when using H.248.15.

(b) **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If H.323 is used, the product shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235Key as described in H.235.0 and H.235.8.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using IKE for IPSec key distribution:

i. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** T he product shall be capable of using IKE version 1.

ii. Reserved.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication.

iv. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using the Quick Mode as the default Phase II authentication mechanism.

v. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates.

vi. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.

A. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the

product shall only support the following erroneous messages associated with a certificate request:

1. Invalid Key
2. Invalid ID
3. Invalid certificate encoding
4. Invalid certificate
5. Certificate type unsupported
6. Invalid CA
7. Invalid hash
8. Authentication failed
9. Invalid signature
10. Certificate unavailable

vii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using Oakley Groups 1, 2, and 2048, as a minimum.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If IPSec is used, the product shall be capable of using AES_128_CBC as the default encryption algorithm.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI]** The product shall be capable of using TLS (dual path method) to provide confidentiality for the AS-SIP as described in RFC 3261.

NOTE: Upon receipt of an INVITE over a TLS-established session, an LSC shall respond to the INVITE (and any subsequent requests received over that TLS path) using this TLS session. If the LSC originates an INVITE or request, then it shall establish a separate and unique TLS session, and the LSC shall expect to receive a response to its request over this new TLS session. Two TLS sessions are established for communications between the LSC and the EBC, MFSS and EBC, LSC and LSC, LSC to AEI via RSF, or EBC and EBC. Since the AEI is required to support the dual path method, it has to act as both a SIP client and server and must support both TLS client and server functionality. Due to the proprietary nature of line-side IP solutions implemented by EIs, EI vendors may support TLS reuse or the dual path method described in this requirement for line-side implementations. The details associated with the reuse method are described in http://tools.ietf.org/html/rfc5923.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The underlying protocol for AS-SIP shall be the TCP.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using as its default cipher suite TLS_RSA_WITH_AES_128_CBC_SHA.

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of using a default of no compression for AS-SIP messages.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges.

(e) **[Required: MFSS, SS, LSC, MG, EBC, RSF, AEI – Conditional: EI]** The product shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto= field. NOTE: EI condition is whether it supports AS-SIP.

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with NM related sessions.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, AEI, EI]** If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process (e.g. a full handshake) is 1 hour.

(g) **[Conditional: MFSS, SS, LSC, EI, EBC, RSF, AEI]** If AS-SIP is used, the product shall transmit only packets that are secured with TLS and use port 5061.

NOTE: The products may use other signaling protocols for interfacing to e.g., MGs, EIs.

(h) **[Required: MFSS, SS, LSC, EI, EBC, RSF, AEI]** The product shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS.

NOTE: This ensures that the product does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.

(i) **[Required: MFSS, SS, LSC, EI, EBC, RSF, AEI]** The product shall only accept and process AS-SIP packets that arrive on port 5061.

NOTE: The product should discard AS-SIP packets that arrive on a different port.

(j) **[Required: RSF]** The product shall support both the reuse and dual path TLS methods.

NOTE: This is required of an RSF since it has to support TLS sessions between the LSC and AEI and proprietary EIs (PEIs). The AEI uses the dual path method and PEIs have the option of using the reuse method.

(k) Reserved.

i. Reserved.

ii. Reserved.

d. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN]** If the product uses web browsers or web servers, the product web browsers and web servers shall be capable of supporting TLS (SSLv3.1) or higher for confidentiality.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of using SSHv2 or TLS 1.0 (SSLv3.1) or higher for remote configuration of appliances.

NOTE: The EIs and AEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

f. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If the product uses TLS, the product shall do so in a secure manner as defined by the following subtended requirements.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, EI, AEI, FW, IPS, VPN, NAC]** If the product uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite.

(2) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If the product uses TLS, the system shall be capable of using a default of no compression.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If the product uses TLS, the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.

(4) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour.

NOTE: This requirement is not associated with NM-related sessions.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process is 1 hour.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, AEI, EI, FW, IPS, VPN, NAC]** If the product supports SSL/TLS renegotiation, the product shall support the capability to disable this feature or the product shall support RFC 5746.

NOTE: Supporting RFC 5746 includes providing a configurable option to terminate a TLS session if the peer does not support the “renegotiation_info” extension.

g. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the system shall do so in a secure manner as defined by the following subtended requirements.

NOTE: An EI’s remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.

(1) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the system shall be capable of

supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm.

(2) Reserved.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0.

NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, the conditions of fielding should clearly specify that this option must be configured.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner.

(d) Reserved.

(e) Reserved.

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the SSH sessions shall minimally support the following encryption algorithms defined in RFC 4253 and RFC 4344:

- AES128-CTR, and
- AES128-CBC (for backwards compatibility with older UCR versions).

i. **[Conditional: MFSS, SS, LSC, MG, EBC, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH sessions shall use as the default (most preferred) encryption algorithm AES128-CTR.

(g) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH sessions shall use TCP as the underlying protocol.

(h) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, it shall be capable of processing packets with uncompressed payload lengths up to 32,768 bytes or shall be configurable to specify that value; also, this length shall be the default value. This does not preclude the system from automatically sizing the MTU if it is less than 32,768.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH packets shall have a maximum packet size of 35,000 bytes or shall be configurable to that value; also, this length shall be the default value.

NOTE: The 35,000 bytes includes the packet_length, padding_length, payload, random padding, and MAC.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the product shall discard SSH packets that exceed the maximum packet size to avoid DoS attacks or buffer overflow attacks.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, SSH packets shall use random bytes if packet padding is required.

(i) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.

(j) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, EI, AEI, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH, the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.

(3) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The use of SSH is Conditional, however, if the product supports the use of SSH in conjunction with X.509v3 certificates (the SSH implementation is DoD PKE) the product shall conform to the subtended requirements.

NOTE: The EIs and AEIs are excluded from this requirement since remote management of the system is disabled after initial installation.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the system shall support the capability to use X.509v3 certificates issued by a DoD-approved PKI to establish the encrypted sessions.

(b) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates and provides an SSH server function, the SSH server shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH Server function shall support, at a minimum, the “x509v3-ssh-rsa” and "x509v3-rsa2048-sha256” key types as defined in RFC 6187.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.

(c) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH client shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.

i. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH and if the SSH client has a CAC (or equivalent) reader, the SSH client may use the X.509v3 certificate on the user's CAC to establish the encrypted session.

ii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DoD-approved PKI, the client may use either its certificate or the certificate on the user's CAC to establish the encrypted sessions.

iii. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH client shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.

(d) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH server shall validate the DoD-approved PKI certificate supplied by the SSH client IAW the specifications in PKI Section 5.4.6.2.1.6, Public Key Infrastructure, of this document.

(e) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH client shall validate the SSH server's DoD PKI certificate IAW the specifications in PKI Section 5.4.6.2.1.6, Public Key Infrastructure, of this document.

(f) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH server shall certify and validate the SSH client's DoD-approved PKI certificate before establishing an encrypted session.

NOTE: The certification and validation consists of determining that the client's certificate has not expired and has not been revoked. The server shall not establish an encrypted session with a client whose certificate has expired or been revoked.

(g) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH client shall certify and validate the SSH server's DoD-approved PKI certificate before establishing an encrypted session.

(h) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the system shall disconnect a session if the PKI certificate validation has not been completed within a configurable period. The default shall be 10 minutes.

(i) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product uses SSH with X.509v3 certificates, the SSH server shall disconnect if the number of failed validation attempts for a single session exceeds a configurable parameter and the default shall be three attempts.

NOTE: All users must be authenticated IAW the specifications presented in Section 5.4.6.2.1.5, Authentication Practices.

h. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of using SNMPv3 for all SNMP sessions.

NOTE: If the product is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the product has developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.

(1) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration.

(2) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The SNMPv3 implementation shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel =3.

(a) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product receives response messages, the product shall conduct a timeliness check on the SNMPv3 message.

(b) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** An SNMPv3 engine shall perform time synchronization using authenticated messages.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall support the capability to use CBC-DES (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3.

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3.

(6) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.

(7) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.

(8) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window.

(9) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.

(11) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product using SNMPv3 shall implement the key-localization mechanism.

i. Reserved.

j. Reserved.

(1) Reserved.

(2) Reserved.

k. **[Conditional: MFSS, SS, LSC, MG, FW, IPS, VPN, NAC]** If the product uses IPSec, the system shall be capable of using AES-CBC as the default IKE encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions.

l. **[Conditional: MFSS, SS, LSC, MG]** If the product uses different signaling protocols (i.e., H.323 and AS-SIP), the system shall be capable of translating or transferring the bearer keys between different signaling protocols.

m. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall rekey each encrypted session after the session has transmitted a maximum of 2^(L/4) blocks of data., where L is the block length in bits (e.g., 128 for AES_128) and shall be configurable.

NOTE: This is to prevent birthday property and other modes of attack.

n. **[Conditional: MFSS, SS, LSC, MG, EI, AEI]** If the product is the originating party and receives a 181 message indicating that the call is being forwarded, then

upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a rekeying.

NOTE: The rekeying is designed to prevent the "forwarding party" from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, the forwarding party would be able to eavesdrop on the forwarded session. LSCs, MFSS, and SS may act as a B2BUA for an EI or an AEI and so would originate the AS-SIP session on behalf of the EI or AEI.

o. **[Conditional: EI, AEI]** If the EI or AEI acts as a bridge or a MCU, it shall establish a unique key for each EI or AEI connection.

p. Reserved.

p. **[Conditional: EBC]** If the product transmits decrypted VVoIP signaling and/or bearer traffic to an external IDS/IPS, confidentiality for the decrypted signaling and media traffic shall be ensured using cryptographic protection, where the strength of the cryptographic protocol/algorithms used is greater than or equal to the TLS and SRTP cryptographic profiles defined in this document.

q. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall provide an encrypted communication path between itself and remote administrators, authorized IT entities, or authenticated proxy users that is logically distinct from the other communication paths and protects the communicated data from disclosure. The product shall use the AES-128 algorithm at a minimum, to protect the confidentiality of the session.

5.4.6.2.4 Non-Repudiation

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing non-repudiation and accountability services.

NOTE: This assumes that authentication has already occurred previously, as required.

a. Reserved.

b. Reserved.

(1) Reserved.

(2) Reserved.

(a) Reserved.

(b) Reserved.

(3) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).

(a) Reserved.

(4) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s)

(a) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of ensuring security log copies maintain time sequentially and include all records stored in the security log up to the initiation of the copy.

(5) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product security log shall survive system restart (e.g., via reloading).

(6) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The security log shall be capable of recording the following events by default as a minimum:

(a) Reserved.

(b) Reserved.

(c) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Changes made in a user's security profile and attributes.

(d) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Changes made in security profiles and attributes associated with an interface or port.

(e) Reserved.

(f) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Changes made in system or security configuration including changes to the audit log configuration.

(g) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Creation and modification of the system resources performed via standard operations and maintenance procedures.

(h) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Disabling a user profile, if the product supports automated or manual disabling of user profiles.

(i) Reserved.

(j) **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the system contains resources that are deemed mission critical (for example, a risk analysis classifies it as critical), then the system should log any events associated with access to those mission-critical resources.

(k) Reserved.

(l) Reserved.

i. Reserved.

ii. Reserved.

iii. Reserved.

iv. Reserved.

(m) Reserved.

(n) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Changes to system time or configuration changes to the source used to establish time, such as the configured NTP server.

(o) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Failures of cryptographic operations and enabling/disabling of key generation self-tests.

(p) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** Detected hardware or firmware configuration changes or new physical connections.

(q) Reserved.

(7) Reserved.

(a) Reserved.

(b) Reserved.

(c) Reserved.

(d) Reserved.

(e) Reserved.

(8) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** The product shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate NOC if the security log fails to record the events that are required to be recorded.

(9) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall not record actual or attempted passwords in the audit log. Additionally, the audit log shall not include plain text private or secret keys or other critical security parameters.

(10) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall ensure that security and security-related audit logs are maintained separate from other types of audit logs (history or CDR audit logs).

(11) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of transmitting all logs to a remote, centralized log server in a secure manner.

NOTE: Secure manner may be accomplished by using industry best practices and following DISA FSO STIG guidance to ensure the confidentiality and integrity of the logs during transfer.

(12) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.

(13) **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall locally store (queue) audit log/event data when communication with the management station is unavailable and transmit the queued data when network connectivity is restored.

NOTE: In the case of protocols that use unreliable delivery, such as syslog over UDP, use of mechanisms at lower OSI layers (e.g., ICMP, OSI layer 1 and 2 mechanisms) must be used to detect such connectivity issues.

c. **[Conditional: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** If the product accesses other systems to pass on a request or activity that has a user ID associated with it, the product shall have the capability to make that user ID available to other systems. Thus, if the other systems have the capability to accept the user ID information, the said user can be traceable for the lifetime of the request or activity.

d. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC]** The product shall be capable of providing post-collection audit analysis tools that can produce typical reports (e.g., exception reports, summary reports, and detailed reports) on specific data items, users, or communication facilities or reports using the complete set of data in the audit log.

e. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS, FW, IPS, VPN, NAC] [Alarm]** When the audit function starts up and shuts down, the product shall support the capability to log this event in the audit log and alert the NMS. The product shall support the capability to configure the logging/alerting of this event.

5.4.6.2.5 Availability

1. **[Required: MFSS, SS, LSC, MG, EBC, RSF, R, LS]** The VVoIP product (MFSS, LSC, etc.) shall meet the availability requirements as stated in Section 5.3.2.14.7, Availability, of this UCR, for System Quality Factors.

a. Reserved.

b. Reserved.

c. Reserved.

d. Reserved.

e. Reserved.

2. **[Required: FW, IPS, VPN, NAC]** The security device shall provide availability IAW the subtended requirements.

a. **[Required: FW, IPS, VPN, NAC]** The product shall support the capability to perform configuration changes (e.g., policies, rules set, system configuration) without requiring a reboot, reload, or power cycle of the system that would cause service interruption or expose the network it protects.

b. **[Required: FW, IPS, NAC]** The controlled interface shall enforce configurable thresholds to determine whether all network traffic can be handled and controlled. If a processing threshold or a failure limit has been met then the controlled interface will not continue to process transactions. These thresholds can be set to detect and defend against DoS attacks such as SMURF or SYN Flood.

c. **[Required: FW, VPN, NAC]** The security device shall provide a high availability failover capability that maintains state. This capability shall be configurable.

d. **[Required: FW, IPS, VPN, NAC]** The security device shall ensure that security device data will be maintained if the security device:

(1) **[Required: FW, IPS, VPN, NAC]** Fails.

(2) **[Required: FW, IPS, VPN, NAC]** Is attacked.

(3) **[Required: FW, IPS, VPN, NAC]** Storage becomes exhausted.

(4) **[Required: FW, IPS, VPN, NAC]** Fails to restart/reboot.

5.4.7 Quality Assurance Provisions

5.4.7.1 Responsibility for Inspection

As part of the UCCO process, the responsibility for inspection of the requirements is assigned to one of many DoD testing laboratories depending on laboratory schedule availability and testing capabilities. If the requirement is an interoperability issue, then the interoperability test team at the appropriate DoD laboratory will test the requirement. Regardless of whether the requirement has an interoperable aspect, the Information Assurance test team for the assigned DoD laboratory

will conduct an Information Assurance assessment of the system to ensure that all Information Assurance requirements are satisfied IAW the "UC Information Assurance Test Plan (IATP)" and the appropriate STIGs. The Information Assurance test team at the JITC is sponsored by a DISA Program Office, however the Information Assurance test team for other DoD laboratories may have different sponsors and even funding models. Due to constantly evolving security threats, the IATP also is used to test Information Assurance-related aspects of a solution that are not necessarily mandated by these requirements.

The UCCO has the responsibility for the coordination of all testing, both Information Assurance and interoperability, between all of the DoD laboratories. With respect to Information Assurance, the Information Assurance test team reports the test results of the Information Assurance assessment to the DISA FSO. The FSO is responsible for writing a recommendation to the DSAWG, in coordination with the CA who signs the DSAWG recommendation letter. The DSAWG is the organization that makes the final decision to accept any residual risks associated with the system before its Information Assurance Certification and Accreditation (C&A). After the system receives DSAWG accreditation and JITC interoperability certification, it is placed on the APL. The details of the IATP can be found on the JITC Telecom Switched Services Interoperability (TSSI) Web site (http://jitc.fhu.disa.mil/tssi/index.html) and the details of the STIGs can be found on the DISA FSO web site (http://iase.disa.mil/stigs/stig/index.html).

After an APL product is procured and installed at a location, it shall comply with the appropriate STIGs and shall report its status to the appropriate Single System Manager (SSM) annually. It is imperative that the system configuration is consistent with the configuration used during the APL process. Upon installation, the Information Assurance configuration settings must be validated as part of the DIACAP, as described in the Interim Department of Defense (DoD) C&A Process Guidance to attain its C&A, ATO, and/or its ATC. Subsequently, these system settings and Information Assurance posture must be reviewed and revalidated annually as part of the annually status update to the appropriate SSM. In addition, the product must be kept up to date with any relevant Information Assurance Vulnerability Management (IAVM) notices. This is usually accomplished by installing security patches that are tested, verified, and distributed by the vendor and/or by upgrading to the latest software or operating system release that is certified and approved for installation.

The UCCO process and APL listing is not a replacement for DIACAP and local instantiation of the DoD C&A process. Listing on the APL states that the product, in the configuration that was presented for testing, is capable of meeting DoD requirements for Information Assurance and interoperability, and so is able to be purchased by DoD components. On the other hand, the DIACAP is necessary to validate and to document the product is installed properly and meets all relevant Information Assurance requirements before it is allowed to operate with or connect to the DISN. Annual reviews and revalidation is necessary to validate and document that the products and systems are being operated in compliance with the Information Assurance requirements and remains secure.

5.4.8 Mitigated Risks

The VVoIP Information Assurance framework is designed to mitigate the Information Assurance risks associated with the VVoIP system. This goal was accomplished using a combination of commercial "best practices" and DoD-unique approaches that are consistent with DoD policies and instructions. The result of this effort was the documentation of a set of requirements for the different appliances used within the DoD VVoIP environment. Based on the requirements, in combination with the VVoIP Information Assurance framework, and in the knowledge that this UCR complements the STIGs, the Information Assurance threats associated with the VVoIP environment have been adjusted to reflect the mitigated risk, and the results are shown in Tables 5.4.8-1 through 5.4.8-8. It is understood that in most cases, the effect of the attack remains constant and the mitigation efforts are mainly focused on reducing the likelihood of the attack.

Table 5.4.8-1. Adjusted General Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G1	Eavesdropping on VVoIP subscriber transport data	1	2	2	The use of SRTP with AES 128 mitigates likelihood to a 1. In addition, the rekeying of a call transferred session mitigates this threat.
G2	Corruption of transport data	1	3	3	The use of an SHA-1 hash (and SHA-256 for some X.509v3 certificates and PKI services) mitigates the likelihood of this attack to a 1.
G3	Eavesdropping on a valid telephone number to determine its location or to masquerade	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates the likelihood to a 1.
G4	Eavesdropping on the signaling data	1	3	3	The use of AS-SIP with TLS (or its equivalent) for all signaling sessions mitigates the likelihood to a 1.
G5	Corruption of signaling data via malformed packets or protocol fuzzing	1	3	3	The use of TLS with SHA-1 mitigates the likelihood to a 1.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G6	Eavesdropping on NM traffic	2	1	2	The use of SNMPv3, SSHv2, SSL3.1, or TLS1.0 with 128-bit encryption mitigates this risk. The reason why the likelihood was not reduced to a 1 is that many vendors cannot implement SNMPv3, and in addition, it is possible other NM protocols, like TFTP, will still be used in the system.
G7	Corruption of NM data	1	3	3	The use of SHA-1 for SNMPv3, SSHv2, SSL3.1, or TLS1.0 reduces the likelihood of this type of attack. At this time, these are the only NM protocols defined for the VVoIP system
G8	Obtaining telephone number from VVoIP EI	1	2	2	The elimination of remote configuration and the use of a PIN (user ID) and password (second PIN) for configuration reduces the likelihood of this attack to a 1.
G9	Denial of service	2	2	4	This type of attack is one of the most difficult to mitigate. However, the use of VLANs in combination with filtering and traffic conditioning limit the effect of this attack. In addition, appropriate NM and authentication limits the likelihood of this type of attack.
G10	Unauthorized access to data	1	3	3	The requirements associated with this type of attack such as access controls based on user profiles and the requirements associated with authentication limit this attack.
G11	Flooding the network	2	2	4	Similar reasons to DoS attacks.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G12	Stolen terminals	1	3	3	The use of CRLs or the OCSP in combination with user authentication for above ROUTINE precedence sessions mitigates the likelihood of this attack. Another consideration is that if the terminal is in a high-risk environment (forward deployment), it is possible to require user authentication for any session, to include ROUTINE. Finally, the use of NM capabilities (Code Block) in combination with the ability to disable individual terminals also mitigates the likelihood to a 1.
G13	Subscription or toll fraud	2	1	2	The implementation of authentication in combination with non-repudiation limits the likelihood of this attack.
G14	Unauthorized access to NM or subscriber database	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database Information Assurance requirements mitigates the likelihood of this type of attack.
G15	Unauthorized access to data in EIs	1	1	1	The elimination of remote configuration and the use of a user ID (PIN) and password (second PIN) for configuration reduces the likelihood of this attack to a 1. In addition, the compliance of the EI and AEI with FIPS 140-2 also reduces the likelihood of this attack.
G16	Masquerading as one legitimate subscriber or signaling device to another	1	3	3	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI and AEI to the LSC also reduces the likelihood of this type of attack.
G17	Man-in-the-middle attack	1	3	3	The use of 128-bit encryption for all session streams in combination with authentication and traffic segmentation (e.g., VLANs, filtering) reduces the likelihood of this type of attack to a 1.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G18	Repudiation of actions	1	2	2	The logging of information and the requirements associated with the storage of logged information reduces the likelihood of this type of attack. In addition, the authentication of appliances and users facilitates the rapid detection of a malicious user.
G19	Replay Attack	1	2	2	The integrity mechanisms required by the system mitigate the likelihood of this attack.
G20	SIP Parser Attack	1	2	2	The requirement to authenticate and the hardening of the EIs and SIP signaling should mitigate the likelihood of this attack.
G21	SIP Registration or INVITE Flooding – DoS Attack	1	3	3	The requirement to authenticate and the hardening of the EIs and SIP signaling appliances should mitigate the likelihood of this attack. This is primarily an insider attack threat and the defense-in-depth strategy should make this an easily detected and isolated attack.
G22	Buffer Overflow Attack	1	3	3	The likelihood of this attack is small due to the requirement to mutually authenticate all signaling appliances. This attack is associated with malformed SIP messages causing the buffer to overflow.
G23	SIP INVITE	2	1	2	The SIP timers should clear this issue within approximately 32 seconds. In addition, this attack would only affect one phone at a time.
G24	SPAM over Internet Telephony (SPIT)	1	2	2	This attack would have to originate within the SBU voice due to the TDM constraint to the PSTN.
G25	Worms, Viruses, and Trojans	1	3	3	Remove applications that are not VVoIP related from VVoIP appliances. Install antivirus software on appliances that have applications.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G26	Exploitation of a "zero-day" vulnerability	2	2	4	Mitigated by requiring vendors to state the extent of their security liability within product warranties. Reputable vendors are used who specify framework/details for expeditious security fixes throughout a period as specified/agreed to by the Government. Vendors should (1) conduct reviews of their components, inspecting for any security issues and, (2) correct any issues expeditiously upon detection. Government processes provide timely implementation of available fixes through CERT coordination/ IAVA response, secure CM policies/procedures, etc. Underlying/complementary defense-in-depth safeguards further lower the probability and impact of occurrence.
G27	Disabling of security controls by authorized users	1	3	3	Controls to prevent (hardening, authorization, limited accounts), detect (audit/monitor), and/or respond (defense-in-depth, compensating controls, manual/automatic resets) to security control circumvention lower the likelihood to a 1.
G28	Exploitation of numerous vendor-specific VVoIP product vulnerabilities	1	2	2	See notes for G26. The likelihood is lower due to this category addressing existing vulnerabilities.
G29	Exploitation of underlying (i.e., not VVoIP-specific) network and/or system vulnerabilities	1	2	2	Integration and compliance with the DoDI 8500.2 baseline controls will largely mitigate this risk through layers of defense-in-depth safeguards.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
G30	Unintentional flooding	2	2	4	Endpoint safeguards to mitigate risk include appropriate configuration designations (e.g., IP phones with sufficient registration interval duration); vendor warranties/fixes (see G26) for component malfunctions that cause flooding; and power-related protection (e.g., UPS) to protect against flooding due to simultaneous endpoint registration after a power outage.
G31	Security devices collectively impact QoS	1	2	2	Performance requirements are included in the UCR to ensure appropriate QoS.
G32	Components within the system from untrusted sources could serve as future attack points, e.g., back doors, logic bombs	1	2	2	See G26 notes. Purchasing from reputable vendors, who conduct internal product reviews/ inspections and warranty against defect (including security-related issues), provides for adequate mitigation.

Table 5.4.8-2. Data Deletion Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
D1	Eavesdropping of old address	2	1	2	The use of NAT may mitigate the likelihood of this attack.
D2	Masquerading as a subscriber to delete data	1	3	3	The limiting of access to the database to authenticated and authorized personnel in addition to the database information assurance requirements mitigates the likelihood of this type of attack.

Table 5.4.8-3. Subscriber Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SR1	Illegal registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The use of mutual authentication for signaling appliances reduces the likelihood of this attack. In addition, the authentication of the EI and AEI to the LSC also reduces the likelihood of this type of attack.

Table 5.4.8-4. Subscriber De-Registration Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
SD1	Illegal de-registration by an attacker masquerading as a voice or video switch/appliance	1	1	1	The requirements associated with authentication of a system before processing commands may mitigate the likelihood of this type of attack.
SD2	Subscriber does not allow de-registration by manipulating the EI	2	1	2	The impact is minimal since the subscriber should be easily isolated using FWs and other security mechanisms such as authentication of the EI and AEI to the LSC, the use of user ID (PIN) and password (second PIN) for the configuration of the EI and AEI, and the encryption of NM.
SD3	Subscriber does not allow de-registration by manipulating VVoIP server	1	3	3	The requirements for authentication and authorization of a user on the system mitigate the likelihood of this type of attack. In addition, the requirements associated with hardening the system and ensuring the integrity of the system also mitigates the likelihood of this type of attack.

Table 5.4.8-5. Incoming Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I1	Masquerading by using someone's ID	1	2	2	Since authentication is mandatory, the likelihood is low.
I2	Masquerading by using someone's ID and authentication	1	3	3	The design of the authentication mechanism should be sufficient to minimize the likelihood of an attack. However, if the mechanism is broken, it makes a large segment of the network vulnerable.
I3	Eavesdropping of the communication on the access interface by use of a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat. In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
I4	Eavesdropping of the start of a communication on the EI	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
I5	Modification of routing data	1	3	3	This is mitigated by requiring mutual authentication between routing appliances in combination with the encryption and applying integrity checks to the routing packets.
I6	Message alteration: call black holing	1	3	3	Safeguards protect unauthorized changes to intermediary device configurations, including authentication and access controls. Signaling streams that traverse the appliance and its ASLAN are encrypted using SIP/TLS.

Table 5.4.8-6. Outgoing Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
01	Masquerading using a subscriber's ID	1	2	2	This attack is associated with outgoing calls and the likelihood is minimized if authentication is required.
02	Masquerading using a subscriber's ID and authentication	1	3	3	There are many policies and procedures established in the DoD that address how one must protect their passwords. This UCR does not address those policies and procedures.
03	Eavesdropping on the access interface by using a session key	1	2	2	There are many requirements in the system associated with the protection of the session key to include the FIPS-140-2 compliance requirements that mitigate the likelihood of this threat. In addition, session keys have a shorter lifespan than the time it should take to break the key. The key is not sent in the clear making it difficult to obtain.
04	Eavesdropping on the network	1	3	3	The use of encryption for all layers should minimize the likelihood of this event occurring.

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
05	Eavesdropping on the start of a communication on the EI	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
06	Eavesdropping on the phone number of a called party	1	1	1	This threat is mitigated by completing authentication of the session before the session is established in combination with completing the distribution of the session key before the session is established.
07	Modification of the dialed number	1	3	3	This threat is mitigated by the use of authentication by appliances and users (for above ROUTINE precedence sessions) in combination with encryption and integrity checks for all sessions.
08	Masquerading using someone's ID	1	1	1	This is not allowed since authentication is required before allowing a session to be established.

Table 5.4.8-7. Emergency and Precedence Call Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
E1	Misuse of emergency call	2	1	2	The use of non-repudiation does not prevent this type of attack, but does allow for the rapid discovery of the malicious user or EI and AEI.
E2	Misuse of precedence calls	1	3	3	This threat is mitigated by the requirements associated with user authentication and EI and AEI authentication for above ROUTINE level sessions.
E3	Manipulation of emergency database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.
E4	Manipulation of precedence database information	1	3	3	The requirements associated with user authentication and authorization for database access decrease the likelihood of this type of attack.

Table 5.4.8-8. Survivability Threat Risk Assessment

	THREAT	LIKELIHOOD	IMPACT	RISK	COMMENT
S1	A node in the network is destroyed or disabled	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, standalone capabilities reduce the impact of this attack.
S2	A device in the network is disabled or destroyed	3	1	3	The requirements associated with survivability such as dual homing, FFR, backup power, COOP requirements, stand-alone capabilities reduce the impact of this attack.

As discussed in the earlier threat section, the threats are defined as critical, major, and minor according to the product of their likelihood of an attack being successful score and the impact of a successful attack score as shown in Figure 5.4.8-1, ETSI TIPHON Threat Risk Score.

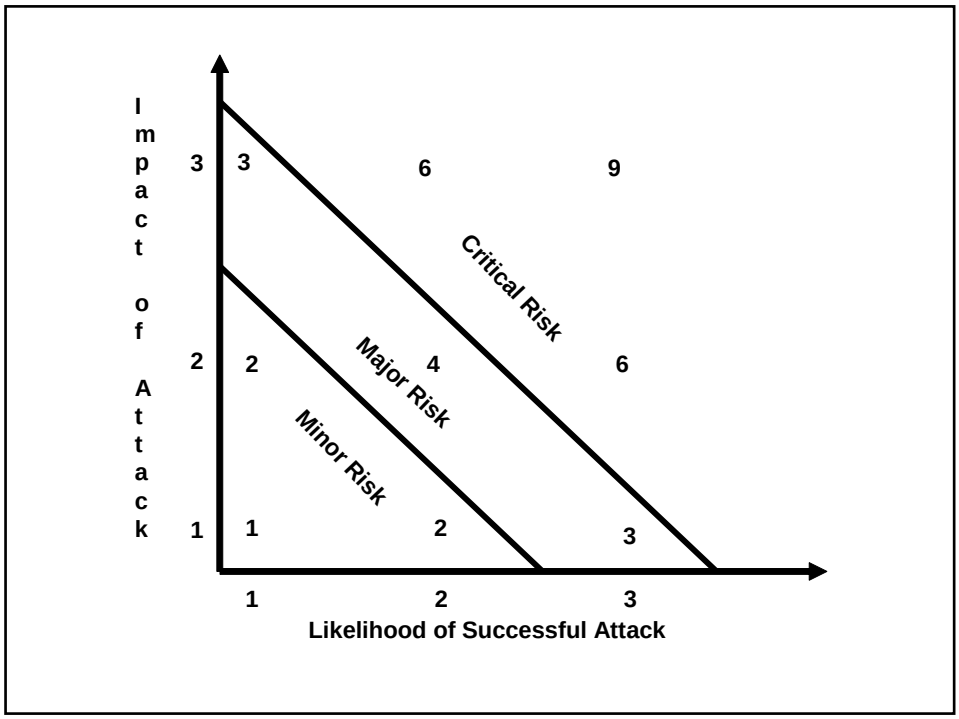

Figure 5.4.8-1. ETSI TIPHON Threat Risk Score

Based on the mitigations discussed in this UCR, all the critical risk threats have been mitigated to a major risk or below category. In addition, many of the major risk threats have been mitigated to a lower score or have been reduced to a minor risk. Table 5.4.8-9, Adjusted Risk Summary, tabulates the results of the risk mitigation effort.

Table 5.4.8-9. Adjusted Risk Summary

RISK LEVEL	NUMBER OF RISKS (BEFORE MITIGATION)	NUMBER OF RISKS (AFTER MITIGATION)
Critical Risks	27	0
Major Risks	16	31
Minor Risks	15	27
Total	**58**	**58**