DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

REAL TIME SERVICES INFORMATION ASSURANCE TEST PLAN

FEBRUARY 2009

REAL TIME SERVICES
INFORMATION ASSURANCE
TEST PLAN

FEBRUARY 2009

Submitted by: **Joseph Schulte**
Chief, Network Systems Branch

Approved by: _____
for RICHARD A. MEADOR
Chief, Battlespace Communications Portfolio

Prepared Under the Direction of:

Michael Napier
Joint Interoperability Test Command
Fort Huachuca, Arizona

(This page intentionally left blank.)

EXECUTIVE SUMMARY

The Department of Defense (DoD) Directive 8500.1 "Information Assurance (IA)," 24 October 2002, established the DoD policies for IA and directed that all information technology systems be IA tested and certified before connection to the Defense Information System Network (DISN). The DoD Instruction 8100.3, "Department of Defense Voice Networks," 16 January 2004, established the IA policy for DoD Voice Networks, including the Defense Switched Network (DSN). The Real Time Services (RTS) IA Unified Capabilities Requirements (UCR) document established the requirements for securing RTS systems. The DSN Single Systems Manager (SSM) is responsible for providing DSN IA test results to the DISN Designated Approving Authorities to grant IA certification and accreditation. The DSN SSM has designated the Joint Interoperability Test Command (JITC) as a responsible organization for DSN IA testing.

The JITC DSN IA Test Team (IATT) supports IA testing and the RTS IA UCR by determining the compliance of products before their use on DISN. Compliance methods include the Security Technical Implementation Guidelines, IA Vulnerability Management announcements (e.g., alerts, bulletins, and technical guidance), and IA requirements. In addition, the IATT performs scans for Internet Protocol (IP) vulnerabilities to determine the residual risks and threat levels of existing security implementations and/or the discovered security deficiencies. When systems meet the RTS IA requirements, this will allow the DSN to migrate smoothly from the current military-unique features of a circuit-switched service to a converged net-centric IP-based assured secure RTS in a manner consistent with the Defense Information Systems Agency (DISA) IP Convergence Master Plan.

Upon completion of IA testing, the IATT will analyze the data collected and present the test findings in an "IA Assessment Findings and Mitigations Report." This report will contain the IATT's findings for the system assessed and will identify the IA compliance status strategies. The IATT will deliver this report to the vendor so that the vendor may add any mitigation solutions. The assessment report, including the vendor's mitigation strategy, will be submitted to the Unified Capabilities Connection Office and the DISA Field Security Office (FSO) for comment. The FSO will write a certification and accreditation letter to the DISN Security Accreditation Working Group (DSAWG) and will brief the final assessment report to the DSAWG in a PowerPoint presentation. The DSAWG will decide whether to place the vendor's system on the Unified Capabilities Approved Products List, based on the findings and mitigations.

(This page intentionally left blank.)

TABLE OF CONTENTS

Page

APPENDICES

LIST OF FIGURES

TABLE OF CONTENTS (continued)

LIST OF FIGURES (continued)

Page

LIST OF TABLES

TABLE OF CONTENTS (continued)

LIST OF TABLES (continued)

Page

(The page intentionally left blank.)

INFORMATION ASSURANCE DESCRIPTION

The Department of Defense (DoD) Directive 8500.1 "Information Assurance (IA)," 24 October 2002, established DoD policies for IA and directed that all information technologies be IA tested and certified before connection to the Defense Information System Network (DISN). The DoD Instruction (DoDI) 8100.3, "Department of Defense Voice Networks," 16 January 2004, established the IA policy for DoD Voice Networks, including the Defense Switched Network (DSN). The DSN Single Systems Manager (SSM) is responsible for providing DSN IA test results to the DISN Designated Approving Authorities to grant the IA certification and accreditation. The DSN SSM has designated the Joint Interoperability Test Command (JITC) as a responsible organization for DSN IA testing.

The purpose of this document and its appendices is to provide information and guidance on Real Time Services (RTS) that must be used to acquisition all hardware and software that support RTS. The RTS Unified Capabilities Requirements (UCR) 2008 document is used to do the following:

- Establish standards and specifications needed by industry to develop compliant RTS solutions.
- Provide the foundation for the development and finalization of Generic System Test Plans for interoperability testing and IA Test Plans for IA testing. These tests assist in making decisions necessary to place products on the DoDI 8100.3 Approved Product List (APL) so that combatant commands, services, and agencies can purchase them.
- Provide the foundation for the development and finalization of the Security Technical Implementation Guidelines (STIG).
- Establish those STIGs needed to operate the approved products once installed in a secure manner.

The IA testing phases cover several areas. The first is the STIG testing phase, which assesses the system's ability to operate reliably in a secure environment. The STIG testing also evaluates the system's management interface. The Internet Protocol (IP) Vulnerability (IPV) phase covers the system's ability to resist attack and determines whether the system operates securely in an IP network. Appendix B lists the requirements used for assessments, and Appendix E lists the specific procedures for each phase of testing.

The architecture of the DSN is a two-level network hierarchy consisting of backbone switches and infrastructure (managed by the Defense Information Systems Agency (DISA)) and installation switches and peripherals (managed by military departments and agencies).

This two-level network hierarchy includes the following: The first level consists of components under test, which includes Tandem Switches, Multifunction Soft Switches (MFSS), Signal Transfer Points (STP), Network Management Systems, End Office (EO)

Switches, Private Branch Exchange (PBX) Types 1 and 2, Small End Office Switches, and Local Session Controllers (LSC). The second level is the backbone of the infrastructure, which consists of Deployable Voice Exchanges, Remote Switching Units, Video Teleconferencing, Customer Premise Equipment, Edge Bounder Controllers (EBC), Network Elements, Echo Cancellers, Integrated Access Switches/Systems, Assured Services Local Area Networks, and Conference Bridge.

The DSN provides end-to-end command and control (C2) capability via dedicated telephone service, facsimile, voice-band data, dial-up firewalls, IP Security (IPSec), and Transport Layer Security. The DSN comprises backbone and tandem switches, signaling system instruments, transmission connectivity between switches, installation switches, network management systems, and end devices. Voice processing and transport technologies, such as Voice over Internet Protocol (VoIP) and packetized Voice over Asynchronous Transfer Mode, are also elements of the DSN.

The RTS IA architecture and the associated UCR 2008 for the Sensitive-But-Unclassified architectures are described in the RTS UCR 2008. The DISN RTS UCR 2008 will ensure that the high-quality mission-critical interoperability and IA preserve today's technologies as the migration to IP is successfully accomplished.

INFORMATION ASSURANCE BACKGROUND

Vendors are continuously developing new features and functions to meet user demands and to correct any deficiencies within the solution. As of January 2004, DoDI 8100.3 mandates all systems that connect to or will connect to the DSN undergo IA certification. The APL is the only listing of equipment authorized by DoD to be fielded in the DISN. The first part of the APL Certification Process is IA accreditation testing (e.g., DSN IA testing). If the product does not meet the requirements for IA accreditation, it returns to the vendor for correction and the testing cycle starts over. If the solution meets the requirements for IA accreditation, it continues to the second part of the test cycle, Interoperability (IO) testing. When IA accreditation and IO certification are granted, the solution is then included on the Unified Capabilities (UC) APL. A product will not progress to an RTS assessment unless its baseline has received certification.

To enhance the vendor's IA posture and readiness strategy, JITC conducts IA assessments of vendors' products before they undergo IO certification. Program Managers or DoD agencies must obtain IA accreditation for all telecommunication equipment that is procured for use on the DSN, whether the equipment is new or is an updated version of equipment already in the DSN. Those DoD information systems must also identify, implement, and manage IA Controls based on the DoD IA Certification and Accreditation (C&A) Process (DIACAP), as described in Appendix B, paragraph B-3.

DEFENSE-IN-DEPTH AND REQUIRED ANCILLARY EQUIPMENT (RAE)

The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigations is through the following: the integration of people, technology, and operations; the layering of IA solutions within and among Information Technology (IT) assets; and the selection of IA solutions based on their relative level of robustness. This combination produces layers of technical and non-technical solutions that do the following: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

The use of RAE components can aid the site in developing and implementing its Plan of Action and Milestones to supplement the DIACAP accreditation package. Use of this equipment or software provides additional security features to the existing environment, which may already be present in a government infrastructure and enforce defense-in-depth. As a minimum, RAE may consist of one or a combination of the following:

1. Microsoft Windows Server 2003 Internet Authentication Service Remote Authentication Dial-In User Server (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+)
2. Active Directory
3. SysLog Server
4. Public Key Infrastructure

INFORMATION ASSURANCE PURPOSE

The purpose of this RTS IA test plan is to provide a consistent set of guidelines for testers and developers to evaluate the operation of any switch system for the applicable STIG, RTS IA requirements, and IPV requirements.

REQUIREMENTS

The number of DoD regulations, policies, and guidance documents for security-related activities has grown significantly over the last several years as the DoD community has devised standard IA practices to protect its assets and information. Government regulations now cover all aspects of IA, including the acquisition, deployment, and use of IA and IA-enabled IT products. Appendix F contains the full list of references. The JITC IA Test Team (IATT) will verify that each system tested will conform, at a minimum, to the requirements in the following documents:

- Chairman of the Joint Chiefs of Staff Instruction 6215.01B – This instruction establishes policy and prescribes responsibilities for use and operation of the

DoD voice networks, specifically the DSN and the Defense Red Switch Network

- Chairman of the Joint Chiefs of Staff Instruction 6510.01 – Provides details and further references for selecting and implementing security requirements, controls, protection mechanisms, and standards
- DoD Instruction 8500.2 – Provides details and further references for selecting and implementing security requirements, controls, protection mechanisms, and standards. It also combines mission assurance categories and confidentiality levels with best security practices, general threat information, federal and DoD policy requirements, and enterprise operational and technical considerations in a graded or banded risk model
- Federal Information Processing Standards Publications (FIPS Pubs) 140-2 – This standard specifies the security requirements that will be satisfied by a cryptographic module used within a security system protecting sensitive but unclassified information
- DIACAP Guidance – Under this directive-type memorandum all DoD components are to immediately follow the DoD C & A guidance for the operation of all DoD information systems. This memorandum supersedes existing DoD Information Technology Security C & A Process (DITSCAP) guidance under DoDI 5200.40 and DoD 8510.1
- The National Information Assurance Partnership – This is a U.S. Government initiative originated to meet the security testing needs of both IT consumers and producers, and is operated by the National Security Agency.
- National Institute of Standards and Technology (NIST) Special Publication 800-40 (Version 2) – Provides guidance on patch and vulnerability management
- NIST Special Publication 800-42 – Provides guidance on network security testing
- NIST Special Publication 800-53 – Requires that vulnerability scanning be conducted using appropriate scanning tools and techniques.

These documents are available on the Internet, either free of charge or for a licensing fee.

SCOPE

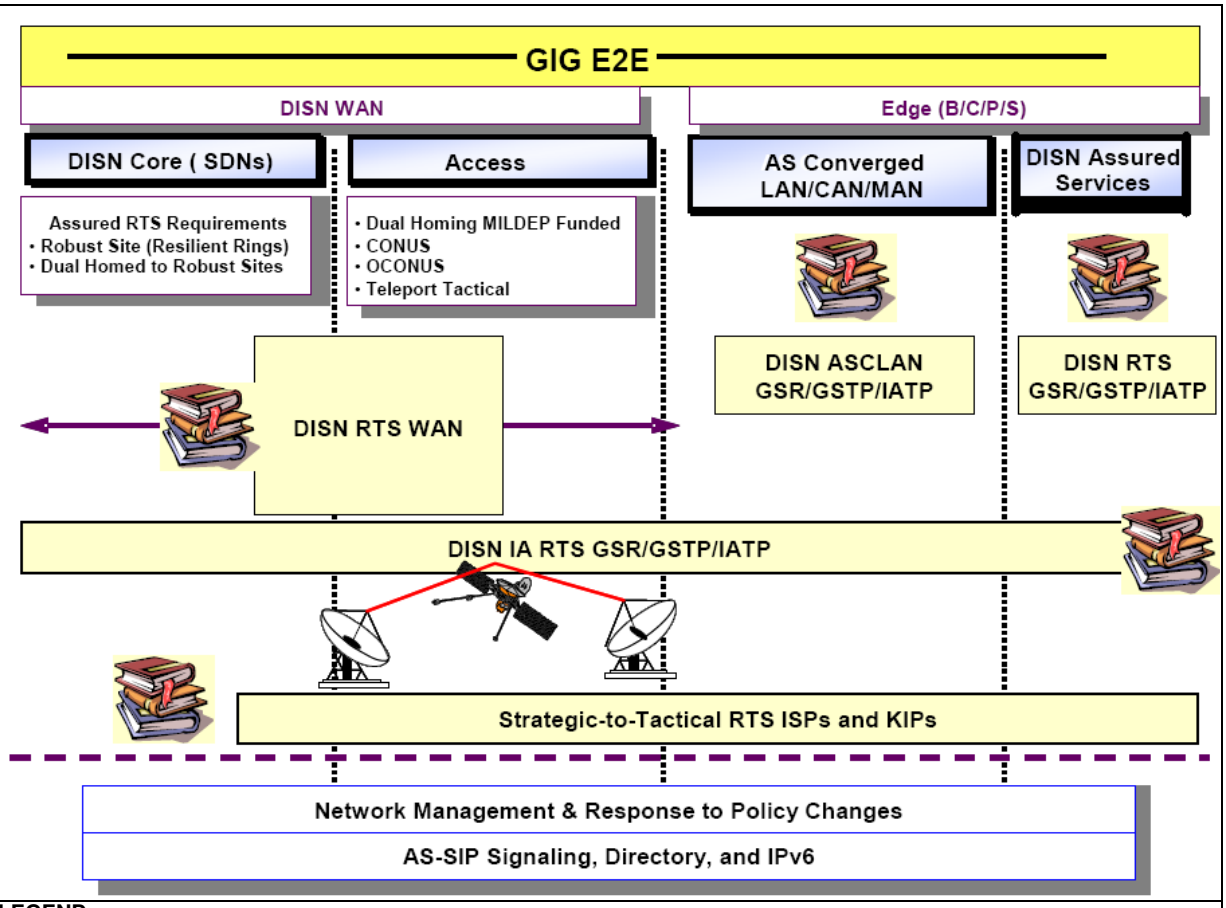
The RTS IA test plan covers both traditional telecommunications (Time Division Multiplexer/Multiplexing components) switching equipment and IP-enabled or IP-centric switching equipment. The JITC IA process for evaluating VoIP products determines the security level of individual VoIP- and IP-enabled products connected to the DSN or on a converged network that is IP enabled from the trunk side as well as the line. The IA phase of testing consists of the following two phases:

- **Phase I: STIG and Other IA Requirements.** Phase I testing involves applying predetermined STIGs and other IA requirements to various components of the vendor solution and recording any discrepancies that may

arise from application of the STIG. The STIG applicability is determined by attributes, such as the underlying operating system for the solution (e.g., Windows, Linux, and UNIX), applications or services that operate on the solution, and the overall functionality of the solution (e.g., MFSS, Local Session Controller (LSC), Edge Border Controller (EBC), Private Branch Exchange (PBX), router, switch, server, and workstation). Any individual solution may require the application of one or multiple STIG. Other requirements from the IA UCR are also applied, and the RTS STIG applies to management interfaces for the solutions. The lab assessment contains a DIACAP control correlation matrix (scorecard) that addresses the DoD IA Control. The DIACAP package, along with the IA report, can assist the site in creating and implementing its baseline, providing a foundation for achieving its Interim Authority to Operate. Both requirements and implementation procedures are discussed in Appendices B and E, respectively.

- **Phase II: IP Vulnerability Scans/Protocol Analysis.** Phase II consists of scanning and/or attacking the vendor's solution using the tools available to an attacker (or hacker) intent on penetrating a network or system. Vulnerability analysis for custom software or applications protocols such as Signaling System 7 (SS7), Primary Rate Interface, Channel Associated Signaling, European Carrier 1 (E1), Telecommunications Carrier 1 (T1) Session Initiation Protocol (SIP), and Secure Real-time Transport Protocol (SRTP) may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, and statistical analysis of source code). The scan results are packaged in human-readable form in portable document format (PDF) and are part of the DIACAP submission. Appendices B and E contain detailed procedures.

Roles of UCR 2008 and Generic System Specification (GSS) Documents. The UCR 2008 is used for acquisitions and with APL and IA testing that JITC conducts. The GSSs were developed for the key technologies and capabilities critical to interoperability, Assured Services SIP and the Wide Area Network (WAN). Each requirement from the UCR 2008 and GSS supports the collaborative development of Information Support Plans (ISP) and Key Interface Profiles (KIP) for programs that meet requirements listed in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E need DISN RTS connection approval. Figure 1 provides an overview of the relationship among the RTS UCR 2008 and their associated test plans, ISPs and KIPs, and RTS architecture.



LEGEND:

AS	Assured Service	IATP	Information Assurance Test Plan
ASCLAN	Assured Service Converged Local Area Network	IPv6	Internet Protocol Version 6
AS-SIP	Assured Services Session Initiation Protocol	ISP	Information Support Plans
B/C/P/S	Base, Camps, Posts, and Stations	KIP	Key Interface Profiles
CAN	Converged Area Network	LAN	Local Area Network
CONUS	Continental United States	MAN	Metropolitan Area Network
DISN	Defense Information System Network	MILDEP	Military Department
E2E	End to End	OCONUS	Outside Continental United States
GIG	Global Information Grid	RTS	Real Time Services
GSR	Generic System Requirements	SDN	Secure Data Network
GSTP	Generic Switch Test Plan	UCR	Unified Capabilities Requirements
IA	Information Assurance	WAN	Wide Area Network

Figure 1. Overview of the Relationship Among the RTS UCR, ISPs, KIPs, and RTS Architecture

LIMITATIONS

Parts of the STIG are not assessed because the System Under Test (SUT) is not deployed in an actual operational environment. The DIACAP Scorecard shows these items as “site responsibility” or “not applicable” for the SUT. Some of these items include aspects of enclave security, personnel qualifications, training, and contingency planning (e.g., disaster recovery plans, backups, storage of media, and incident reporting). The RTS assessments include local network and firewall configuration and meet appropriate standards. As part of the local C & A package the installers should assess these items, as well as other DoDI 8500.2 IA Controls, at the local site.

METHODOLOGY

The RTS IATT performs assessments using the methodologies presented in this plan. The methods cover Phase I and Phase II IA testing, including STIG testing and other IA requirements, IPV scanning tests, Protocol Analysis (PA) SS7, SIP, H.323, and SRTP protocol analysis testing.

Certification Process Overview. Figure 2 depicts the steps in the IA and IO APL product certification process. The RTS accreditation process will follow the same steps as the APL process. When a vendor desires to have a product evaluated, the vendor contacts the DSN Unified Capabilities Connection Office (UCCO). The UCCO has standard procedures for processing vendor requests for placement on the APL testing cycle. The APL Test Bundle has detailed procedures and is located at <http://www.disa.mil/gs/dsn/jic/index.html>.

Part One of the APL Certification Process is the IA certification testing. If the product does not meet the requirements for IA certification, the solution is returned to the vendor for correction and the testing cycle starts over. If the solution meets the requirements for IA certification, it then continues with Part Two of the test cycle, IO testing.

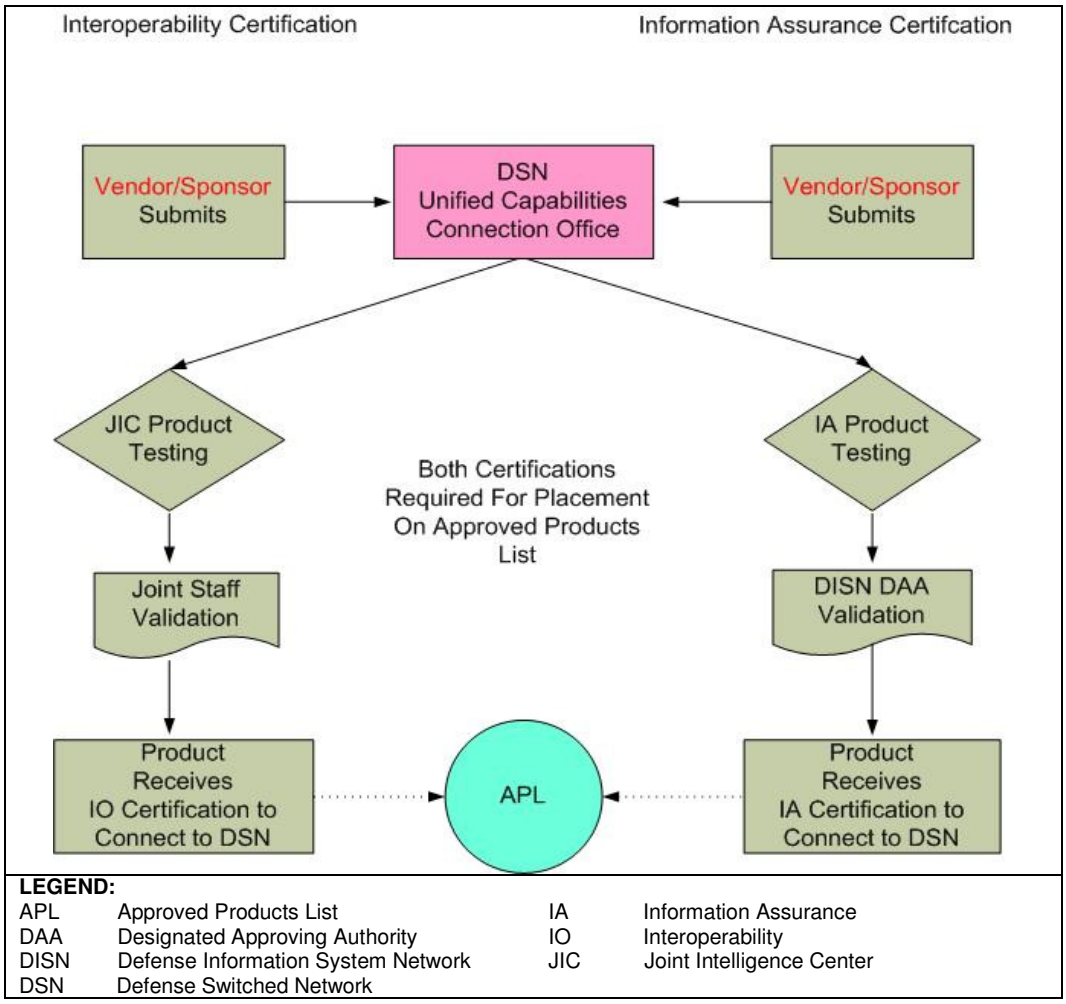


Figure 2. IA and IO APL Certification Process Flow

The following is a brief overview of the UC IA testing process and describes what the vendor should expect:

- The AO coordinates payment of lab testing fees/Cooperative Research and Development Agreement (CRADA) agreements with Action Officer (AO).
- The vendor downloads APL Test Bundle at <http://www.disa.mil/dsn/jic/>. The vendor also reviews the bundle and submit documentation in accordance with the APL Documentation Guide, which is included in the APL Test Bundle.
- The IATT applies applicable STIGs and submit to UCCO within 2 weeks before the scheduled test window.
- The UCCO receives and reviews the test submittal package from the applicant. A tracking number is assigned to the solution and the package is provided to the Government AO. The AO will contact the vendor with further instructions.
- The vendor provides on-site engineering support for the SUT during all phases of testing.

- Once the DSN-UCCO has assigned the vendor a tracking number, the DSN-UCCO, in coordination with the IATT, will assign testing dates. The vendor is required to submit a Self-Assessment Report (SAR).

Appendix E provides detailed instructions for testing. A self-assessment determines if the vendor's product will meet standards necessary to proceed to test. Self-assessments should include STIGs identified in the initial contact meeting. The meeting minutes describe what STIGs will apply, as well as the "what, when, where, and how" to test the vendor solution. The following also may apply during a test:

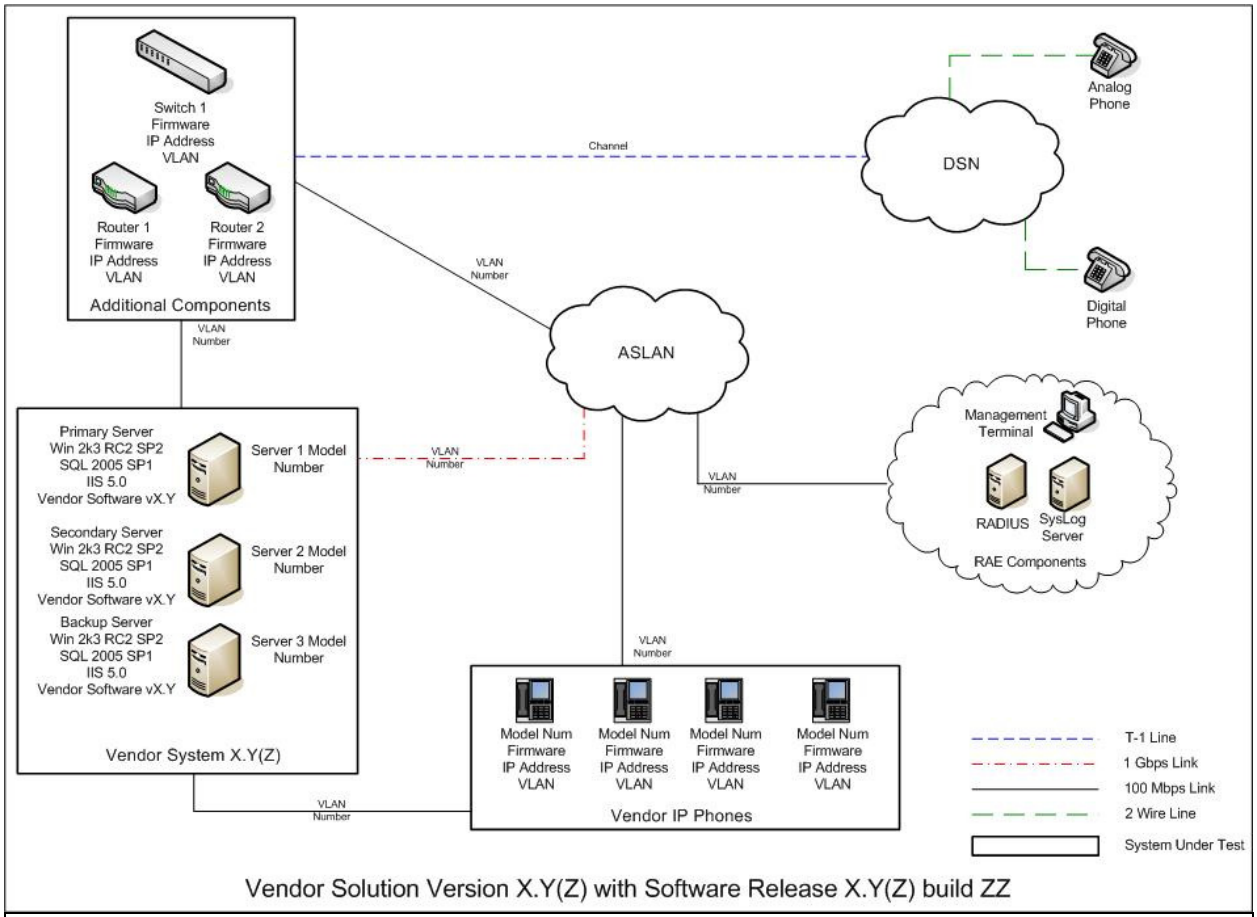
- Security Readiness Review (SRR) Evaluation Scripts – Test products for STIG compliance. Scripts are available for all operating systems and databases that have STIG and web servers using Internet Information Services.
- Gold Disks – The DISA Field Security Office (FSO) designed and developed Gold Disks to assist system administrators in securing Windows operating systems and desktop applications in accordance with the guidance in the DISA STIG and checklists. The Gold Disks support the ability to detect installed products, identify and remediate applicable vulnerabilities, and generate a file that the tester can use for the assessment. The software assists to secure:
    - Windows 2000 (Professional, Member Server, Domain Controller)
    - Windows Experience (XP)
    - Windows 2003 (Member Server, Domain Controller)
    - Desktop applications (e.g., Microsoft Office, Netscape Navigator, Internet Explorer, and Antivirus products)
    - Internet Information Services Versions 5.0 and 6.0
- RTS IA Requirements – These requirements are defined in the RTS UCR 2008 and cover all other requirements that the DISA STIG do not address. The set of derived requirements developed for the RTS IA Architecture threats and countermeasures are a combination of the different functions that vendors created to meet the requirements of a particular type of appliance.

The vendor must deliver a SAR based on their results to the UCCO no later than 30 days before the test. Not receiving the SAR within the 30-day timeframe results in the UCCO canceling the test. The UCCO consolidates self-assessment results and sends them to the IATT and the FSO for review. The IATT and FSO notify the UCCO with a recommendation whether to proceed to test. If the vendor receives a negative recommendation from the FSO, they will have the opportunity to address their concerns. The IATT will ensure the vendor, sponsor, and IATT have constant communication, so that the vendor has the opportunity to complete any fixes before arriving on site. Appendix E provides additional details about self-assessment procedures.

TESTING METHODOLOGY

This section describes the methodology used for testing and the steps taken during the various phases of testing STIG, IA Requirements, IPV, and PA SS7. Because of the sensitive nature of testing, all data collected is considered sensitive and is exempt from the Freedom of Information Act. All tests consist of developing a test packet, obtaining vendor documentation, conducting a functionality test before and after each phase of testing, and then conducting an outbrief that leads to the Final IA Assessment Report. Appendix E contains detailed procedures.

Test Packet. Appendix C illustrates the data collection forms used at JITC. The IATT use the forms during Phase I. The forms include the SUT network diagram and components within the test lab as shown in Figure 3. The tester may add testing information to this document during the course of the assessment as needed. The IPV testers also use this information to perform their assessment's. The vendor and the testers will verify all hardware and software before starting the IO test.



LEGEND:

ASLAN	Assured Services Local Area Network	RAE	Required Ancillary Equipment
DSN	Defense Switched Network	SP	Service Pack
Gbps	Gigabits per second	SQL	Structured Query Language
IP	Internet Protocol	T-1	T-Carrier 1
IIS	Internet Information Service	VLAN	Virtual Local Area Network
Mbps	megabits per second	Win2k	Windows 2000
Num	Number	Win2k3	Windows 2003
RADIUS	Remote Authentication Dial In User Services		

Figure 3. Sample Diagram for Submission

Vendor Documentation. Reviewing vendor documentation is vital to a successful test. Although testing all possible scenarios within the vendor scope is not possible, understanding the product's general use, features, and functionality assists the test team in its evaluation. The documentation and information includes the vendor's web page, product manuals, whitepapers, newsgroups, forums, user mailing lists, and vendor self-assessments. The team members look at these, as well as other documents, to understand the products they are evaluating and to find possible weaknesses and vulnerabilities that other sources may have found.

The test preparation document generated during the Phase I of testing contains the vendor and tester contact information, IP addresses, test equipment hardware, software, and version information, IP phone information, and other applicable information to the testers. Figure 3 depicts a sample vendor diagram that is used to aid

the tester and reader in understanding how the system interconnects. An example of the test preparation document is located in Appendix C, Test Preparation Documents. The signature page shows the names of individuals who have verified that the hardware, software, and version information is correct. The testers sign the page and deliver the packet to the tester responsible for Phase II when they are finished; when all IA phases are completed, the packet is turned over to the IO tester for verification and is used to minimize duplicate efforts.

Functionality Tests. Testing the SUT's functionality ensures that the product operates as designed in a fielded production environment. Results due to services not functioning correctly, disabled services, and applications not communicating correctly can provide a false sense of security because not all aspects of the test product could be evaluated. Completing the functionality test at the beginning and end of every phase of testing ensures that any settings or changes made during testing did not affect the functionality of the product. Functionality testing will vary from test-to-test, depending on the SUT. The functionality test will target basic operational functions. It is not an IO test.

Some products, such as Customer Premise Equipment (CPE), rely on external systems to exercise their capabilities. For example, a secure modem solution does not function unless an external switch initiates a call. In this case, the external switch is outside the scope of the IA test; however, the tester and vendor must ensure it is operational to perform testing on the secure modem solution. While conducting functionality tests, IP traffic is monitored (sniffed) and saved at the conclusion of the functionality test for further evaluation, if necessary.

RTS-SPECIFIC REQUIREMENTS AND METHODOLOGY

The RTS system is an inter-base, nonsecure or secure C2 IP telecommunications system. It provides end-to-end command use and dedicated telephone service, voice-band data, and dial-up and dedicated Video Teleconferencing (VTC) for C2 and non-C2 DoD, to authorized users, in accordance with national security directives. Dial-up telephony, conferencing, and video services are the system’s principal requirement, in accordance with the CJCSI 6215.01B, “Policy for Department of Defense Voice Services.”

Security threats are the primary concern for all stages of the IA process; however, other factors such as politics, time, and technical motivators influence architectures. The structure of the RTS IA UCR is in a manner that follows the IA process in the development of the RTS IA Architecture and requirements.

Tables 1 and 2 display the threat matrix used by the DISN IP RTS. It is based on one developed by the European Telecommunications Standards Institute (ETSI) Technical Standard and described in the “Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); Protocols Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis.” The threats identified by the ETSI

TIPHON work focus on the nonphysical threats and do not address the physical threats to the system. The test team conducts a risk analysis of the identified 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 impact. The overall security risk is the product of the likelihood of occurrence and the impact scores.

Table 1. 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 state 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.

LEGEND:
ETSI European Telecommunications Standards Institute TIPHON Telecommunications and Internet Protocol Harmonization over Networks

Table 2. ETSI TIPHON Threat Impact Scoring Criteria

Score	Impact	Description
1	Low	The concerned party is not severely harmed; 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.

LEGEND:
ETSI European Telecommunications Standards Institute TIPHON Telecommunications and Internet Protocol Harmonization over Networks

The tester determines a final score by multiplying the likelihood score by the impact score to establish the final threat level for the system tested. In the converged networks planned for DoD, this may involve either data or RTS-type attacks. Of particular concern is an RTS attack that involves a high number of illegitimate precedence calls preventing access to the network for legitimate high-precedence RTS calls. A Denial of Service (DoS) attack can occur at all three layers: signaling, bearer, or network management. The principal security goal affected by this type of attack is availability and is more likely to occur in a converged network.

STIG ASSESSMENT METHODOLOGY

The DoD uses STIGs to strengthen and assess the security posture of a system or component. Findings resulting from applying the Gold Disks and scripts are indications of weaknesses in the security posture of the system or component. Findings from the STIG are grouped into four Categories (CAT) based on the severity of the weakness. The findings will correspond to IA Controls that are listed in Appendix B and

annotated on the DIACAP Scorecard, as shown in Appendix E. The scorecard is a summary report illustrating the certified or accredited implementation status of a DoD information system's assigned IA Controls. It supports or conveys a certification determination and/or accreditation decision. The DIACAP Scorecard is intended to convey information about the IA posture of a DoD information system in a format that can be easily understood by managers and be easily exchanged electronically. The DIACAP is the DoD process for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, federal, and DoD requirements. The following list shows the high-level procedures for Phase I testing:

1. **Apply STIG/SRR/Checklists**
    - Validate SUT is operational and conduct functionality checks before starting the assessment.
    - The DoDI 8500.2 defines Mission Assurance Category (MAC) I as: "Systems categorized as 'MAC I' process data that is vital to the operational readiness or mission effectiveness in terms of both content and timeliness. MAC I systems require high confidentiality, integrity, and availability to accomplish their missions; therefore, they are categorized as critical network components." It is understood that the Defense Red Switch Network is a MAC I system and the DSN is a MAC II system, but since it is unknown where the system will be deployed and if the MAC levels will remain consistent, it is appropriate to test every system at the MAC I level. If the system performs at the MAC I level, then all MAC levels will be satisfied.

2. **Collect Data**

    - Document findings:
        - Note any findings deemed not applicable.
        - Note any fixes performed by the vendor and ensure they are documented in the vendor's security configuration guide.
        - Note any findings deemed as false positives.
    - Document the IA Controls as needed to the DIACAP Scorecard.
    - Document test limitations.
    - Determine that SUT is operational and conduct functionality checks after completion of assessment.

3. **Perform Data Analysis and Report Results**

Data collected from the STIGs, their respective checklists, and any SRR scripts will be analyzed to accomplish the following assessment objectives:

- Identify and attempt to eliminate false positive results.
- Highlight and categorize findings according to their level of importance, whether vulnerabilities are CAT I (high), CAT II (medium), and CAT III (low).
- Provide recommendations to remediate or mitigate the risks.

- Document the IA Controls as compliant or non-compliant to the DIACAP Scorecard.

RTS IA REQUIREMENTS METHODOLOGY

All requirements are derived from the 39 documents/instructions referenced in Section 2, Appendix D, of the RTS UCR. The requirements are divided into six sections: General, Authentication, Integrity, Confidentiality, Non-Repudiation, and Availability. Tables E-7 through E-12 list the requirements, delineated by the affected system and the relevant test procedures.

The requirements in Appendix E are consistent with the those in the Generic Requirement (GR)-815-CORE, but are adapted for the unique DoD RTS environment as required by the Generic Switching Center Requirements and contains detailed procedures. The test procedure field in Appendix E describes how the services are applied to the system and how the appliances interact in a secure manner.

1. Determine Test Conditions

- Perform a functionality test at the beginning and end of the test.
- Identify and verify all IP interfaces are operational.
- Verify that the system is operational.

2. Prepare for Test

- If the SUT supports lines, the following manual calls should be attempted: Analog-to-Analog, IP-to-IP, Analog-to-IP, and IP-to-Analog. Confirm that test calls are completed and all IP handsets are identified.
- If the SUT supports trunks, the following manual calls should be attempted: Analog over trunk and IP over trunk. Confirm that all test calls are completed. Trunks are defined as allowing a group of inlet switches or circuits to connect at the same time. Thus, the service provider can provide a lesser number of circuits than might otherwise be required, allowing many users to “share” a smaller number of connections and achieve capacity savings.

3. Apply Test Procedures

- Follow the test procedures in Tables E-7 through E-12 in Appendix E.
- Document findings:
    - Note any findings deemed not applicable.
    - Note any fixes performed by the vendor and ensure they are documented in the vendor’s security configuration guide.
    - Note any findings deemed as false positives.
- Document the IA Controls as needed to the DIACAP Scorecard.
- Document test limitations.
- Determine that SUT is operational and conduct functionality checks after completion of assessment.

4. Perform Data Analysis and Report Results

- Identify and attempt to eliminate false positive results.
- Highlight and categorize findings according to their level of importance, whether vulnerabilities are CAT I (high), CAT II (medium), or CAT III (low).
- Provide recommendations to remediate or mitigate the risks.
- Document the IA Controls as compliant or non-compliant to the DIACAP Scorecard.

5. Document the IA Controls as compliant or non-compliant to the DIACAP Scorecard.

IPV TESTING/PROTOCOL ANALYSIS METHODOLOGY

The IPV test team conducts vulnerability assessments and penetration testing for RTS telecommunication equipment destined for connection to the DSN.

The purpose of a vulnerability assessment is to analyze the system in its entirety and find areas where attacks might be more likely to occur, without necessarily exploiting the problems identified. A vulnerability assessment typically involves investigation of the operating system to determine whether current patches are applied, whether the system is configured in a manner that makes attacks more difficult, and whether the system exposes any information that an attacker could use to exploit other systems in the enclave. Vulnerability assessments use a number of commercial and proprietary tools to minimize false positives.

The purpose of a penetration test is to simulate an attack on the vendor's system within a specified environment. While a number of changing parameters might determine how the attacks are initiated and conducted, the defining characteristic of a penetration test is that IA testers will be actively attacking the system using the same or similar methods to what an actual attacker would use.

The following DoDI 8500.2 IA Controls apply to the IPV testing procedures: Design and Configuration Ports Protocols and Services (DCPP-1), Enclave and Computing Environment Voice over IP (ECVI-1), Enclave and Computing Environment Transmission Integrity Controls (ECTM-2), Vulnerability Incident and Vulnerability Management (VIVM-1), and Enclave and Computing Monitoring and Testing (ECMT-1).

The IPV test team conducts vulnerability scanning with penetration tools and techniques. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for application, source code reviews, and statistical analysis of source code). The following steps outline the general procedures that the test teams employ. Appendix E contains detailed procedures.

1. Perform Identification and Verification

- IP Interface Identification – Identify and verify all operational IP interfaces.

2. Determine Test Components

- If the system supports lines, the following manual calls should be attempted: Analog-to-Analog, IP-to-IP, Analog-to-IP, and IP-to-Analog. Confirm that all test calls are completed and all IP handsets are identified.
- Trunks allow a group of inlet switches or circuits to connect at the same time. The service provider can provide a lesser number of circuits than might otherwise be required, allowing many users to "share" a smaller number of connections and achieve capacity savings. If the system supports trunks, the following manual calls should be attempted: Analog over trunk and IP over trunk. Confirm that all test calls were completed.

3. Discover Host

Finding all the hosts in use by the system is the first step in the technical evaluation. Detecting all the protocols and services in use by the system and their corresponding IP addresses and port information is required to begin any further technical evaluation.

4. Conduct Ping Sweep

A general ping sweep will determine what hosts are available via the Internet Control Message Protocol (ICMP). This is generally an ICMP echo request (type 8) to elicit an ICMP echo reply (type 0) from a host.

5. Conduct Transmission Control Protocol (TCP) Sweep

The TCP sweep provides insight into available hosts when ICMP is disabled. A TCP sweep will attempt to make TCP connections to a host range on a specified port list. The client will send a Synchronize (SYN) and, if the host is available on that port, the client will receive a SYN/Acknowledge (ACK) and respond with an ACK packet to the target host with a sequence number incremented by one.

6. Perform Traffic Analysis

Traffic Analysis allows the test team to determine all the hosts that are included within the solution under test.

7. Perform Port Enumeration

Port Enumeration provides a list of services or applications that could be running on the host and gives the tester a good indication of what operating system might be present on the end-point. Port scanning of each host will provide a detailed list of which ports are open, closed, or filtered on a specified host. Port scans are conducted using a variety of methods to include different protocols, packet flags, and DoS techniques. These different scans can yield different results in different situations, depending on the

configurations and protections of each host. Additional Open Source Security Testing Methodology Manual strategies are in Appendix E.

8. Conduct Service Enumeration

Service Enumeration determines what services are listening on an IP port of the system. Services and their versions can provide the IATT with a list of known exploits or weaknesses that might be effective against a given target.

9. Perform Service Analysis

The use of Service Analysis provides the test team with specific service details in further attacks. Upon discovery of a service, a variety of checks may be completed against it.

10. Evaluate DoS

A DoS determines the system's susceptibility to attacks. The IATT might take a particular end-point offline to capture one of its attributes, such as IP address or Media Access Control address.

11. Package for DIACAP

Package all raw results generated from the test into a readable format and add to the report.

Protocol Analysis (PA). The test team conducts generic PA requirements for the APL inclusion. Additional specifications include those found in American National Standard Institute T1.111 through T1.116. The system is evaluated for its ability to maintain confidentiality, integrity, and availability. Detailed test procedures are in Appendix E.

Example Results. Results that testers document in the draft IA Findings and Mitigations Assessment Report are shown in the example below. Findings from each STIG, IA Requirements, and Penetration testing requirement with and without RAE influence the vendor's system. All findings will show each component affected by the finding and any findings that the vendor or sponsor mitigated by secure RAE. The findings with RAE are the remaining number of findings inherent to the system. Each finding will show the security requirement, associated vulnerability, and impact of the vulnerability. Section 5, Summary, shown below, is from an actual result findings report of a SUT; however, actual test results have been removed and annotated with fields marked "##".

> **5. SUMMARY.** Table 3 depicts critical testing requirements and summary findings that were identified while undergoing Defense Switched Network (DSN) Approved Products List (APL) certification. A finding is a discrepancy requiring investigation for a potential vulnerability that could be exploited given certain conditions. An analysis of each finding must be conducted to determine its impact to the overall security posture of the system under test. The findings listed in the column without secure Required Ancillary Equipment (RAE) (W/O-RAE), see Appendix, are the total number of findings present within the system.

These findings would be present if a defense in depth strategy or any other mitigations are not applied by the site acquiring this product. The findings in the column with RAE (W-RAE) are the remaining number of findings inherent to the system. If properly fielded with secure RAE, which comprise equipment installed and maintained in a secure facility in accordance with Enclosure 4 to Department of Defense Instruction (DoDI) 8500.2, "IA Implementation," dated 6 February 2003, can be eliminated. Additional details are found in Paragraph 13, Test Results and IA Findings, explaining which secure device and vendor mitigations needs to be used to mitigate the specific finding.

Table 3. SUT IA Test Summary

Requirements	Critical	W/O-RAE	W-RAE	Page Number
STIG	Yes	## Findings ## CAT I ## CAT II ## CAT III	## Findings ## CAT I ## CAT II ## CAT III	2-8
IP Vulnerability	Yes	## Findings ## High Risk ## Medium Risk ## High Risk	## Findings ## High Risk ## Medium Risk ## High Risk	2-45

LEGEND:

CAT	Category	SUT	System Under Test
IA	Information Assurance	W-RAE	With Required Ancillary Equipment
IP	Internet Protocol	W/O-RAE	Without Required Ancillary
STIG	Security Technical Implementation Guidelines		

Following the outbrief meeting and the completion of all action items, the IA task leader prepares a final report and submits it to the government for approval. The IA task leader distributes copies to all parties, including the FSO for the Certifying Authority (CA). The CA will send a letter to the DISN Security Accreditation Working Group recommending that the SUT be placed on the APL. Scan and test results are provided with the recommendation letter as baseline examples for sites to use when assessing their solutions and creating their DIACAP artifacts.

MANAGEMENT STIG/RTS STIG

System/device and network element management access is typically the most vulnerable part of any system. Management access is subject to an insider threat from those individuals who have authorized access to the management interface/system. Management access is also vulnerable to the outsider threat from those individuals or entities that can gain access to the management traffic and interface from the network through legitimate or nefarious means. This test plan references the IA measures or requirements necessary to secure and control the management interface of the managed device itself, as well as the management access methods. This begins with the various connection types and their access methods.

For the purpose of this test plan, a "network/system component" refers to network elements or attached systems/devices. Network elements are the hardware devices that provide transport of information in the form of data packets. A network

element can be a router (in the Local Area Network (LAN) or WAN), Layer 2 or Layer 3 LAN switch, multiplexer (M13, Add-Drop, etc.), multi-service provisioning platform, optical transport device (Synchronous Optical Networking (SONET) of Dense Wavelength Division Multiplexing (DWDM)), Digital Cross Connect, or Telecommunications switch (tandem/backbone, Mulifunction Switch (MFS), MFSS, Soft Switch, EO, PBX, LSC, etc.). A system is a single device (box/platform) or a collection of devices. Devices and systems have associated applications that provide services to users. A network attached system/device uses the network transport services to communicate with other systems/devices. A firewall is a system/device that is between networks but can also evaluate a network element. Network traffic and other information related to the management of DoD systems or devices is always considered, at a minimum, to be sensitive information and must be protected as such. It is never publicly releasable nor is it releasable to the general DoD workforce and/or warfighter. In general, management traffic and associated documentation take on the classification of the system managed. Some requirements were derived from the Telcordia Technologies Generic Requirements and are separated into specific areas, as shown in Table 4, and into four parts, as shown in Table 5.

Table 4. Additional IA Requirements (GR-815 CORE)

GR-815 CORE		
Requirement	**Date**	**Standard**
Identification	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Authentication	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Confidentiality	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
System Access Control	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Resource Access Control	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Audit Log	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Data Integrity	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
System Integrity	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Continuity of Service	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Security Administration	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
Non-Repudiation	Issue 2; Mar 2002	Telcordia Technologies Generic Requirement
LEGEND: GR Generic Requirement		

Table 5. RTS STIG Sections

RTS STIG	
Part	**Description**
Part 1	Part 1 of the RTS STIG contains the following five sections: Introduction, DoDD 8500.1 and DoDI 8500.2 policies, the system/device management types to include the methods and definitions, In-band management implementation requirements (e.g., traffic encryptions, to/from authorized IP addresses), and out-of-band management implementation requirements.
Part 1B	This STIG portion includes the remote management from outside the management enclave (e.g., privileged access requirement, justification, boundary protection mechanisms, remote access VPN, etc.).
Part 2	Part 2 contains STIG portion for Enterprise System Management and NMS Applications, Management Asset Security, System/Device Management Port Security and Behaviors, and Management Traffic and Protocol Security (e.g., DoD IP ports and protocols, FTP/SSH usage, SNMP, etc.).
Part 3	Part 3 includes the following: Management Access Control to include AAA and the implementation requirement (e.g., password requirements).
Part 3B	Part 3B contains the specifications for Local Emergency Management Accounts to include the creation of Local Emergency Management Accounts, managed access of RTS accounts, and management for group accounts.
Part 4	Part 4 contains the final portions of the RTS STIG pertaining to Privileged Accounts, Roles and Authorization, Account documentation and storage to include configuration files, and access to audit files. Discussion of Accounting and Accountability in relation to auditing of DoD Information Systems, reporting requirements for audit trails, alarms/alerts, and review and monitoring of management systems. Vulnerability and Patch Management are also included in this portion of the STIG checklist.

LEGEND:

AAA	Authentication, Authorization, and Accounting	NMS	Network Management System
DoD	Department of Defense	RTS	Real Time Services
DoDD	Department of Defense Directive	SNMP	Simple Network Messaging Protocol
DoDI	Department of Defense Instruction	SSH	Secure Shell
FTP	File Transfer Protocol	STIG	Security Technical Implementation Guidelines
IP	Internet Protocol	VPN	Virtual Private Network

MANAGEMENT TRAFFIC

Management Traffic is any network traffic that is related to NetOps, Operation, Administration, Maintenance, and Provisioning, and/or Fault, Configuration, Administration, Performance, and Security monitoring. Network traffic between network elements, such as routing and spanning tree protocols, could also be considered management traffic. For the purpose of this document, the word “management” is used for simplicity and may refer to some or all of the functions listed here.

Management Traffic includes, but is not limited to, system monitoring information such as:

- System or circuit alarms, both operational and security related
- Simple Network Management Protocol traps – alarms, gets, and writes
- SysLog information
- Log retrieval – polling or downloads – auditing or history logs
- SS7 signaling
- Configuration database replication between redundant devices or systems
- System administration/configuration/operation sessions performed by a qualified System Administrator, e.g., Management Information Base access
- Automated system operation/control sessions/information
- Routing information or updates
- Spanning Tree protocol and neighbor discovery

MANAGEMENT CONNECTION METHODS

Local management is defined as the management terminal, console, or workstation, etc., that is directly connected to the management port on the managed device.

Remote management occurs when any device management port or interface is extended beyond the cabling distance afforded by the direct connect method used (typically between 15 and 100 meters). This involves attaching the management port to a network and passing the management traffic across that network. Management ports may be connected directly to the LAN (if network enabled) or may be connected via an interface device. There are two types of remote management methods: In-band and Out-of-Band (OOB).

- In-band management is the process of providing device management connectivity via the normal production or user network carried by the device (e.g., the same network (or channel) used to provide user or customer services). A management workstation uses a remote terminal communications application to connect to the management software on the device via the production network connected to the device. In-band management could be implemented within an enclave/LAN or across an extended enterprise Intranet, or across a WAN such as the Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) of Internet.
- The OOB Management is the process of providing device management connectivity outside of the normal production or user network carried by the device (e.g., the same network (or channel) used to provide user or customer services). Describing OOB as a system or network having a management plane and a production or user plane. Architecturally, the management plane (i.e., the management traffic) is normally segregated from the production/user plane (i.e., general user traffic). No production or general user traffic traverses an OOB management plane. Devices should have dedicated management ports or interfaces and a direct local connection to the OOB plane. The OOB Management can be implemented within an enclave/LAN or across an extended enterprise Intranet, or across a WAN, such as the NIPRNet of Internet, using a number of methods.

APPENDIX A

ACRONYMS

3DES	Triple Data Encryption Standard
4W	4 Wire
5ESS	Class 5 Electronic Switching System
A/B	AB Switch
AAA	Authentication, Authorization, and Access
ACK	Acknowledge
ACL	Access Control List
ACS	Access Control Service
AD	Active Directory
ADAM	Active Directory Application Mode
ADM	Add/Drop Multiplexer
AES	Advanced Encryption Standard
AIS	Automated Information System
AO	Action Officer
APL	Approved Products List
ARP	Address Resolution Protocol
ARTS	Assured Real Time Services
AS	Assured Services
ASCLAN	Assured Service Converged Local Area Network
Ass	Autonomous system scanner
AS-SIP	Assured Services Session Initiation Protocol
ASLAN	Assured Services Local Area Network
ATO	Authority to Operate
B2BUA	Back-to-Back User Agent
BBP	Best Business Practices
BC	Border Controller
BIOS	Basic Input/Output System
BRI	Basic Rate Interface
C	Compliant
C2	Command and Control
CA	Certifying Authority
C&A	Certification and Accreditation
CAC	Common Access Card
CALEA	Commission on Accreditation of Law Enforcement Agencies
CAN	Converged Area Network
CAT	Category
CB	Channel Bank
CBC	Cipher Block Chaining
CCA	Call Connection Agent
CCB	Configuration Control Board

CCM	Configuration Control Manager
CD	Compact Disk
CDP	Computer Data Processing
CDR	Compact Disk Recordable
Cert	Certification
CIS	Center for Internet Security
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLI	Command Line Interface
CM	Communications Manager
CND	Computer Network Defense
COAS	Continuity Alternate Site
COBR	Continuity Backup Restoration
CODB	Continuity Data Backup
COEF	Continuity Identification of Essential Functions
COI	Community of Interest
COMS	Continuity Maintenance Support
COMSEC	Communication Security
CONUS	Continental United States
COPS	Continuity Power Supply
COSP	Continuity Spare Parts
COSW	Continuity Software
COTR	Continuity Trusted Recovery
COTS	Commercial-Off-the-Shelf
CPE	Customer Premise Equipment
CR	Conditional Requirement
CRADA	Cooperative Research and Development Agreement
CRD	Customer Requirements Document
CRL	Certificate Revocation List
CRM	Customer Relations Management
CTL	Certificate Trusted List
CTO	Communications Tasking Order
CVE	Common Vulnerabilities and Exposures
DAA	Data Access Arrangement
DAA	Designated Approving Authority
DB	Database
DBMS	Database Management System
DC	Domain Controller
DCAR	Design Configuration Procedural Review
DCAS	Design Configuration Acquisition Standards
DCBP	Design Configuration Best Practices
DCC	Data Communications Channel
DCCS	Design Configuration Configuration Specification
DCCT	Design Configuration Compliance Testing
DCDD	Design Configuration
DCDS	Design Configuration Security Documentation

DCFA	Design Configuration Functional Architecture
DCHW	Design Configuration Hardware
DCIT	Design Configuration Information Technology
DCMC	Design Configuration Mobile Code
DCNR	Design Configuration Non-Repudiation
DCPA	Design Configuration Partitioning Application
DCPD	Design Configuration Public Domain
DCPP-1	Design and Configuration Ports Protocols and Services
DCSD	Design Configuration Security Documentation
DCSQ	Design Configuration Software Quality
DCSR	Design Configuration Specific Robustness
DCSS	Design Configuration System State
DCSW	Design Configuration Software
DHCP	Dynamic Host Control Protocol
DES	Data Encryption Standard
DIACAP	DoD Information Assurance Certification and Accreditation Process
DiD	Defense in Depth
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoS	Denial of Service
DRSN	Defense RED Switch Network
DSA	Digital Signature Alogrithm
DSAWG	DISN Security Accreditation Working Group
DSCP	Differentiated Services Code Point
DSN	Defense Switched Network
DVX	Deployable Voice Exchange
DWDM	Dense Wavelength Division Multiplexing
E1	European Carrier 1
E2E	End to End
EAP	Extensible Authentication Protocol
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol – Tunneled Transport Layer Security
EBBD	Enclave Boundary Boundary Defense
EBC	Edge Border Controller
EBCR	Enclave Boundary Connection Rules
EBRP	Enclave Boundary Remote Privileged
EBRU	Enclave Boundary Remote User

EBVC	Enclave Boundary Virtual Local Area Network (VLAN) Controls
ECAD	Enclave Computing Affiliation Display
ECAN	Enclave Computing Access Need-To-Know
ECAR	Enclave Computing Audit Record
ECAT	Enclave Computing Audit Trail
ECCD	Enclave Computing Changes to Data
ECCR	Enclave Computing Confidentiality at Rest
ECCT	Enclave Computing Confidentiality at in Transit
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIC	Enclave Computing Interconnections
ECID	Enclave Computing Intrusion Detection
ECLO	Enclave Computing Logon
ECLP	Enclave Computing Least Privilege
ECML	Enclave Computing Marketing and Labeling
ECMT-1	Enclave and Computing Monitoring and Testing
ECND	Enclave Computing Network Device
ECPA	Enclave Computing Privileged Account
ECRC	Enclave Computing Resource Control
ECRG	Enclave Computing Report Generation
ECSC	Enclave Computing Security Compliance
ECTC	Enclave Computing Tempest Controls
ECTM-2	Enclave and Computing Environment Transmission Integrity Controls
ECTP	Enclave Computing Trail Protection
ECVI-1	Enclave and Computing Environment Voice over IP
ECWM	Enclave Computing Warning Message
EI	End Instrument
EMSS	Enhanced Mobile Satellite Services
EO	End Office
ERP	Enterprise Resource Planning
ESA	Enterprise Systems Architecture
ESM	Enterprise System Management
ETSI	European Telecommunications Standards Institute
EWSD	Elektronisches Wählsystem Digital
FCAPS	Fault, Configuration, Administration, Performance, and Security Monitoring
FIN	Finish
FIPS Pubs	Federal Information Processing Standards Publications
FISMA	Federal Information Security Management Act
FOS	Fixed On Site
FSO	Field Security Office
FTP	File Transfer Protocol
FY	Fiscal Year
GAO	Government Accountability Office
GB	Gigabyte
GIG	Global Information Grid

GNO	Global Network Operations
GNU	GNU's Not UNIX
GOTS	Government off the Shelf
Gpg	GNU Privacy Guard
GR	Generic Requirement
GSS	Generic System Specification
GSTP	Generic System Test Plan
GTK	Gimp Tool Kit (program)
GUI	Graphical User Interface
HKLM	Hkey Local Machine
HMAC	Hashed Message Authentication Code
HP-UX	Hewlett Packard UNIX
HSRP	Hot Standby Router Protocol
HTM	Hyper Text Markup
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
HW	Hardware
IA	Information Assurance
IAAC	Enclave Computing Account Control
IAGA	Identification Authentication Group Authentication
IAIA	Individual Identification and Authentication
IAKM	Identification Authentication Key Management
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAS	Internet Authentication Server
IASE	Information Assurance Support Environment
IATF	Information Assurance Task Force
IATO	Interim Authority to Operate
IATP	IA Test Plan
IATS	Identification Authentication Token Standards
IATT	IA Test Team
IAVA	IA Vulnerability Alerts
IAW	In Accordance With
IAW	In Accordance With
IBM	International Business Machines
ICD	Initial Capabilities Document
ICM	Initial Contact Meeting
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IE	Internet Explorer
IG	Inspector General
IGMP	Internet Group Management Protocol

IGRP	Internet Gateway Routing Protocol
IIS	Internet Information System
IKE	Internet Key Exchange
INFOSEC	Information Systems Management and Information Security
IO	Interoperability
IP	Internet Protocol
IPSec	Internet Protocol Security
IPT	IP Telephony
IPV	IP Vulnerability
IPv6	Internet Protocol version 6
IRDP	ICMP Router Discovery Protocol
IS	Information System
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Information Support Plan
ISS	IS Security
ISSM	IS Security Manager
ISSO	IS Security Officer
IST	Inter-Switch Trunk
IT	Information Technology
IWF	Interworking Function
J2EE	Java TM 2 Platform Enterprise Edition
JIC	Joint Intelligence Center
JIDS	Joint Information Defense System
JITC	Joint Interoperability Test Command
JTA	Joint Technical Architecture
JTF	Joint Test Facility
KIP	Key Interface Profile
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LS	Local Switch
LSC	Local Session Controller
M	Meter
MA	Mission Area
MAC	Media Access Controller
MAC	Mission Assurance Category
MCU	Multipoint Controller Unit
MD5	Message Digest 5
MEGACO	Gateway Control Protocol
MFS	Multifunction Switch
MFSS	Multifunction Soft Switch

MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Message Information Block
MILDEP	Military Department
MMC	Microsoft Management Console
MR	Manual Review
MS	Management System
MS	Microsoft
MsgIDs	Message Identifications
MSL	Meridian Switching Load
MUF	Military Unique Features
NA	Not Applicable
NAPT	Network Address Port Translation
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NC	Non-Compliant
NE/NS	Network Element/Network Switch
NetOps	Network Operations
NF	Not a Finding
NTFS	New Technology File System
NGCS	NATO General Purpose Segment Communication System
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIPRNet	Unclassified-But-Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
Nmap	Network Mapping
NMS	Network Management System
NOC	Network Operation Center
NR	Not Reviewable
NSA	National Security Agency
NT	New Technology
Num.	Number
OAM&P	Operations Administration Maintenance and Planning
OCONUS	Outside Continental United States
OOB	Out-of-Band
OS	Operating System
OSC	On-Line Status Check
OSCR	On-Line Status Check Router
OSSTM	Open Source Security Testing Methodology Manual
OVAL	Open Vulnerablity Assessment Language
P	Provider
PA	Protocol Analysis

PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PC	Personal Computer
PCCC	Personal Computer Communications Client
PDF	Portable Document Format
PDI	Potential Discrepancy Indicator
PDU	Protocol Data Unit
PEAP	Protected Extensible Authentication Protocol
PEEL	Physical Environmental Emergency Lighting
PEFD	Physical Environmental Fire Detection
PEFI	Physical Environmental Fire Inspection
PEFS	Physical Environmental Fire Suppression
PEHC	Physical Environmental Humidity Controls
PEMS	Physical Environmental Master Switch
PETC	Physical Environmental Temperature Controls
PETN	Physical Environmental Training
PEVR	Physical Environmental Voltage Regulator
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKCS #7	Public Key Cryptography Standard #7
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PMO	Personnel Management Officer
POA&M	Plan of Action and Milestone
PPS	Ports and Protocol Security
PROTOS	Protocol Security Test Suite
PRRB	Personnel Rules Responsible Behavior
PSTN	Public Switch Telephone Network
Pubs	Publications
R	Release
R	Router
RADIUS	Remote Authentication Dial In User Service
RAE	Required Ancillary Equipment
RAS	Remote Access Service
Ref	Reference
Req	Request
RFC	Request For Comment
RIP	Routing Information Protocol
Rq	Request
RSA	Rivest, Shamir, and Aldeman
RST	Reset
RSU	Remote Switching Unit
RTS	Real Time Services

SA	System Administrator
SAM	Security Accounts Manager
SAR	Self-Assessment Report
SBU	Sensitive But Unclassified
SCCP	Simple Client Control Protocol
SCS	Session Control and Signaling
SCTP	Stream Control Transmission Protocol
SDES	Session Descriptions
SDID	Secure Digital ID
SDN	Secure Data Network
SDP	Session Description Protocol
SE	Security Engineer
SE	Succession Enterprise
SFTP	Secure File Transport Protocol
SHA	Secure Hash Algorithm
SHA1	Secure Hash Algorithm Version 1.0
SIP	Session Initiation Protocol
SIP	System Identification Profile
SiVus	SIP Vulnerability Scanner
SM	Security Manager
SMB	Server Message Block
SMEO	Small End Office
SMU	Switch Multiplexer Unit
SNMP	Simple Network Messaging Protocol
SNMPv3	Simple Network Management Protocol Version 3
SONET	Synchronous Optical Networking
SP	Service Pack
SP	Special Publication
SPAN	Sharing Peripherals Across the Network
SPoA	Service Point of Attachment
SQL	Structured Query Language
SRR	Security Readiness Review
SRRDB	Security Readiness Review Data Base
SRTP	Secure Real-time Transport Protocol
SS	Soft Switch
SS7	Signaling System 7
SSH	Secure Shell
SSL	Secure Socket Layer
SSLv3	Secure Socket Layer 3
SSM	Single Systems Manager
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guidelines
STP	Signal Transfer Points
SUT	System Under Test
SW	Software
SYN	Synchronize

T1	Telecommunications Carrier 1
TACACS+	Terminal Access Controller Access Control System Plus
TAG	Technical Advisory Group
TBD	To Be Determined
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TDM	Time Division Multiplexer/Multiplexing
TFTP	Trivial File Transfer Protocol
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks
TLS	Transport Layer Security
TpoA	Transport Point of Attachment
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
TS	Technical Standard
TTLS	Tunneled Transport Layer Security
UA	User Agent
UC	Unified Capabilities
UCCO	Unified Capabilities Connection Office
UCR	Unified Capabilities Requirements
UDP	Universal Datagram Protocol
URL	Universal Resource Locator
USB	Universal Serial Bus
V	Version
VB	Visual Basic
VIIR	Vulnerability Incident and Incident Response
VIVM-1	Vulnerability and Incident Management Vulnerability Management
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMPS	VLAN Management Policy Server
VMS	Vulnerability Management System
VoIP	Voice over IP
VVoIP	Video and Voice over IP
VoSIP	Voice over Session Initiation Protocol
VPN	Virtual Private Network
VSE	Voice Services Equipment
VTC	Video Teleconferencing
W/O-RAE	Without Required Ancillary Equipment
WAN	Wide Area Network
Win	Windows
Win2k	Windows 2000
Win2k3	Windows 2003
WLAN	Wireless Local Area Network

W-RAE	With Required Ancillary Equipment
XML	Extensible Markup Language
XP	Experience
XSLT	Extensible Stylesheet Language Transformations

(The page intentionally left blank)

APPENDIX B

RESOURCES AND TOOLS

B-1 IA RESOURCES. This appendix lists the resources needed for assessing the Information Assurance (IA) security posture of an Information System (IS): Security Technical Implementation Guidelines (STIG), Gold Disks, Security Readiness Review (SRR) scripts by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Operating System Security Guides, NSA Router and Switch Guides, and Microsoft Security Guides for Microsoft-based software. Department of Defense (DoD) IA security baselines are established by the requirements in DoD Directive (DoDD) 8500.1 and DoD Instruction (DoDI) 8500.2. In addition, IA security standards testing is designed to focus on the proper protection of the system under test. Many different methods and tools can successfully assess a system for vulnerability; are not limited to the above list nor is this appendix all inclusive.

B-1.1 Security Technical Implementation Guidelines (STIG). The DoD uses STIG to strengthen and assess the security posture of a system or component. Findings resulting from running the Gold Disks and scripts are indications of weaknesses (or "holes") in the security posture of the system or component. Findings from the STIG are grouped into three Categories (CAT) based on the severity of the weakness. **CAT I** findings are those that allow an attacker to gain immediate access to a system or component, allow elevating a user's rights to administrator (or super user) level, or allow bypassing a firewall. These are the most severe findings. Systems or components having multiple CAT I findings may not be accepted for additional testing or for placement on the Defense Switched Network (DSN) Approved Products List (APL). **CAT II** findings are those that provide information about the system or component and therefore have a high potential of allowing unauthorized access to an intruder (the more that is known about a computer or system, the easier it is to find the weaknesses in the hardware, firmware, or software.) **CAT III** findings are those that give away enough information for an intruder to compromise the system or component. High numbers of CAT II and III findings may indicate an overall weakness in the security posture of the system or component and may preclude placement on the DSN APL. Table B-1 provides the description for each STIG.

Table B-1. STIG Listing

STIG	Description
Access Control STIG	Access Control STIG details a security framework for use when planning and selecting access control for protecting sensitive and classified information in the DoD. It provides a consolidated starting place for the security planning team responsible for ensuring compliance with DoD policies. This STIG presents a practical methodology for selecting and integrating logical and physical authentication techniques while tying the solution to the asset's value, environment, threat conditions, and operational constraints. For classified access, the solution must protect access to sensitive or classified systems and data while considering the need for appropriate and authorized access in uncontrolled areas for DoD personnel, contractors, and coalition forces.
Active Directory	AD Security Checklist provides the procedures for conducting a SRR to determine compliance with the requirements in the AD STIG. This Checklist document must be used together with the corresponding version of the STIG document. As in the related STIG, this Checklist addresses three review subjects: 1. Active Directory Implementation - This subject covers checks for AD Domain Controllers, AD Domains, and the AD Forest that make up an implementation of Active Directory. 2. Synchronization/Maintenance Application - This subject covers checks for an individual installation of an application used to perform synchronization or maintenance on one or more AD implementations. 3. ADAM - This subject covers checks for an individual installation of ADAM as a directory service.
Application Security Checklist	Application Security Checklist is used for custom developed software, either COTS or Government Off The Shelf, and the programming code used for the application that resides on top of an OS. The checklist covers all aspects of the application, including identification, authentication, interaction with ActiveX, Java, e-mail clients, web browsers, session logging, auditing, and enclave impact.
Application Services STIG/Checklist	Application Services STIG provides security configuration and implementation guidance for application server products designed to comply with the J2EE™. The J2EE defines a standard security framework of configuration and implementation for the protection of application servers.
Backbone Transport Services STIG	Backbone Transport Services STIG provides IA guidance and addresses security issues relating to the Global Information Grid backbone network. Guidance in this STIG is provided for all transport components, their relationships, interoperability, and principles used for governing their configuration, implementation, management, and operation.
Biometrics STIG	Biometrics is used to enhance security; however, there are security risks associated with it, which must be mitigated. The Biometrics STIG provides guidelines for implementing technological systems, such as biometrics.
Collaboration Infrastructure STIG	Collaboration Infrastructure STIG provides secure, available, and reliable data to enhance the confidentiality, integrity, or availability of sensitive DoD Automated Information Systems. This document will assist sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure environments.
Database STIG	Database STIG provides the technical security policies, requirements, and implementation details for applying security concepts to database servers. It generally covers all database servers and specifically Oracle, Microsoft Structured Query Language SQL Server, and DB 2 database servers supporting data storage and retrieval from local, intranet, or Internet clients.

Table B-1. STIG Listing (continued)

STIG	Description
DSN STIG	DSN STIG provides the technical security policies, implementation details, and requirements for applying security concepts to the DoD telecommunications systems. The DSN encompasses inter-base and intra-base non-secure and/or secure C2 telecommunications systems that provide end-to-end common use and dedicated telephone service, voice-band data, and dial-up Video Teleconferencing for authorized DoD C2 and non-C2 users. Non-secure dial-up voice (telephone) service is the system's principal requirement. The span or scope of the DSN covers the CONUS and a large portion of the world outside of the CONUS.
Desktop Application STIG	Desktop Application STIG provides the technical security policies, requirements, and implementation details for applying security concepts to COTS applications on desktop workstations. This STIG also applies to the lock-down procedures for Exchange Servers.
DRSN STIG	DRSN STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the DRSN. This STIG is directive in nature and applies to all DoD components and government agencies, including their contractors that are served by the DRSN, or whose RED (secure) switch interconnects with the DRSN.
DNS STIG	DNS STIG is designed to assist administrators with configuration DNS server software and related portions of the underlying operating system. This STIG also provides guidance for standard operating procedures related to configuration management, business continuity, and other topics.
Enclave STIG	Enclave STIG security provides the guidance necessary for information protection to implement secure IS and networks while ensuring interoperability. This STIG includes security considerations at the network level needed to provide an acceptable level of risk for information transmitted throughout an enclave.
ERP STIG	ERP STIG provides the technical security policies, requirements, and implementation details for COTS ERP application software. For this STIG, ERP software will refer to all commercially available software packages that supply one or more of the functions generally found within ERP packages. The functions include but are not limited to Human Resources, Financial processes, Customer Relations Management, sales, warehousing, inventory control, and manufacturing.
ESM STIG	ESM STIG provides security configuration guidance for software products designed to deliver enterprise-class system management functions. While the boundaries of the ESM discipline are such that there is no authoritative definition of an ESM product, Section 2, Enterprise System Management Overview, provides a generic description of the elements characteristic of most ESM products. Section 3, Enterprise System Management Security, provides general guidance for ESM products. Specific commercial products are addressed in appendices.
Keyboard, Video, and Mouse (KVM) Switch Checklist	Keyboard, Video, and Mouse (KVM) switches are used to connect a single keyboard, video monitor, and mouse to multiple IS, saving space and equipment. They are commonly found in testing laboratories, in server rooms, and with the advent of small inexpensive switches, on desktops to reduce clutter. A/B switches are used by a single peripheral between multiple ISs or multiple peripheral devices on a single interface. Switch (es) will refer to both KVM and A/B switches unless otherwise Noted.
Macintosh STIG	Macintosh STIG provides the technical security policies and a requirement for deploying a secure IS running Macintosh OS X in a DoD Network environment.

Table B-1. STIG Listing (continued)

STIG	Description
Network STIG	Network STIG has been developed to enhance the confidentiality, integrity, and availability of sensitive DoD Automated AIS. Each site network/communications infrastructure must provide secure, available, and reliable data for all customers. This document is designed to supplement the security guidance provided by DoD-specific requirements and will assist sites in meeting the minimum requirements, standards, controls, and options required for secure network operations. The intent of this STIG is to include security considerations at the network level needed to provide an acceptable level of risk for information transmitted throughout an enclave.
OS/390 MVS Logical Partition STIG	OS/390 MVS Logical Partition STIG defines the technical criteria necessary to implement MAC II Sensitive functionality within DISA non-classified multiple partitions and classified partitions. This document does not define policy, but it documents the procedures and parameters necessary to implement policy.
OS/390 STIG	OS/390 STIG for most mainframe IAs deployed throughout DoD use the IBM OS/390 or z/OS operating system. Controls within OS/390 and z/OS have been developed and documented in IBM references to ensure operating system integrity is maintained. This document is in the process of transitioning from OS/390 to z/OS. Any and all references to OS/390 will apply to both OS/390 and z/OS.
SPAN STIG	Sharing Peripherals Across the Network STIG provides the technical security policies, requirements, and implementation details for applying security concepts to COTS hardware peripheral devices. For this STIG, peripheral will mean, “any device that allows communication between a system and itself, but is not directly operated by the system.” However, this document does not deal with devices found wholly within the main cabinet of the computer or, with the exception of A/B switches, those devices connected via legacy parallel and serial interfaces.
Secure Remote Computing STIG	Secure Remote Computing STIG provides the technical security policies and requirements for providing a secure remote access environment to users in DoD components. This document discusses both the remote user environment and the network site architecture that supports the remote user. Since information can be stored, processed, or transmitted from a number of locations, IAs Systems Management and Information Security must encompass the total environment.
Tandem STIG	Tandem STIG includes security considerations needed to provide an acceptable level of risk for the information that resides on the Tandem systems. The requirements set forth in this document will assist in securing the Tandem NonStop Kernel OS for each site. The Tandem OS includes the Tandem NonStop SQL DB Management System (MS) and the Tandem file MS Enscribe.
Unisys STIG	Unisys STIG will define the minimum requirements, standards, controls, options, and procedures that have to be in place for the Unisys Executive and standard system software to meet MAC II sensitive compliance as described in the DoDI 8500.2. Individual sites may implement additional security measures as deemed necessary.
UNIX STIG	Security requirements contained within this STIG are applicable to all DoD-administered systems and all systems connected to DoD networks. This document provides requirements and associated steps to limit the security vulnerabilities for a UNIX system. These requirements are designed to assist Security Manager, Information Assurance Manager, Information Assurance Officer, and SA with configuring and maintaining security controls in a UNIX environment. DoD customers use several different UNIX platforms that support different versions of UNIX. All UNIX systems share some common characteristics, but they may implement features differently. This document provides security requirements for all common variants of UNIX.

Table B-1. STIG Listing (continued)

STIG	Description
VM/ESA STIG	VM/ESA is a multi-access, interactive operating system used in conjunction with the S/390 architecture. VM provides a platform not only for hosting the traditional guest operating systems such as Voice Services Equipment and OS/390, but also for dependent guests such as Multi-User Micro Electrical Machine System Processing System/VM and Advanced IBM UNIX and ESA.
VoIP STIG	VoIP STIG is published as a tool to assist in securing networks and systems supporting VoIP technology in converging voice and data networks. When applied to DoD networks and systems, this document must be used in conjunction with the DSN STIG, as it contains specific requirements for DoD telecommunications systems and systems connected to the DSN. Additionally, this STIG must be used in conjunction with other STIGs relating to OSs, databases, Web servers, network infrastructure, enclaves, etc., as appropriate. The VoIP STIG will be superseded by the RTS STIG when it is published.
Web STIG	Web Server STIG targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interrupted operations. Additionally, the STIG ensures the site has properly installed and implemented the database environment and that it is being managed in a way that is secure, efficient, and effective. Items on the Web STIG for Internet Information Server are now covered in the DISA Gold Disk V2 and findings will be reported in the relevant Windows portion of this report.
Windows 2000/XP/2003 Addendum	This Addendum to Microsoft's Windows 2003 Security Guide and National Security Agency's Guides to Securing Windows 2000 and XP was developed to enhance the confidentiality, integrity, and availability of sensitive DoD Automated Information System using the Windows 2003, 2000, and XP OSs. These security settings include those that can be set via the Security Configuration Manager, through Group Policy, as well as manual settings.
Wireless Draft Secure RAS STIG	Wireless Draft Secure RAS is an important capability for remote users. It provides the ability to connect to a network from any location with a valid Internet connection. This addendum provides a technical overview of a general DoD remote access architecture, guidance for secure remote computing, and an evaluation of the risks that wireless connections present, and it gives best practices to follow to ensure proper security for these connections. This addendum also discusses the functionality of the security components. DoD entities using this framework should be able to select the solution that best fits the requirements of their environment and successfully implement a secure network.
Wireless STIG	Wireless STIG is published as a tool to assist in improving the security of DoD commercial wireless IAs. The document is meant to be used in conjunction with the Network STIG and appropriate operating system STIGs.
Wireless LAN Security Framework Addendum	Wireless LAN document provides a conceptual framework for implementing WLANs securely. To this end, the document provides details concerning WLAN technologies and solutions that enable a secure connection to the Unclassified but Sensitive Internet Protocol Router Network.
Wireless Mobile Computing Addendum	Wireless Mobile Computing addendum provides a technical overview for properly securing the various types of mobile wireless devices currently available to users connecting to the DoD enclave. The mobile device is considered a critical component within the WLAN and is often overlooked as a network component extension. This extension consists primarily of mobile devices (e.g., cellular devices, Personal Digital Assistants, laptops, and tablet Personal Computers). A critical risk associated with the device lies in the user authentication to the device. Although most mobile devices do ship with some form of user-authentication capability, these mechanisms are usually weak and easily exploitable and should not be relied on to provide optimal levels of security.

Table B-1. STIG Listing (continued)

STIG	Description
Wireless LAN Site Survey Addendum	WLAN Site Survey Addendum to the Wireless STIG is published as a tool to assist in the effective deployment of WLANs within the DoD. This addendum is meant to be used in conjunction with the Wireless STIG. The information in this addendum is to supplement and enhance the security requirements found in the Wireless STIG by providing more details in conducting a basic site survey for deploying WLAN equipment.

LEGEND:

A/B	AB Switch	IS	Information System
AD	Active Directory	J2EE	Java™ 2 Platform Enterprise Edition
ADAM	Active Directory Application Mode	KVM	Keyboard, Video, and Mouse
AIS	Automatic Information System	LAN	Local Area Network
C2	Command and Control	MAC	Mission Assurance Category
CONUS	Continental United States	MS	Management System
COTS	Commercial Off the Shelf	MVS	Multiple Video Systems
DB	Database	OS	Operating System
DISA	Defense Information Systems Agency	RAS	Remote Access Service
DNS	Domain Name Server	RTS	Real Time Services
DoD	Department of Defense	SA	System Administrator
DoDI	Department of Defense Instruction	SPAN	Sharing Peripherals Across the Network
DRSN	Defense Switch Red Network	SQL	Structured Query Language
DSN	Defense Switched Network	SRR	Security Readiness Review/Database
ERP	Enterprise Resource Planning	STIG	Security Technical Implementation Guidelines
ESA	Enterprise Systems Architecture	VM	Virtual Machine
ESM	Enterprise System Management	VoIP	Voice over Internet Protocol
IA	Information Assurance	XP	Experience
IBM	International Business Machines	WLAN	Wireless Local Area Network

B-1.2 Gold Disk. Findings that result from running the Gold Disk and other scripts are indications of weaknesses (or "holes") in the security posture of the system or component.

Figure B-1 depicts the current version and release date for each STIG available at <http://iase.disa.mil/stigs/stig/index.html>. Figure B-1 is a screenshot from DISA's Information Assurance Support Environment (IASE) website.

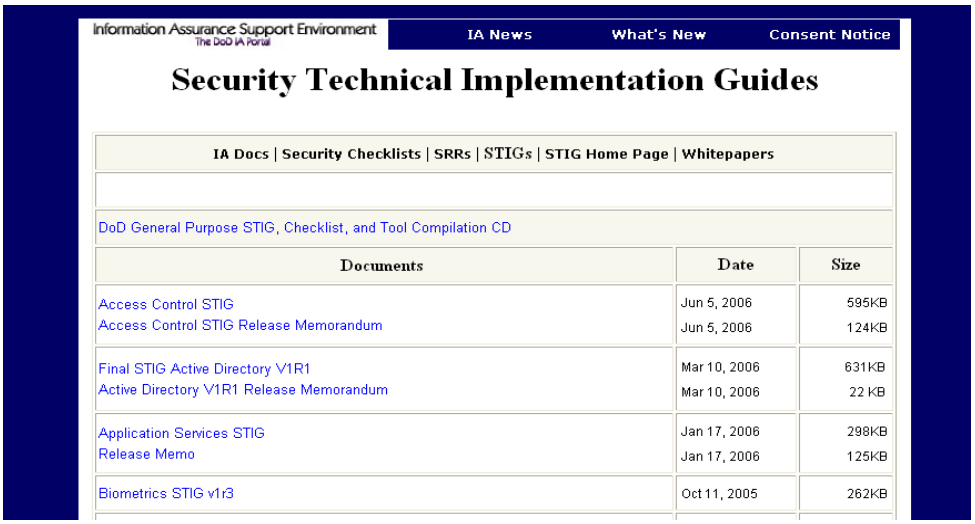


Figure B-1. IASE Website

B-1.3 Security Readiness Review Scripts/Gold Disk. The DISA Field Security Office (FSO) develops the Gold Disks and SRR to assist System Administrators (SA) in securing systems and applications in accordance with the DISA STIG, Checklists, and applicable Center for Internet Security benchmarks. This functionality was developed to meet the needs of the system auditors and SA in accessing the security posture of the respective IS. The SA, Gold Disks, and SRR encompass the ability to detect installed products, identify and remediate applicable vulnerabilities, and generate a file that is used for asset registration within the vulnerability management system, which enables the IA Test Team to generate a findings report.

B-1.4 NSA Operating System Security Guides/NSA Router and Switch Guides. The NSA has written information guides to enhance the posture of both commercial and open source software. These guides cover different versions of software for workstations, switches, and routers. The objective of the NSA research program is to develop technological advances and share that information with the software development community through a variety of transfer mechanisms. Figure B-2 shows the documents available at <http://www.nsa.gov/snac/downloads_all.cfm?MenuID=scg10.3.1>.

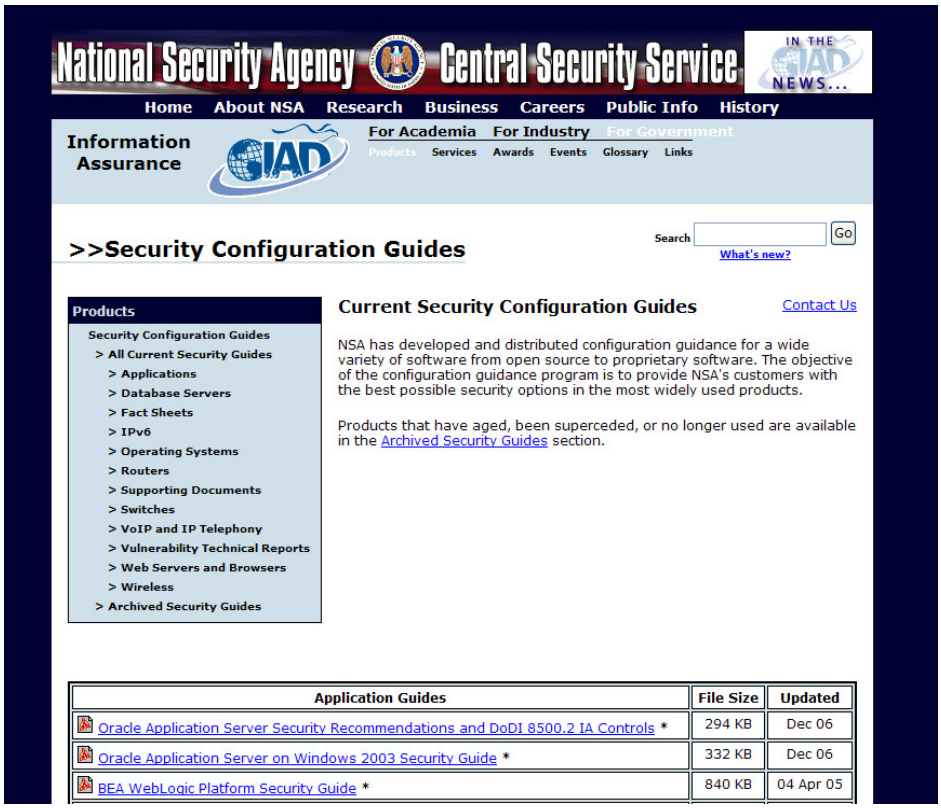


Figure B-2. NSA Website

B-1.5 Microsoft Security Guides. These guides apply only to systems that use Microsoft products. Microsoft engineering teams, consultants, support engineers, customers, and partners review and approve Microsoft Security guides. Microsoft worked with consultants and systems engineers when it implemented Windows Server 2003, Windows XP, and Windows 2000 in a variety of environments to establish the latest choice practices to secure these servers and clients. The detailed information guides are available at the following website: <http://www.microsoft.com/technet/security/guidance/default.mspx>

B-1.6 National Information Assurance Partnership (NIAP). The NIAP is a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers and is operated by the NSA. The long-term goal of NIAP is to help increase the level of trust consumers have in their IS and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, NIAP seeks to:

- Promote the development and use of evaluated IT products and systems
- Champion the development and use of national and international standards for IT security
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics
- Support a framework for international recognition and acceptance of IT security testing and evaluation results
- Facilitate the development and growth of a commercial security testing industry within the United States
- Information is available at the following website: <http://niap-ccevs.org/>

B-1.7 DoDD 8500.1 and DoDI 8500.2. The DoDD 8500.1 and DoDI 8500.2 establish policy and assign responsibilities to achieve IA objectives through a defense-in-depth approach integrating the capabilities of personnel, operations, and technology, and the DoDD support the evolution to network-centric warfare. The responsibility of the DoD is crucial to protect and defend information and support IT. The DoD information is shared across a Global Information Grid (GIG) that is inherently vulnerable to exploitation and denial of service. The following are contributing factors to vulnerabilities within the GIG:

- Increased reliance on commercial information technology and services
- Increased complexity and risk propagation through interconnection
- Extremely rapid pace of technological change
- Distributed and non-standard management structure
- Relatively low cost of entry for adversaries

DoDI 8500.2, Enclosure 3, establishes fundamental IA requirements for DoD IS in the form of two sets of graded baseline IA Controls. The baseline sets of IA Controls are pre-defined based on the determination of the Mission Assurance Category (MAC) and Confidentiality Levels.

B-2 CONFIDENTIALITY LEVELS. The IA Controls that address availability and integrity requirements are tied to the system's MAC based on the importance of the information to the mission, particularly the warfighters' combat mission. Basing the IA Controls addressing confidentiality requirements on the sensitivity or classification of the information ensures a good security posture. The set of IA Controls applicable to any given DoD information system is always a combination of the IA Controls for its MAC and the IA Controls for its Confidentiality Level.

Applying the specified set of IA Controls to achieve baseline IA levels in a comprehensive IA program includes acquisition, proper security engineering, connection management, and IA administration. An IA Control describes an objective IA condition achieved through the application of specific safeguards or through the regulation of specific activities. The objective condition is testable, compliance is measurable, and the activities required to achieve the IA Control are assignable and thus accountable. Table B-2 shows the IA Control subject areas.

Table B-2. IA Control Subject Areas

Abbreviation	Subject Area Name
DC	Security Design and Configuration
IA	Identification and Authentication
EC	Enclave and Computing Environment
EB	Enclave Boundary Defense
PE	Physical and Environmental
PR	Personnel
CO	Continuity
VI	Vulnerability and Incident Management

LEGEND:

CO	Continuity of Operations	IA	Identification and Authentication
DC	Domain Controller	PE	Physical and Environmental
EB	Enclave Boundary	PR	Personnel
EC	Enclave and Computing	VI	Vulnerability and Incident

An IA Control comprises the following:

- Control Subject Area: One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned
- Control Name: A brief title phrase that describes the individual IA Control
- Control Text: One or more sentences that describe the IA condition or state that the IA Control is intended to achieve
- Control Number: A unique identifier comprised of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control Name

The Joint Interoperability Test Command (JITC) tests only four of the eight IA Control Subject areas. This is due to the limitations of the laboratory environment of JITC's testing facilities; the rest of the requirements are site specific. The JITC will

address DCxx-x, ECxx-x, IAxx-x, and EBxx-x and will partially assess COxx-x and VIxx-x.

B-3 DoD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) SCORECARD. This is a summary report that shows the certified or accredited implementation status of a DoD IS assigned IA Controls and supports or conveys a certification determination and/or accreditation decision (see Appendix C, Test Preparation Documents). The intent of the DIACAP Scorecard is to convey information about the IA posture of a DoD IS in a electronic format that managers understand. As part of the certification decision and after the tester validates the individual IA Controls as compliant, non-compliant, or not applicable, a residual risk analysis (an analysis that determines risk due to partial or unsatisfactory implementation of assigned IA Controls) should be conducted. To determine the likelihood of a future adverse event, testers must analyze the threats to a system in conjunction with potential vulnerabilities. Their analysis must include the IA Controls that are in place for the system and the urgency of completing corrective action. Two indicator codes aid in this analysis: impact codes and severity codes.

The DoD assigns impact codes to IA Controls, and they are maintained through the DIACAP Configuration Control Manager. The impact code for the IA Control is the Technical Advisory Group's assessment of the magnitude of network-wide consequences for a failed IA Control. Within an IA Control Set, the impact code indicates each IA Control's relative contribution to the target IA posture, and it is expressed as high, medium, or low. A high impact code is an indicator of greatest impact. Impact Codes are listed on the IA Controls detail pages and accessed from within the IA Controls section.

The CA assigns severity codes to specific findings and deficiencies identified during certification. Severity codes are used to assess of the likelihood of system-wide IA exploitations. The CA assigns the severity code to a weakness as part of the certification analysis to indicate risk and urgency for corrective action. The severity codes are expressed as CAT I, CAT II, and CAT III. The CAT I code is an indicator of greatest risk and urgency.

The certification determination is based on the validation of actual results and an associated risk analysis. It considers impact codes associated with IA Controls in a non-compliant status, associated severity codes, expected exposure time (i.e., the projected life of the system release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars and functionality reductions). Certification aids in the development of a Plan of Action and Milestones (POA&M) and characterizes residual risk.

The JITC scorecard gives organizations the ability to extract test data into the scorecard of their choosing. The scorecard covers the following seven items needed to track IA Controls: IA Control Subject Area, IA Control Number, IA Control Name,

Compliant/Non-Compliant, Impact Code, Responsible Entity, and Findings Results Definitions:

- **IA Control Subject Area:** One of eight groups indicating the major subject or focus area to which an individual IA Control is assigned.
- **IA Control Number:** A unique identifier composed of four letters, a dash, and a number. The first two letters are an abbreviation for the subject area name and the second two letters are an abbreviation for the individual IA Control Name. The number represents a level of robustness in ascending order that is relative to each IA Control.
- **IA Control Name:** A brief title phrase that describes the individual IA Control.
- **Compliant/Non-Compliant:**
    - **Compliant:** A satisfactory verification of previously agreed to security requirements based on the STIG Checklists.
    - **Non-Compliant:** Failure to meet the recommended security requirements found in the STIG Checklists will result in a Non-Compliant status. Non-Compliant IA Controls will list the checks that require the site to draft a POA&M that describes the corrective actions that will bring their system to a secure state. The findings will show in a dropdown tab (+) on the left of the screen.
- **Impact Code:** Primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system.
- **Responsible Entity:** Used to aid in setting the limits and boundaries identified in testing in a lab environment versus deploying the system to the sponsor's site.
- **Findings Results Definitions:** Below are explanations of terms from the IA STIG and used the scorecard.
    - **Open:** As applied to the scorecard, an "OPEN" classification in the status column indicates this is a finding for that particular check for that STIG.
    - **Closed:** As applied to the scorecard, a "CLOSED" classification in the status column indicates it may have been originally given an "OPEN" classification in the status, but has now been closed.
    - **Fixed On Site (FOS):** As applied to the scorecard, a "FOS" classification in the status column indicates that the vendor was able or had the ability to fix or change their system in the JITC lab, to meet the requirement as directed by the STIG.
    - **Not Applicable (NA):** As applied to the scorecard, a "NA" classification in the status column indicates that the requirement given by the STIG check was not relevant to the equipment under test.
    - **Not a Finding (NF):** As applied to the scorecard, a "NF" classification in the status column indicates that as the STIG check is applied to the system, the check is not found to be a finding against the system.
    - **Not Reviewable (NR):** As applied to the scorecard, a "NR" classification in the status column indicates the tester cannot view the check in the STIG (e.g. VxWorks, an Operating System (OS), is oftentimes embedded

with a solution that the tester cannot access without a decompiler and a vendor test bench to view).

- **Required Ancillary Equipment (RAE):** As applied to the scorecard, "RAE" classifications in the status column indicates equipment that has been identified as conditions of fielding when the system is deployed into an operational environment**.** "RAE" is then used in place of an "OPEN" classification in the status column.
- **To Be Determined (TBD):** As applied to the scorecard, a "TBD" classification in the status column indicates extra information needed before the status can be changed in the scorecard.

Within the delivered scorecard, the following instruction explains how to obtain the corresponding data addressed in the respective acquiring organization's IA Assessment Report.

On the upper-left-hand side of the DIACAP Scorecard, two buttons act as toggle switches that will display or hide information depending on which button is selected. If "1" is selected, it will show only the IA Controls. If "2" is selected, it will show the IA Controls and associated STIG Potential Discrepancy Indicator Requirement Findings, as shown in Figure B-3.

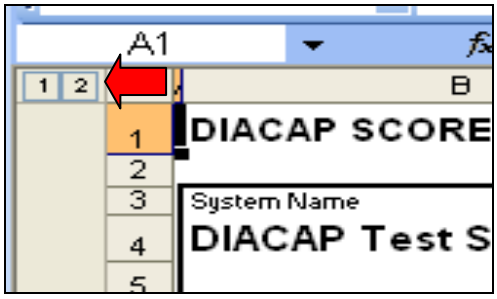


Figure B-3. Toggle Buttons

The scorecard is designed to pull findings from the checklists, associate them to the appropriate IA Controls, and provide access to additional information in the finding notes.

Table B-3 addresses further IA Controls and the portions that are the sites' responsibility for fielding the equipment.

Table B-3. IA Control Details

Subject Area	Control Num.	IA Control Name	C/NC	Impact Code	Last Update
Continuity	COAS-2	Alternate Site Designation		Medium	
Continuity	COBR-1	Protection of Backup and Restoration Assets		High	
Continuity	CODB-3	Data Backup Procedures		Low	
Continuity	CODP-3	Disaster and Recovery Planning		Low	
Continuity	COEB-2	Enclave Boundary Defense		Medium	
Continuity	COED-2	Scheduled Exercises and Drills		Low	
Continuity	COEF-2	Identification of Essential Functions		Low	
Continuity	COMS-2	Maintenance Support		Low	
Continuity	COPS-3	Power Supply		Medium	
Continuity	COSP-2	Spares and Parts		Low	
Continuity	COSW-1	Backup Copies of Critical Software		High	
Continuity	COTR-1	Trusted Recovery		High	
Security Design and Configuration	DCAR-1	Procedural Review		Medium	
Security Design and Configuration	DCAS-1	Acquisition Standards		High	
Security Design and Configuration	DCBP-1	Best Security Practices		Medium	
Security Design and Configuration	DCCB-2	Control Board		Low	
Security Design and Configuration	DCCS-2	Configuration Specifications		High	
Security Design and Configuration	DCCT-1	Compliance Testing		Medium	
Security Design and Configuration	DCDS-1	Dedicated IA Services		Medium	
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications		Medium	
Security Design and Configuration	DCHW-1	HW Baseline		High	
Security Design and Configuration	DCID-1	Interconnection Documentation		High	
Security Design and Configuration	DCII-1	IA Impact Assessment		Medium	
Security Design and Configuration	DCIT-1	IA for IT Services		High	
Security Design and Configuration	DCMC-1	Mobile Code		Medium	
Security Design and Configuration	DCNR-1	Non-repudiation		Medium	
Security Design and Configuration	DCPA-1	Partitioning the Application		Low	
Security Design and Configuration	DCPB-1	IA Program and Budget		High	
Security Design and Configuration	DCPD-1	Public Domain Software Controls		Medium	
Security Design and Configuration	DCPP-1	Ports, Protocols, and Services		Medium	
Security Design and Configuration	DCPR-1	CM Process		High	
Security Design and Configuration	DCSD-1	IA Documentation		High	
Security Design and Configuration	DCSL-1	System Library Management Controls		Medium	
Security Design and Configuration	DCSP-1	Security Support Structure Partitioning		Medium	
Security Design and Configuration	DCSQ-1	Software Quality		Medium	
Security Design and Configuration	DCSR-3	Specified Robustness – High		High	
Security Design and Configuration	DCSS-2	System State Changes		High	
Security Design and Configuration	DCSW-1	SW Baseline		High	
Enclave Boundary Defense	EBBD-3	Boundary Defense		Low	
Enclave Boundary Defense	EBCR-1	Connection Rules		Medium	
Enclave Boundary Defense	EBRP-1	Remote Access for Privileged Functions		High	
Enclave Boundary Defense	EBRU-1	Remote Access for User Functions		High	
Enclave Boundary Defense	EBVC-1	VPN Controls		Medium	
Enclave and Computing Environment	ECAD-1	Affiliation Display		Medium	

Table B-3. IA Control Details (continued)

Subject Area	Control Num.	IA Control Name	C/NC	Impact Code	Last Update
Enclave and Computing Environment	ECAN-1	Access for Need-to-Know		High	
Enclave and Computing Environment	ECAR-3	Audit Record Content		Low	
Enclave and Computing Environment	ECAT-2	Audit Trail, Monitoring, Analysis and Reporting		Low	
Enclave and Computing Environment	ECCD-2	Changes to Data		Medium	
Enclave and Computing Environment	ECCM-1	COMSEC		High	
Enclave and Computing Environment	ECCR-2	Encryption for Confidentiality (Data at Rest)		Medium	
Enclave and Computing Environment	ECCR-3	Encryption for Confidentiality (Data at Rest)		High	
Enclave and Computing Environment	ECCT-2	Encryption for Confidentiality (Data in Transit)		High	
Enclave and Computing Environment	ECDC-1	Data Change Controls		Medium	
Enclave and Computing Environment	ECIC-1	Interconnection among DoD Systems and Enclaves		Medium	
Enclave and Computing Environment	ECID-1	Host Based IDS		Medium	
Enclave and Computing Environment	ECIM-1	Instant Messaging		Medium	
Enclave and Computing Environment	ECLC-1	Audit of Security Label Changes		Low	
Enclave and Computing Environment	ECLO-2	Logon		Medium	
Enclave and Computing Environment	ECLP-1	Least Privilege		High	
Enclave and Computing Environment	ECML-1	Marking and Labeling		High	
Enclave and Computing Environment	ECMT-2	Conformance Monitoring and Testing		Low	
Enclave and Computing Environment	ECND-2	Network Device Controls		Low	
Enclave and Computing Environment	ECNK-1	Encryption for Need-To-Know		Medium	
Enclave and Computing Environment	ECNK-2	Encryption for Need-To-Know		Medium	
Enclave and Computing Environment	ECPA-1	Privileged Account Control		High	
Enclave and Computing Environment	ECPC-2	Production Code Change Controls		Medium	
Enclave and Computing Environment	ECRC-1	Resource Control		Medium	
Enclave and Computing Environment	ECRG-1	Audit Reduction and Report Generation		Low	
Enclave and Computing Environment	ECRR-1	Audit Record Retention		Medium	
Enclave and Computing Environment	ECSC-1	Security Configuration Compliance		High	
Enclave and Computing Environment	ECSD-2	Software Development Change Controls		High	
Enclave and Computing Environment	ECTB-1	Audit Trail Backup		Medium	
Enclave and Computing Environment	ECTC-1	Tempest Controls		High	
Enclave and Computing Environment	ECTM-2	Transmission Integrity Controls		Medium	
Enclave and Computing Environment	ECTP-1	Audit Trail Protection		Medium	
Enclave and Computing Environment	ECVI-1	Voice over IP		Medium	
Enclave and Computing Environment	ECVP-1	Virus Protection		High	
Enclave and Computing Environment	ECWM-1	Warning Message		Low	
Enclave and Computing Environment	ECWN-1	Wireless Computing and Networking		High	
Identification and Authentication	IAAC-1	Account Control		High	
Identification and Authentication	IAGA-1	Group Identification and Authentication		Medium	
Identification and Authentication	IAIA-2	Individual Identification and Authentication		High	
Identification and Authentication	IAKM-2	Key Management		Medium	
Identification and Authentication	IAKM-3	Key Management		Medium	
Identification and Authentication	IATS-2	Token and Certificate Standards		Medium	
Physical and Environmental	PECF-2	Access to Computing Facilities		High	

Table B-3. IA Control Details (continued)

Subject Area	Control Num.	IA Control Name	C/NC	Impact Code	Last Update
Physical and Environmental	PECS-2	Clearing and Sanitizing		High	
Physical and Environmental	PEDD-1	Destruction		High	
Physical and Environmental	PEDI-1	Data Interception		High	
Physical and Environmental	PEEL-2	Emergency Lighting		Medium	
Physical and Environmental	PEFD-2	Fire Detection		High	
Physical and Environmental	PEFI-1	Fire Inspection		Medium	
Physical and Environmental	PEFS-2	Fire Suppression System		Medium	
Physical and Environmental	PEHC-2	Humidity Controls		Medium	
Physical and Environmental	PEMS-1	Master Power Switch		High	
Physical and Environmental	PEPF-2	Physical Protection of Facilities		High	
Physical and Environmental	PEPS-1	Physical Security Testing		Low	
Physical and Environmental	PESL-1	Screen Lock		Medium	
Physical and Environmental	PESP-1	Workplace Security Procedures		Medium	
Physical and Environmental	PESS-1	Storage		High	
Physical and Environmental	PETC-2	Temperature Controls		Low	
Physical and Environmental	PETN-1	Environmental Control Training		Low	
Physical and Environmental	PEVC-1	Visitor Control to Computing Facilities		High	
Physical and Environmental	PEVR-1	Voltage Regulators		High	
Personnel	PRAS-2	Access to Information		High	
Personnel	PRMP-2	Maintenance Personnel		High	
Personnel	PRNK-1	Access to Need-to-Know Information		High	
Personnel	PRRB-1	Security Rules of Behavior or Acceptable Use Policy		High	
Personnel	PRTN-1	Information Assurance Training		High	
Vulnerability and Incident Management	VIIR-2	Incident Response Planning		Medium	
Vulnerability and Incident Management	VIVM-1	Vulnerability Management		Medium	

LEGEND:

AIS	Automated Information System	IDS	Intrusion Detection System
C	Compliant	IP	Internet Protocol
CM	Configuration Management	IT	Information Technology
COMSEC	Communication Security	NC	Non-Compliant
DoD	Department of Defense	Num	Number
HW	Hardware	SW	Software
IA	Information Assurance	VPN	Virtual Private Network

B-4 DEFENSE INFORMATION SYSTEM NETWORK (DISN) REAL TIME SERVICE (RTS) UNIFIED CAPABILITIES REQUIREMENTS (UCR). The purpose of this document and its appendices is to provide the RTS UCR that must be used for the acquisition of all hardware and software that support RTS. Table B-4, which was extracted from the RTS UCR, lists the components that pertain to Appendix D, DSN Architecture.

Table B-4. DISN RTS UCR Documentation Components

DISN RTS UCR Documentation Components	
Main Document	Section 1: Documentation Overview and Scope
	Section 2: RTS Requirement Sources
	Section 3: RTS Migration Framework
	Section 4: Migration of DSN GSCR to RTS UCR
	Section 5: RTS Architecture Overview
	Section 6: RTS Appliance Concept, System Under Test and JITC APL Process
UCR Appendices	Appendix A: ASCLAN UCR
	Appendix B: ARTS UCR
	Appendix C: WAN UCR
	Appendix D: IA
	Appendix E: AS-SIP GSS
	Appendix F: IPv6 UCR
	Appendix G: DSN GSCR
	Appendix H: Requirements
	Appendix I: Definitions, Acronyms and Abbreviations

LEGEND:

APL	Approved Products List	IA	Information Assurance
ARTS	Assured Real Time Services	IPv6	Internet Protocol version 6
ASCLAN	Assured Service Converged LAN	JITC	Joint Interoperability Test Command
AS-SIP	Assured Services Session Initiation Protocol	LAN	Local Area Network
DISN	Defense Information System Network	RTS	Real Time Services
DSN	Defense Switched Network	UCR	Unified Capabilities Requirements
GSCR	Generic Switching Center Requirements	WAN	Wide Area Network
GSS	Generic System Specification		

The RTS UCR document will be used to:

- Establish the standards and specifications needed by industry to develop requirements compliant RTS solutions.
- Provide the foundation for the development and finalization of the Generic System Test Plan (GSTP) for interoperability testing and IA Test Plan. These tests are used to make the decisions necessary to place products on the DoDI 8100.3 DSN APL so that combatant commands, services, and agencies can purchase them.
- Provide the foundation for the development and finalization of the STIG needed to properly operate the approved products once installed.

The system architecture and its associated requirements will define the technical solution for the system and its appliances, and a specific countermeasure which may or may not be used dependent on the architecture. Before discussing the countermeasures, it is important to define the terms used in the discussion.

- Registrant. An appliance, which 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 End Instrument (EI), Personal Computers, and Local Session Controller (LSC):

    - EI. An EI is a user appliance that initiates, accepts, and/or terminates RTS sessions. An EI may be standalone applications or may be used in conjunction with other applications (e.g., softphone). They may provide a single service (e.g., voice or video) or multiple services (e.g., videophone). In addition, end instruments may signal the LSC with standardized protocols or proprietary protocols
    - LSC. The primary role of the LSC is the session control and signaling (SCS) function. The SCS function comprises of two subfunctions called the Call Connection Agent (CCA) and the Assured Services Admission Control functions. The CCA can be further segmented into three functions: the CCA function, the Interworking function, and the Media Gateway Controller function.
- Registrar. The registrar is 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 RTS environment, examples of the registrar include LSC and DoD Public Key Infrastructure (PKI) servers. A registrar may reside on the same appliance and be integrated with a Service Point of Attachment (SpoA).
- SpoA. A SpoA is an appliance to which a registrant establishes a session over the Internet Protocol (IP) network. The session may be established to pass signaling or network management traffic. In the DoD RTS environment, examples of a SpoA are LSC, Multifunction Soft Switch (MFSS), Soft Switch (SS), directory servers, or gateways.
- MFSS. The MFSS is a network appliance that supports end office and tandem switch capabilities. In addition, the MFSS also includes LSC1 and Assured Real-Time Services SS functions to support line-side IP end instruments and trunk-side Assured Services Session Initiation Protocol (AS-SIP) signaling.
- The SS within the DoD environment is defined in accordance with the International Softswitch Consortium definition and is a programmable network appliance.
- 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 RTS environment include routers, Local Area Network switches, firewalls, border controller (BCs), MFSS, and gateways:
    - BC. BCs allow their owners to control the kinds of sessions that can be placed through the networks on which they reside and to overcome some of the problems that firewalls and Network Address Translation cause for IP RTS sessions.

B-5 RTS PROTOCOL ARCHITECTURE

The RTS protocol architecture consists of a combination of standards-based protocols and proprietary based protocols. However, every proprietary protocol must be secured in a manner that is at least as secure as can be achieved using a standardized protocol. The RTS architecture mandates the use of Transport Layer Security (TLS)

with AS-SIP to provide confidentiality and integrity. Independent of the protocol or cryptographic algorithm used, many common IA mechanisms are required of all appliances. In compliance with DoD requirements and policies, most RTS appliances will also be Public Key Enabled (PKE) so that they may interoperate with the DoD PKI with the exception of the EI for which the PKE requirement is the objective.

B-6 SIGNALING APPLIANCE AUTHENTICATION AND AUTHORIZATION/AS-SIP

The signaling appliances must also mutually authenticate to each other using the DoD PKI. Because all signaling appliances support AS-SIP, the authentication mechanisms must be integrated with AS-SIP to provide interoperability. Because the AS-SIP model chosen is a hierarchical signaling model, TLS was chosen as the IA protocol to secure AS-SIP because its hop-by-hop security model integrated nicely with the hierarchical signaling model. Fortunately, all AS-SIP signaling appliances (Objective for an EI) are required to be DoD PKE and support the DoD PKI. The process for obtaining a DoD PKI certificate is a manual process and has to be completed before or during the initial installation.

B-7 INTERNET PROTOCOL VULNERABILITY (IPV). Table B-5 shows the tools the IPV test team uses to conduct vulnerability scanning and penetration testing. Tools in bold are currently part of the JITC tool chest.

Table B-5. IPV Test Tools

Scanning	
Cisco global exploiter (Cisco scanner)	Nmap (Network scanner)
Cisco torch (Cisco oriented scanner)	NmapFE (Graphical network scanner)
ExploitTree search (ExploitTree collection)	Proxychains (Proxifier)
Metasploit (Metasploit command line)	Scanrand (Stateless scanner)
Metasploit (Metasploit console GUI)	Timestamp (Requests timestamp)
Metasploit (Metasploit web interface**)**	Unicornscan (Fast port scanner)
Nessus (Security scanner)	Isrscan (Source routed packets scanner)
Raccess (Remote scanner)	Amap (Application identification)
Retina (Security Scanner)	Bed.pl (Application fuzzer)
Httprint (Webserver fingerprinting)	SNMP-Fuzzer (SNMP protocol fuzzer)
Nikto (Webserer scanner)	ScanSSH (SSH identification)
Stunnel (Universal SSL tunnel)	SiVus (SIP Vulnerability Scanner)
Cheops (Network neighborhood)	Nbtscan (Netbios scanner)
GTK-Knocker (Simple GUI portscanner)	SMB-Nat (SMB access scanner)
IKE-Scan (IKE scanner)	Ozyman (DNS tunnel)
Knocker (Simple portscanner)	Ass (Autonomous system scanner)
Netenum (Pingsweep)	Protos (Protocol identification)
Netmask (Requests netmask)	
Analyzer	
Driftnet (Image sniffer)	IPTraf (Traffic monitor)
Mailsnarf (Mail sniffer)	NGrep (Network grep)
Paros (HTTP interception proxy)	NetSed (Network edit)
URLsnarf (URL sniffer)	SSLDump (SSLv3/TLS analyzer)
smbspy (SMB sniffer)	Sniffit (Sniffer)
Etherape (Network monitor)	TcPick (Packet stream editor)
Ethereal (Network analyzer)	Dsniff (Password sniffer)
Ettercap (Sniffer/Interceptor/Logger)	Core Impact
Hunt (Sniffer/Interceptor)	

Table B-5. IPV Test Tools (contined)

Spoofing	
Arpspoof (ARP spoofer)	Fragroute (Egress rewrite)
Macof (ARP spoofer/generator)	HSRP (HSRP generator)
Nemesis-ARP (ARP packet generator)	IGRP (IGRP injector)
Nemesis-Ethernet (Ethernet packet generator)	IRDP (IRDP generator)
CDP (CDP generator)	IRDPresponder (IRDP response generator)
DNSSpoof (DNS spoofer)	Nemesis-IGMP (IGMP generator)
Nemesis-DNS (DNS packet generator)	Nemesis-RIP (RIP generator)
DHCPX (DHCP flooder)	File2Cable (Traffic replay)
Hping2 (Packet generator)	Fragrouter (IDS evasion toolkit)
ICMPRedirect (ICMP redirect packet generator)	Nemesis-IP (IP packet generator)
ICMPUSH (ICMP packet generator)	Nemesis-TCP (TCP packet generator)
Nemesis-ICMP (ICMP packet generator)	Nemesis-UDP (UDP traffic generator)
Packit (Traffic inject/modify)	SendIP (IP packet generator)
TcPick (Packet stream editor)	TCPReplay (Traffic replay)
Yersinia (Layer 2 protocol injector)	Etherwake (Generate wake-on-LAN)
Bruteforce	
ADMsnmp (SNMP bruteforce)	SMB-Nat (SMB access scanner)
Guess-who (SSH bruteforce)	TFTP (bruteforce)
Hydra (Multi purpose bruteforce)	VNCrack (VNC bruteforce)
K0ldS (LDAP bruteforce)	Xhydra (Graphical bruteforcer)
Obiwan III (HTTP bruteforce)	
Password Craker	
BKHive (SAM recovery)	Nasty (GPG secret key cracker)
Fcrackzip (Zip password cracker)	Rainbowcrack (Hash cracker)
John the Ripper (Multi-purpose password cracker)	Samdump2 (SAM file dumper)
Default password list	Wordlists (Collection of wordlists)
Forensics	
Autopsy (Forensic GUI)	Testdisk (Partition scanner)
Recover (Ext2 file recovery)	Wipe (Securely delete files)

LEGEND:

ADM	Add Drop Multiplexer	IRDP	ICMP Router Discovery Protocol
ARP	Address Resolution Protocol	LAN	Local Area Network
Ass	Autonomous system scanner	LDAP	Lightweight Directory Access Protocol
CDP	Computer Data Processing	RIP	Routing Information Protocol
DHCP	Dynamic Host Configuration Protocol	SAM	Security Accounts Manager
DNS	Domain Naming Services	SIP	System Identification Profile
GPG	GNU Privacy Guard	SMB	Server Message Block
GNU	GNU's Not UNIX	SNMP	Simple Network Messaging Protocol
GTK	Gimp Tool Kit (program)	SSH	Secure Shell
GUI	Graphical User Interface	SSL	Secure Socket Layer
HSRP	Hot Standby Router Protocol	SSLv3	Secure Socket Layer 3
HTTP	Hypertext Transfer Protocol	TCP	Transmission Control Protocol
IDS	Intrusion Detection System	TFTP	Trivial File Transfer Protocol
ICMP	Internet Control Message Protocol	TLS	Transport Layer Security
IGMP	Internet Group Management Protocol	UDP	Universal Datagram Protocol
IGRP	Internet Gateway Routing Protocol	URL	Universal Resource Locator
IKE	Internet Key Exchange	VNC	Virtual Network Connection
IP	Internet Protocol		
IPV	IP Vulnerability		

(The page intentionally left blank.)

APPENDIX C

TEST PREPARATION DOCUMENTS

The Information Assurance Test Team (IATT) uses the Test Preparation document to record information relevant to the System Under Test (SUT). The information recorded is detailed component information, including manufacturer, make, and model, operating system, vendor-developed software, other commercial software, version, and firmware. The IATT tracks the date of the test, tracking number of the SUT, tester's name, vendor's name, vendor's solution name, e-mail addresses, and phone numbers.

DSN IA Test Team Test Preparation Document
Tracking Number: _____

Vendor Information	
Vendor Name	Mitel
Name of SUT	3300 ICP Release 8.0.6.1
Type of System	MFS ☐ SMEO ☐ EO ☐ NE ☐ CPE ☐ NMS ☐
	ASLAN ☐ ECAN ☐ Other ☐ List:
Vendor POC	
Email	
Phone	

Testing Dates		
Phase I		Complete ☐
Phase II		Complete ☐
Phase III		Complete ☐
IO Testing		Complete ☐

Tester Information		
Phase I Tester (STIG)	Name	
	Phone	
	Email	
Phase I Tester (GR-815)	Name	
	Phone	
	Email	
Phase II Tester	Name	
	Phone	
	Email	
Phase III Tester	Name	
	Phone	
	Email	

System Information		
STIG Test	Functionality	
	Before Testing ☐ YES ☐ NO	After Testing ☐ YES ☐ NO
GR-815 Test	Functionality	
	Before Testing ☐ YES ☐ NO	After Testing ☐ YES ☐ NO
IPV Test	Functionality	
	Before Testing ☐ YES ☐ NO	After Testing ☐ YES ☐ NO
PA/TDM Test	Functionality	
	Before Testing ☐ YES ☐ NO	After Testing ☐ YES ☐ NO

DSN IA Test Team Test Preparation Document
Tracking Number: _____

System Information			
System Diagram (Copy to "T" Drive)	Attached ☐ YES ☐ NO	Type	Visio ☐
			Jpeg ☐
			PowerPoint ☐
Appendix B system and component description attached? ☐ YES ☐ NO			
Appendix C in-brief minutes attached? ☐ YES ☐ NO			
Location GNTF ☐ GNTF ANNEX ☐	Circle on map and note rack numbers below		
RAE Equipment connections	RADIUS ☐ SysLog ☐ AD ☐ TACACS ☐ Client ☐		

IP Information			
DHCP in use ☐ DHCP capable ☐			
IP Address Start	IP Address End	Subnet	VLANs
Routers ☐	Configurations collected ☐		
Switches ☐	Configurations collected ☐		
Note: Store information on "T" Drive			

Adjust the top portion as needed with the correct switch information and versions.

System Name	Hardware/Software Release		
Siemens EWSD (MFS, EO)			
Nortel Networks MSL-100 (MFS, EO)			
Avaya S8710/20 (SMEO, PBX 1, PBX 2)			
Lucent 5ESS (MFS, EO)			
	Hardware	**Card Name** **Part Number/ Name**	**Software/ Firmware**
SUT Telephones			
Telephone type	**Model**	**Firmware**	

Note: Put in logical order and ensure information is complete; if there are no cards/part numbers/etc., remove that information from this table before completing the report.

DSN IA Test Team Test Preparation Document
Tracking Number: _____

By signing this document, I have verified that all information is identified correctly and all version numbers identified within this document have been physically verified on the system under test.

_____ Date:_____
Vendor

_____ Date:_____
STIG Tester

_____ Date:_____
GR-815 Tester

_____ Date:_____
IPV Tester

_____ Date:_____
PA/TDM Tester

_____ Date:_____
IO Tester

_____ Date:_____
STIG Technical Lead (Gardner)

_____ Date:_____
IPV Technical Lead (Searle)

Have the passwords been turned over to the GNTF System Administrator?

☐ YES ☐ NO (check one)

_____ Date:_____
GNTF System Administrator

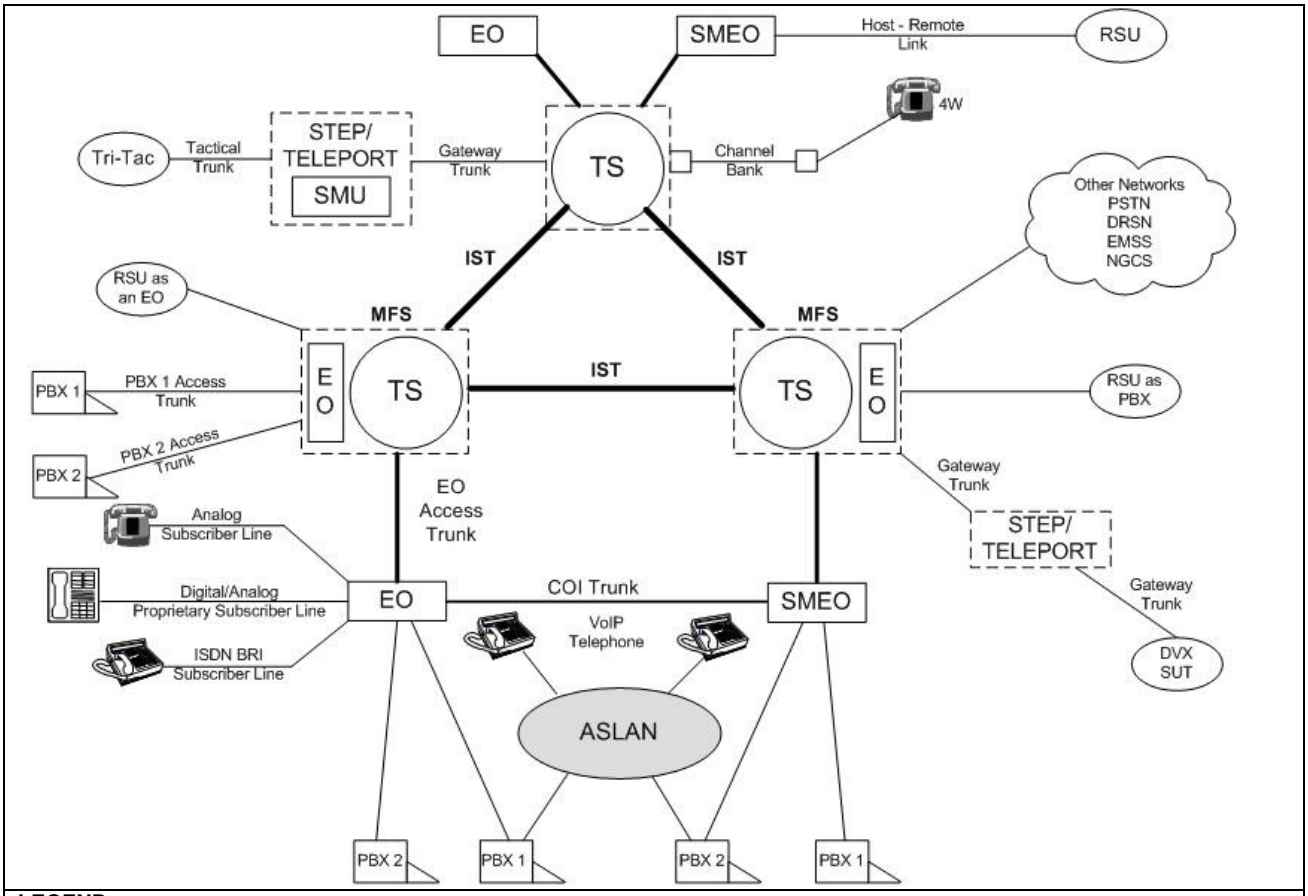
**Note: Turn over all required documents (this document, copies of relevant results, etc.) to the next tester(s). Place original test preparation document in designated storage area.

(The page intentionally left blank.)

APPENDIX D

DSN ARCHITECTURE

The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Each Information Assurance findings report will include the system as shown in Figure D-1 as indicated by the System Under Test.



LEGEND:

4W	4 Wire	NATO	North Atlantic Treaty Organization
ASLAN	Assured Services Local Area Network	NGCS	NATO General Purpose Segment Communication System
BRI	Basic Rate Interface		
CB	Channel Bank	PBX	Private Branch Exchange
COI	Community of Interest	PBX 1	Private Branch Exchange 1
DRSN	Defense Red Switch Network	PBX 2	Private Branch Exchange 2
DSN	Defense Switched Network	PSTN	Public Switched Telephone Network
DVX	Deployable Voice Exchange	RSU	Remote Switching Unit
EMSS	Enhanced Mobile Satellite Services	SMEO	Small End Office
EO	End Office	SMU	Switch Multiplexer Unit
ISDN	Integrated Services Digital Network	STEP	Standardized Tactical Entry Point
IST	Inter-Switch Trunk	Tri-Tac	Tri-Service Tactical Communications Program
MFS	Multifunction Switch	TS	Tandem Switch

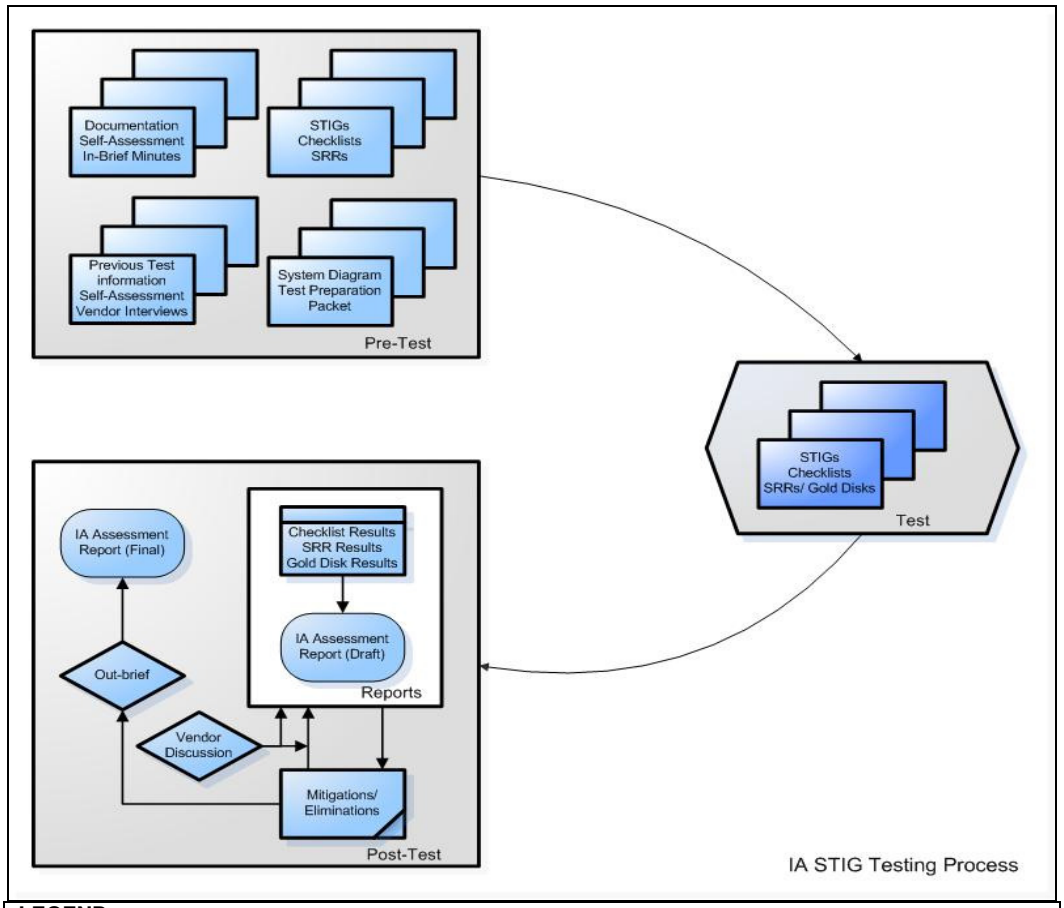
Figure D-1. DSN Architecture

(The page intentionally left blank.)

APPENDIX E

ASSESSMENT OBJECTIVES, CRITERIA, PROCEDURES, AND DATA REQUIRED

The following sections outline the objectives, criteria, procedures, and data required for the Information Assurance (IA) assessment of a System Under Test (SUT). An IA assessment is required before a SUT can be considered for the Defense Switched Network (DSN) Approved Products List (APL). This process is divided into three phases, as shown in Figure E-1, Pre-Test, Test, and Post-Test.



LEGEND:

IA	Information Assurance	STIG	Security Technical Implementation Guidelines
SRR	Security Readiness Review		

Figure E-1. Information Assurance STIG Testing Process

E-1 TESTING PROCEDURE.

E-1.1 Preparing Test.

E-1.1.1. Information Collection. This section covers the entire information collection process required to conduct an IA assessment of a SUT, including special cases.

E-1.1.2 Vendor Documentation. The vendor's documentation includes system diagrams, system descriptions, user guides, administration manuals, technical manuals, and white papers about a SUT. This information is critical to ensure the test team fully understands the system and can properly test it. The SUT information includes the following details for each component: software name and version number(s), and hardware name and model number(s) description and function.

E-1.1.3 In-Brief. The in-brief, also called an Initial Contact Meeting, occurs after the vendor submits a system for testing and all documentation has been received at the Unified Capabilities Connection Office (UCCO). During the in-brief, the points of contacts, sponsor, Field Security Office (FSO), and vendor representatives are confirmed with the UCCO. In some cases, the test team will conduct a Verification and Validation (V&V). At the request of the FSO, the IA Test Team (IATT) will verify and validate specific items. This is documented in an additional report or sometimes the same report previously written, depending on how many items are being verified or validated.

E-1.1.4 Self-Assessment. The purpose of the self-assessment is twofold: the first is for the vendor to understand the status of their system, in regard to the applicable regulations from the Department of Defense (DoD) perspective; the second is to allow all involved parties to understand the status of the system in regard to IA.

E-1.1.5 Reference Materials. The following section provides a description of references that are used when performing an IA assessment.

E-1.1.6 Security Technical Implementation Guidelines (STIG). The STIG are based on Best Business Practices, DoD Directives (DoDD), other DoD publications, Public Laws, and other Federal Government regulations. These documents are detailed descriptions how to secure the SUT and establish a baseline security for a DoD information system. The detailed information documents are available at <http://iase.disa.mil/stigs/stig/index.html>.

E-1.1.7 Security Readiness Review (SRR)/Gold Disks. The Defense Information Systems Agency (DISA) Gold Disks and SRRs are partially automated tools used to test a system's security posture against the DISA-established baseline. The detailed information documents are available at <http://iase.disa.mil/stigs/SRR/index.html>.

E-1.1.8 Checklists. The checklists used in conjunction with the parent STIG are part of a manual review method to assess the security posture of a system against the DISA security baseline. The detailed information documents are available at <http://iase.disa.mil/stigs/checklist/index.html>.

E-1.1.9 Test Packet. The test packet allows the tester to compile system information and to include components to be tested and specific component descriptions regarding the SUT.

E-1.1.10 DSN IATT Test Preparation Document. The IATT uses this document to record information relevant to the SUT. The information recorded is detailed component information, including manufacturer, make, model, operating system, vendor-developed software, other commercial software, version, and firmware. The IATT tracks the date of the test, tracking number of the SUT, tester's name, vendor's name, vendor's product name, e-mail addresses, and phone numbers.

E-1.1.11 System Diagram. The system's network diagram shows how all the components of the SUT are connected. The diagram should include the following information: component name, including host name or function, Internet Protocol (IP) address for each component, media type, interfaces, and boundary markings. Note: If documentation is found to be insufficient, the tester must request additional information from the UCCO through his task lead.

E-2 STIG TEST The STIG testing evaluates the security readiness of the system against the DISA minimum-security baseline.

The first day of testing will typically include the following:

- The tester meets with a vendor representative to discuss the SUT.
- The vendor explains the purpose of the SUT and how it operates.
- The vendor and the tester validate the system diagram and SUT description (the tester may require the vendor to provide an updated diagram or detailed description.)
- The vendor and the tester determine what each component in the SUT does and determine if any additional components are present that were not previously noted.
- After the vendor has explained the system and described its components, testers may add STIGs.
- The tester restates the test boundaries, which the vendor cannot change, and ensures all boundaries are stated and clear.
- The tester informs the vendor that during the test, time will be set aside for a meeting with the government, if desired, to answer questions regarding the test and APL process and address vendor concerns.
- The tester performs a full functionality test to determine if all components are working before applying the STIGs.

The configuration of the system being tested is determined before testing, based on the number of components, availability of resources, and allotted period. Tables E-1 through E-4 contain information for using the DISA Gold Disk, which is only applicable to Windows Systems. Table E-5 contains information for using the SRR scripts. Table E-6 contains manual testing procedures. The following references are used in Tables E-1 through E-5:

- STIG/Security Guides/National Security Agency (NSA) Guides
- SRRs/Gold Disk
- Manual Checklists

Table E-1. Gold Disk Minimum System Requirements

Gold Disk Minimum System Requirements	
Operating System	Windows 2000 Professional Windows 2000 Member Server Windows 2000 Domain Controller Windows 2003 Member Server Windows 2003 Domain Controller Windows XP
Internet Explorer	Internet Explorer 6.0 or above
Account Privileges	User account used to run the Gold Disk must have Administrator privileges.
User Right	User account used to run the Gold Disk must have "Manage Auditing and Security Log"
Minimum Screen Resolution	800 x 600
LEGEND: XP Experience	

Table E-2. DISA Gold Disk Test Procedure

Objective	To determine if the SUT is compliant with the DISA security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional before execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection for computer-generated reports in an easily accessible place. 7. Insert the Gold Compact Disk into an available optical drive. 8. Using Windows Explorer, double-click on the file "Launcher.exe". 9. After the pre-scan is completed, the following items must be selected for each asset listed in the "Asset Posture" window: • Mission Critical • Sensitive • Platinum 10. Select the "Evaluate Asset" button from the tool bar. 11. After evaluation is completed, save a preliminarily report to the temporary folder that was created in step 6. • Click Reports tab on the file toolbar. • Select VMS 6.X. • Save the file as VMS 6.X before.xml. 12. Evaluate all items listed for potential vulnerabilities and false positives. 13. If time permits, the vendor may remediate any findings that are marked as open. 14. Evaluate all findings marked as unknown. If time permits, the vendor may remediate these findings. 15. Click Reports tab on the file Toolbar. 16. Select VMS 6.X. 17. Save a final report with a different name to the temporary folder that was created in step 6. See section E-4.1 for instructions on reading the Extensible Markup Language file. 18. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number of findings that resulted in errors • IA Control information
Collection Forms	Information Assurance Assessment Report. DIACAP Scorecard

LEGEND:

DIACAP	DoD IA Certification and Accreditation Process	IA	Information Assurance
DoD	Department of Defense	SUT	System Under Test
DISA	Defense Information Systems Agency	VMS	Vulnerability Management System

Table E-3. DISA Gold Disk Test Procedure Alternate No Optical Drive

Objective	To determine if the SUT is compliant with the DISA security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional before the execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection of computer-generated reports in an easily accessible place. 7. Insert the Gold Compact Disk into an available optical drive on separate machine. 8. Copy the content of the Gold Disk to the SUT or to a portable USB drive (USB drive must have more than 512 megabytes of free space). 9. Using Windows Explorer, double-click on the file “Launcher.exe”. 10. After the pre-scan is completed, the following items must be selected for each asset listed in the “Asset Posture” window • Mission Critical • Sensitive • Platinum 11. Select the “Evaluate Asset” button from the tool bar. 12. After evaluation is completed, save a preliminarily report to the temporary folder that was created in step 6: • Click Reports tab on the file toolbar. • Select VMS 6.X. • Save the file as VMS-6xbefore. 13. Evaluate all items listed for potential vulnerabilities and false positives. 14. If time permits, the vendor may remediate any findings that are marked as open. 15. Evaluate all findings marked as unknown; if time permits, the vendor may remediate these findings. 16. Save a final report, with a different name, to the temporary folder that was created in step 6. See section E-4.1 for instructions on reading the Extensible Markup Language file. 17. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number of findings that resulted in errors • IA Control information
Collection Form	Information Assurance Assessment Report. DIACAP Scorecard

LEGEND:

DIACAP	DoD IA Certification and Accreditation Process	IA	Information Assurance
DISA	Defense Information Systems Agency	SUT	System Under Test
DoD	Department of Defense	USB	Universal Serial Bus
		VMS	Vulnerability Management System

Table E-4. DISA Gold Disk Test Procedure Alternate Command Line

Objective	To determine if the SUT is compliant with the DISA security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Gold Disk is the most current version available. 2. Review the Gold Disk user guide to verify any changes to procedure for running the Gold Disk. 3. Perform a full functionality test. 4. Ensure Internet Explorer 6 is installed and fully functional before the execution of the Gold Disk. 5. Determine the applicable procedure to be used based on system configuration. 6. Create a folder for temporary collection of computer-generated reports in an easily accessible place. 7. Insert the Gold Compact Disk into an available optical drive. 8. The command line option for non-interactive mode is “pgd.exe /f:<path:filename>”, where “<path:filename>” is replaced by the full path and filename of the non-interactive run control file. 9. The Non-Interactive Control File you must specify all of these options: • MAC • Confidentiality • Report Path • Report Filename • Report Format(s) • Whether to create an asset XML file (TRUE/FALSE) o Target(s)Target Identification (ID) Number o Policy ID Number o Whether to perform fixing (TRUE/FALSE) 10. Any vulnerabilities for which fixing should be skipped for this target (using the Vulnerability ID(s)). 11. Save a final report, with a different name, to the temporary folder that was created in step 6. See section E-4.1 for instructions on reading the XML file. 12. Perform a full functionality test.
Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable Data: • VMS Identification Number • Potential Discrepancy Indicator • Number of findings that resulted in errors • IA Control information
Collection Form	Information Assurance Assessment Report DIACAP Scorecard

LEGEND:

DIACAP	DoD IA Certification and Accreditation Process	MAC	Mission Assurance Category
DISA	Defense Information Systems Agency	SUT	System Under Test
DoD	Department of Defense	VMS	Vulnerability Management System
IA	nformation Assurance	XML	Extensible Markup Language
ID	Identification		

Table E-5. SRR Test Procedure

Objective	To determine if the SUT is compliant with the DISA security baseline.
Criteria	Systems shall maintain and guarantee operation within a secure environment without disruption of service and be able to sustain secure operations (Objective).
Procedures	1. Ensure the Security Technical Implementation Guidelines and SRR to be used are the most current version. 2. Perform a full functionality test. 3. The tester will ensure a means of logging onto the system as root (using su -) has been established for conducting the SRR. 4. Load and untar the scripts in a directory tree that will not interfere with the actual SRR, i.e., not in somebody's home directory tree. Some suggestions are: • /export/home/SRR, for Solaris • /home/SRR for HP-UX 5. Use a directory tree where there is a lot of available space (determined by using df -k on Solaris (and others) and bdf on HP. 6. The SRR directory will be used to transfer the UNIX scripts, which instructs the SRR to build the output data from (hostname.tar.Z). 7. Ensure file transfers are accomplished using the binary file transfer mode of the data transfer utility. 8. After transferring the script tar file to the machine, the reviewer will execute su -, and the vendor will enter the root password. • Ensure the root SHELL is /sbin/sh. 9. Ensure the account/directory established for the SRR is located in a sizeable file system that is NOT one of /, /etc, /var, /usr/bin, /usr/sbin, /sbin or any other level file system. A user file system with adequate space is appropriate. Adequate space is 50 megabytes or more. Ensure permission on the account/directory into which the scripts are transferred is 700 and the permission of the script tar file is 700. Check file system space using the following command: • df (for Solaris) or bdf (for HP-UX) 10. Uncompress the tar file using one of the following commands. (Note: Ensure the name of SRR file is typed EXACTLY as the one transferred and remember case sensitivity.) uncompress ddmmmyy-Unix.tar.Z • gunzip ddmmmyy-Unix.tar.gz • unzip ddmmmyy-Unix.tar.zip • bzip2 -d ddmmmyy-Unix.tar.bz2 Note: If there is an error when reading the file, it usually means the file was NOT transferred using the binary command. 11. Extract the tar file. This process will create a directory named Script in the SRR directory and that directory will contain all the Script subdirectories and data. Make sure you are in the SRR directory. Extract the scripts using the following command: • tar xvf ddmmmyy-Unix.tar Note: If there is an error, such as "checksum error", it usually means the tar file was NOT transferred using the binary option. 12. Change directory to the newly created Script directory using the following command: • cd Script.Month

Table E-5. SRR Test Procedure (continued)

Procedures	13. The scripts can now be applied using one of the following commands: • Use nohup /Start-SRR & (if running the scripts in background and using nohup to create a record of all the actions in the nohup.out file). This command will also run the utilities for crack and the global find. It will not take the "Tivoli" option, which would run the scripts and create an output report for installations performing self-assessments using the Tivoli Distribution function to distribute the scripts, execute the scripts, and retrieve the output of the scripts into a home grown reporting facility). • Use ./Start-SRR & (to just run the scripts in background without the nohup.out file and with all the other options listed above). • Use ./Start-SRR nocrack (may also be used with nohup and in background will run the SRR scripts but skip running crack, which can take hours to execute on a large system). • Use ./Start-SRR tivoli (may also be used with nohup, in background and in combination with nocrack will simply run the scripts and generate a report file for transfer back to the master Tivoli console). • Use ./Start-SRR nofind (may be used in combination with any or all of nocrack and tivoli. The nofind option bypasses the execution of the global find that may be useful if re-running numerous scripts that do not use the output of the global find). • The defaults for the options for Start-SRR are: nocrack=y (run crack), nofind=y (run the global find), and Tivoli=n (do not produce Tivoli output). 14. Outputs from running the scripts will include (Note: Item Number = Checklist Item Number = PDI Number (or, Secure Digital Identification) = Script number): • Hostname: Directory created under the Script directory where the following output files are stored: • PDI.Result: A file for each script containing finding status, description, and examples (if status is Open, Not Reviewed, or Not Applicable). • PDI.Examples: A file containing the full list of findings for an item. It will only exist if there have been findings, if the item is a manual review item or, it is not applicable to the operating system/machine type. • Hostname.Log: A file created for each item. It will contain error messages if the script failed or, it will be size zero. • SRR.Initial.Results: A file containing a summary list of PDIs marked as Not Reviewed; Counts of findings in all categories; PDIs marked as Open findings; PDIs marked as Not a Finding; Scripts which did not complete (if any); Scripts which found Category I Findings (if any). • Hostname.patch.report: For Solaris systems, a file that contains a detailed patch report for the reviewed Solaris system. The system must have perl 5.005 in the search PATH or it will not be produced. Otherwise, the manual side will run and all the results will be in the G033.Examples file. • FindFile: A file containing the results of the global find run at the beginning of the SRR from Start-SRR. • Hostname.txt: A file created by the SRRDB update program for import into the SRR database. SiteConfiguration: Directory, containing copies of several configuration files, to be used by the reviewer to check findings results and for technical review to verify the accuracy of all SRR checks. They are default* hosts.deny Passwd device.tab inetd.conf PkgInfo devlink.tab Inittab Pslist df-file Last RootCron dgroup.tab localpatches System Group Mnttab VarAdmin Hosts.allow Netstatus Vfstab (NOTE: Directory containing /etc/default files). • guessed.pw.report: A file created in the following directory by running Crack. It is placed in the ~Script/CRACK/SystemName directory. • hostname.Report: A file created by running the Review-Findings program. It summarizes SRR findings in one of five different choices.

Table E-5. SRR Test Procedure (continued)

Procedures	15. Run the Manual-Review script. It must be run in this order the first time. Once it has been run for a system, it need not be run again unless the status of a finding changes to Not Reviewed. The Manual-Review script serves these purposes: • Creates system and key personnel information. ○ Creates the Asset record data ○ Creates the module record data ○ Allows reviewers to update Not Reviewed items 16. When the Manual-Review program is completed, all items will be filled in (automated and manual). The process includes interviews with the System Administrator/Information System Security Officer, and even the Information Systems Security Manager, for answers to some of the Not Reviewed items. The program will prompt to automatically run the next utility program: SRRDBupdate. Run the Manual-Review from the Script directory with the following command: • ./Manual-Review 17. Run the SRRDBupdate script. It creates the import file for the SRRDB and the output name is hostname.txt. The Manual-Review script will automatically execute SRRDBupdate. It prints a dot on the screen for each record it processes. The SRRDBupdate program initially prompts for the name of the system to create the SRR database input file, so it could be used to create outputs for multiple systems as long as the data is provided in a hostname directory under the Script directory. It may be run more than once, as long as the Manual-Review program has been run before it. 18. Execute the script stand-alone, type from the Script directory: • ./SRRDBupdate 19. Run the Review-Findings script. For SRR reviewers, Review-Findings scripts may not be run unless the SRRBDupdate program has been run successfully before. For site users performing self-assessments, it may be run out of order while SRRDBupdate file is tuning the system. For SRR reviewers, it may be run stand-alone at any time after the first time it has been run, and may be run multiple times for different systems. Review-Findings generate the hostname.report with a summary of findings from the SRR. It has five choices for the type of output it produces: • Output all items • Output only open items • Output only Not Reviewed items • Output only Not Applicable items • Output only Not a Finding items 20. The Review-Findings Script must be run after the SRRDBupdate script, which will prompt for execution when it completes. Since the Review-Findings script produces the output tar file, and the SRRDBupdate script creates the hostname.txt file that must be with it, the script Review-Findings must be run before it. The Review-Findings script from the Script directory must be run with the following command: • ./Review-Findings 21. Review and validate the findings with the vendor. 22. If time permits, the vendor may remediate any findings that are marked as open. 23. Retrieve the tar file of the SRR data (from the hostname directory) from the system. It will be found in the directory above the Script directory by the Review-Findings script. See section E-4.1 for instructions on reading the Extensible Markup Language file. 24. Perform a full functionality test.

Table E-5. SRR Test Procedure (continued)

Data Required	Test conductor will collect test information on: • System configurations at time of test • Findings that are fixed on site • Findings that are open • Findings that are closed • Findings that are Not Applicable **Data:** • VMS Identification Number • Potential Discrepancy Indicator • Number finding that resulted in errors • IA Control information
Collection Form	Information Assurance Assessment Report DIACAP Scorecard

LEGEND:

DIACAP	DoD IA Certification and Accreditation Process	PDI	Potential Discrepancy Indicator
DISA	Defense Information Systems Agency	SRR	Security Readiness Review
DoD	Department of Defense	SRRDB	Security Readiness Review Data Base
HP	Hewlett-Packard	SUT	System Under Test
HP-UX	Hewlett Packard UNIX	VMS	Vulnerability Management System
IA	Information Assurance		

E-3 MANAGEMENT WORKSTATION HARDENING PROCEDURES. The purpose of this procedural document is to account for the deviations from the required settings listed in the Windows XP STIG. Each application that is installed on the management workstation introduces additional vulnerabilities to the workstation and the entire system. The following procedure will account for the changes by having before and after results showing the differences due to the installation of the application. The resultant differences are annotated as findings on the DoD Information Assurance Certification and Accreditation Process (DIACAP) Scorecard and the findings report. Note: This procedure is intended for un-partitioned hard disk drives.

E-3.1 Windows XP Professional Installation.

E-3.1.1 All partitions must be configured as New Technology File System (NTFS) unless otherwise needed for images or other small storage requirements. There must be no un-partitioned space on the hard disk drives.

E-3.1.2 Perform a clean install for the system, ensuring all previous data is removed.

E-3.1.3 Install Service Pack 2.

E-3.1.4 If JavaRE is needed install it at this time.

E-3.1.5 Install all Windows updates.

E-3.1.6 Install all device drivers for the system.

E-3.1.7 Disable all excessive devices in the systems' Basic Input/Output System (BIOS).

E-3.2 Anti-Virus.

E-3.2.1 Install and update anti-virus as needed.

E-3.2.2 Set up Weekly full scans (see the Desktop Application Checklist

for procedures).

E-3.2.3 Set up a Quick Scan daily (see the Desktop Application Checklist for procedures).

E-3.3 POSIX Subsystem File Components.

E-3.2.1 Select the "Search" button from the Tools bar.

E-3.2.2 Enter the following name in the "Search for files and folders named" field: **POSIX, PSX**

E-3.2.3 Click on the "Search" button.

E-3.2.4 If the search indicates that the files "POSIX.EXE," "PSXSS.EXE" or "PSXDLL.DLL" exist, then delete these files.

E-3.4 Securing the Event Logs. Reference the Windows 2003/XP/2000/VISTA Addendum for details.

Under Windows, when an event log is cleared, the system deletes and re-creates the log file. This, in effect, restores the default file permissions to those of the parent directory. Permissions for the "Auditors" group are removed and the Administrators group receives full control. To prevent the problem of having to reset permissions on the event log whenever it is cleared, follow the procedures below:

E-3.4.1 Create a subdirectory for the event logs: %SystemRoot%\system32\config\EventLogs.

E-3.4.2 Set Access Control Lists (ACL) permissions on this directory. (Auditors – Full Control, System – Full Control, Administrators – Read)

E-3.4.3 Copy the event logs from the \config directory to the new EventLogs directory.

E-3.4.4 Edit the Registry using regedit.exe.

E-3.4.5 Expand the following key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog.

E-3.4.6 Select the Application key.

E-3.4.7 Double-click the "File" value.

E-3.4.8 Change the string value to: %SystemRoot%\system32\config\EventLogs\Appevent.evt.

E-3.4.9 Repeat Steps E-3.4.5 through E-3.4.7 for "Security (Secevent.evt)" and "System (Sysevent.evt)".

The next time the machine is rebooted, it will use the event logs in the EventLogs directory. After the reboot, remove the old event logs from the \config directory.

E-3.5 Password Filter. Reference the Windows XP Checklist Section 5 for details. The Joint Test Facility (JTF)-Global Network Operations (GNO) Communications Tasking Order (CTO) 06-02, states: Passwords will contain a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters. The password will be a minimum of 15 characters in length. Note: Enpasflt.dll included with the Gold Disk will enforce these requirements. It can be found on Compact Disk 1 in the Install\Misc directory. Installation Instructions:

E-3.5.1 Install in %systemroot%\system32.

E-3.5.2 Restart the system.

E-3.5.3 Registry key.
"HKLM\System\CurrentControlSet\Control\LSA\Notification Packages" must include "enpasflt".

E-3.5.4 Disable Microsoft Password Complexity (5.4.1.5). Set policy "Password must meet complexity requirements" to disabled.

Note: Several system-generated user accounts may generate findings in an SRR, saying that the account is not required to have a password (i.e., IUSR_…, TSUser). To correct this problem, enter the following on a command line:
"Net user <account_name> /passwordreq:yes".

E-3.6 Pre-hardening Script.
This script will set all values for Internet Explorer (6.0 only), create an auditor user and group, and set membership. This script is updated on a continuous basis.

E-3.6.1 From Explorer open a command prompt by clicking start->run->type "cmd" in the window and enter.

E-3.6.2 At the prompt, type in "run Hardening Script.bat".

E-3.6.3 Any errors will be in the Script.log file, viewable with Notepad.

E-3.7 Using the Microsoft Management Console (MMC). Refer to the Windows XP checklist, section 5, for details. The MMC is the primary system configuration tool for Windows XP. It uses "snap-in" functions to configure the various parts of the system. The security configuration and analysis snap-in permits the analysis of account policy, system auditing, local policies, event logs, services, registry ACLs and auditing, and file ACLs and auditing.

E-3.7.1 Procedure: Use the following procedure to use the MMC and load the Security Configuration and Analysis snap-in:

E-3.7.1.1 Select "Start" and "Run" from the desktop.

E-3.7.1.2 Type "mmc.exe" in the Run dialog.

E-3.7.1.3 Select "File" from the MMC menu bar.

E-3.7.1.4 Select "Add/Remove snap-in" from the drop-down menu.

E-3.7.1.5 Click the "Add" button on the Standalone tab.

E-3.7.1.6 Select the "Security Configuration and Analysis" snap-in and click the "Add" button.

E-3.7.1.7 Click "Close".

E-3.7.1.8 Click "OK". See Figure E-2.

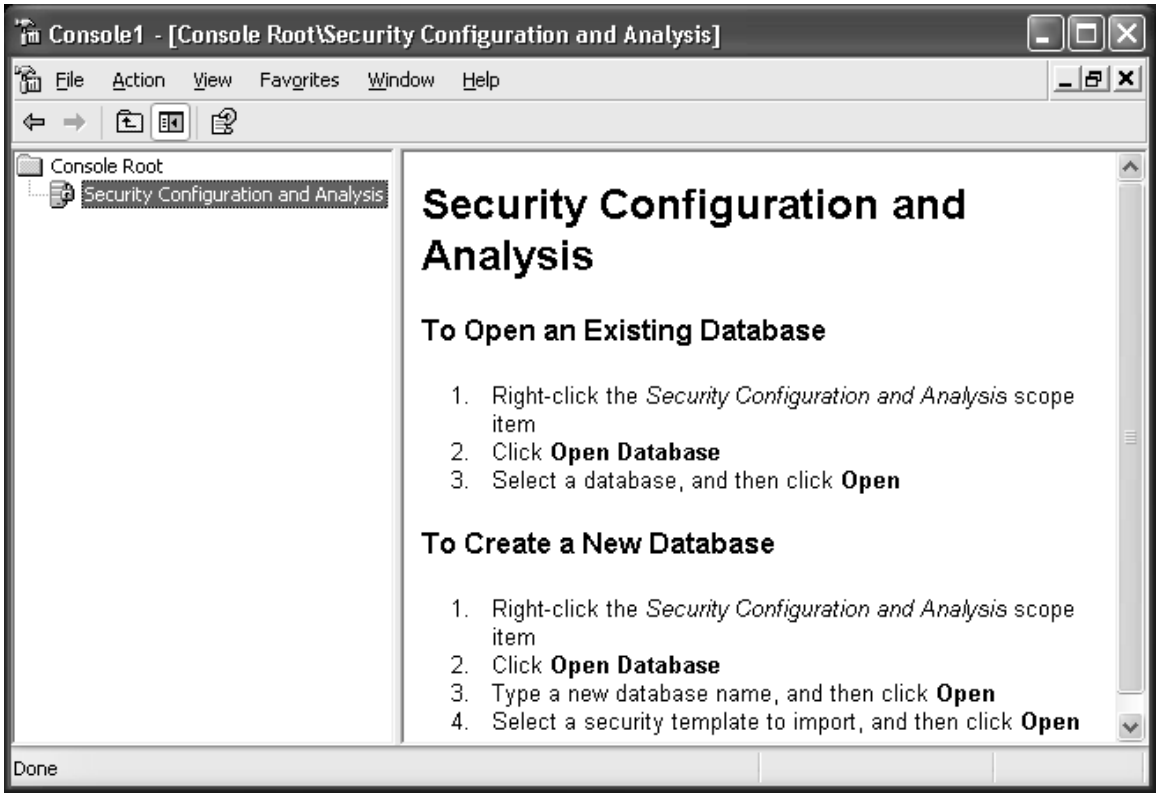


Figure E-2. Security Configuration and Analysis

E-3.7.2 Use the following procedure with the Security Configuration and Analysis snap-in and Figure E-3 to prepare the files for analyzing the system:

E-3.7.2.1 Right-click on the Security Configuration and Analysis object in the left window.

E-3.7.2.2 Select “Open Database”.

E-3.7.2.3 Enter “C:\temp\scan\srr.sdb” for the database name.

E-3.7.2.4 In the ‘Import Template’ window, enter the appropriate file name for a workstation (i.e., Hardening.inf).

E-3.7.2.5 Check the box to “Clear the database before importing”.

E-3.7.2.6 Select “Open”.

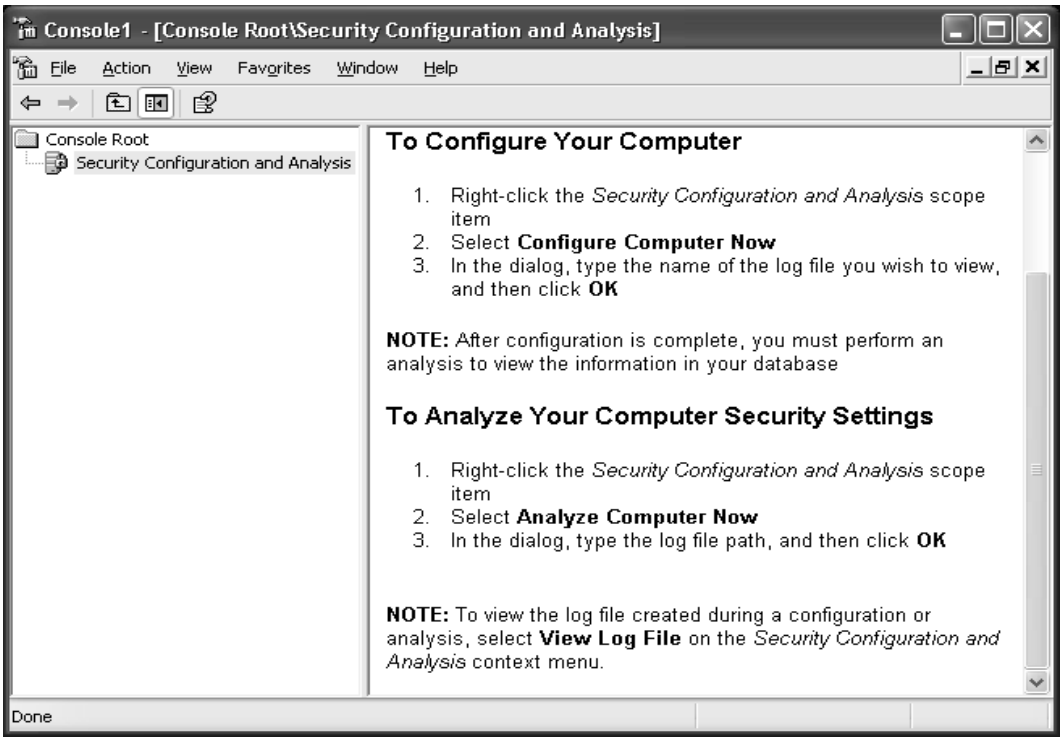


Figure E-3. Configure Your Computer

E-3.7.3 Use the following procedure to analyze the system:

E-3.7.3.1 Right-click on the Security Configuration and Analysis object in the left window.

E-3.7.3.2 Select “Analyze Computer Now.”

E-3.7.3.3 Enter “C:\temp\scan\srr.log” for the log name in the “Error log file path” window and click OK.

E-3.7.4 The following window, Figure E-4, will display:

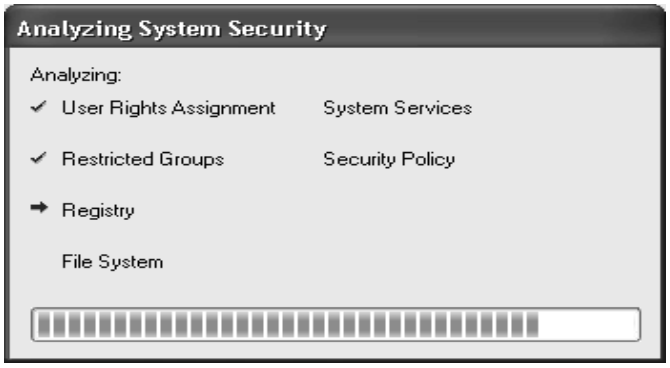


Figure E-4. Analyzing System Security

E-3.7.5 When the analysis is completed, the right pane will show the analysis objects. See Figure E-5.

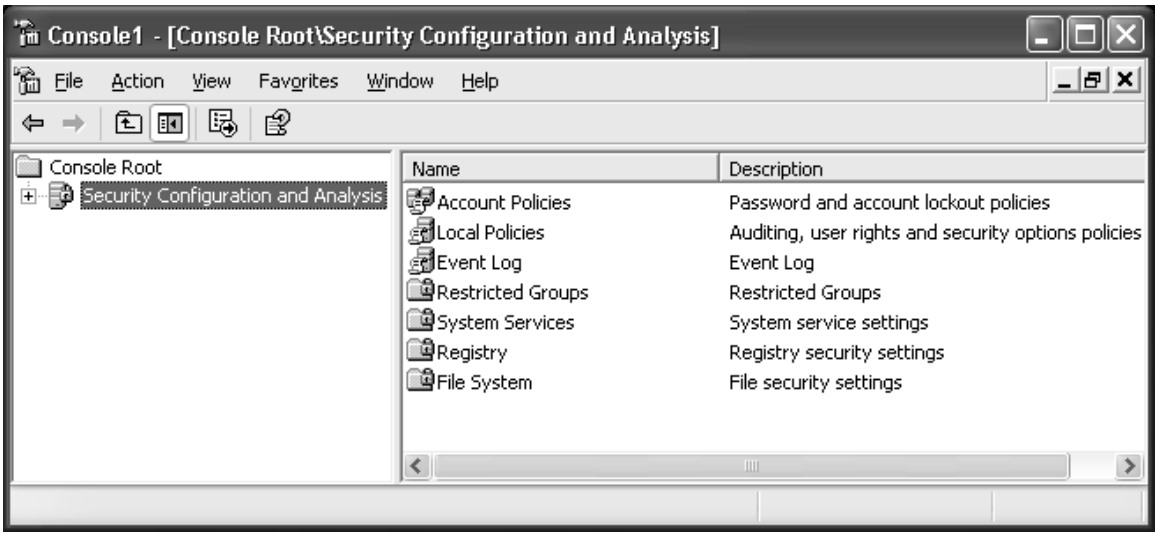


Figure E-5. Analysis Objects

E-3.7.6 To configure your computer:

E-3.7.6.1 Right-click on the Security Configuration and Analysis object in the left window.

E-3.7.6.2 Select "Configure Computer Now."

E-3.7.6.3 Enter "C:\temp\scan\srr.log" for the log name in the "Error log file path" window and click OK.

E-3.7.6.4 Reboot the workstation.

E-3.8 Gold Disk Initial Results.

E-3.8.1 Log into the workstation and ensure Windows functionality.

E-3.8.2 Follow the procedures outlined in Table E-2, to use the Gold Disk and verify the security settings.

E-3.8.3 Record the results of the Gold Disk scan as the before results.

E-3.9 Application Installation. The following procedure is general guidance to install the vendor specific management application for the SUT. Note: Any time a failure occurs and a setting is changed, this must be documented. If it is a security setting, this will also be documented as a finding.

E-3.9.1 Install any supplemental applications required to run the management application, .NET, Adobe Reader, etc.

E-3.9.2 Use the Vendor's Procedure to install the management application.

E-3.9.3 Configure the application as needed.

E-3.9.4 Perform a functionality test of the management application.

Note: If the system is fully functional proceed to 8.5.

E-3.9.4.1 Back off any security settings, one item at a time, until

full functionality is reached.

E-3.9.4.2 Document any changes to the workstation.

Note: Any time a failure occurs and a setting is changed, this must be documented. If it is a security setting, this will also be documented as a finding.

E-3.10 Gold Disk After Results.

E-3.10.1 Log into the workstation and ensure Windows functionality.

E-3.10.2 Follow the procedures outlined in Table E-2 to use the Gold Disk and verify the security settings.

E-3.10.3 Record the results of the Gold Disk scan as the after results.

E-3.10.4 Document the differences between the before results and after results on the findings report and the DIACAP scorecard.

E-4 POST-TEST. During Post-Test, the IATT generates the IA Assessment Draft Findings Report. The vendor provides feedback and mitigations for findings that cannot be resolved during testing.

E-4.1 Results. The following sections give instructions on how to use the .XML file that was generated from the Gold Disk and SRR script to review the findings for the components of the SUT.

E-4.2 SRR Results. Select the following four files from the DISA Gold Disk, Disk 1 (Engine), copy and save on the SRR .XML file:

- GoldDiskReports.htm
- MROnly_VMS6_Display.xslt
- NROnly_VMS6_Display.xslt
- VMS6_Display.xslt

Launch the GoldDiskReports.htm file, and it will appear in your browser with three buttons at the top. The message shown in Figure E-6 will display at the top of your screen.

Figure E-6. IE Warning Message

Click on the message to launch the pop-up menu shown in Figure E-7.

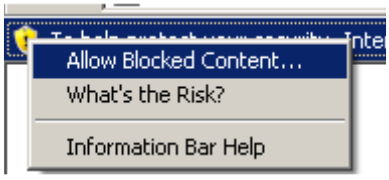


Figure E-7. IE Message Box

Click Allow Blocked Content. The dialog box shown in Figure E-8 will display asking to confirm the operation. Click Yes to proceed.

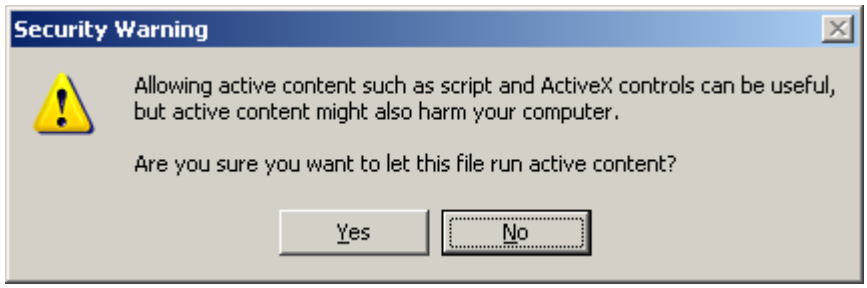


Figure E-8. IE Dialog Box

Note: This method only allows the content of the page to be unblocked for this session; it will not permanently set anything once the browser is closed. Repeat the process to view the reports again.

E-4.3 Gold Disk Results. The newest version of the Gold Disk has the ability to generate human-readable reports from a given asset. These reports use a combination of .HTM, .XML, and .XSLT files to give a viewable and printable report that shows the evaluated posture of an asset. There are three different reports:

- Standard Asset Posture Report (VMS6_Display.xslt)
- Manual Review Only Vulnerabilities Report (MROnly_VMS6_Display.xslt)
- Non-Reviewed Only Vulnerabilities Report (NROnly_VMS6_Display.xslt)

These reports are used in conjunction with .XML, which will be created by running the Gold Disk Version 2.0. It is important to have run the Gold Disk and evaluated your asset before generating any of these reports. To use the Status Specific Reports (e.g., one that allows filtering between Manual Review (MR) and Not Reviewed (NR)), invoke the report with the default name.

A different name can be used to save it and can be renamed back to the default to use the status specific reports. After saving it, navigate to the Program Compact Disc (CD) from the Gold Disk Set.

This will be the same CD from which the Gold Disk is executed. It will contain a list of files that should look similar to Figure E-9.

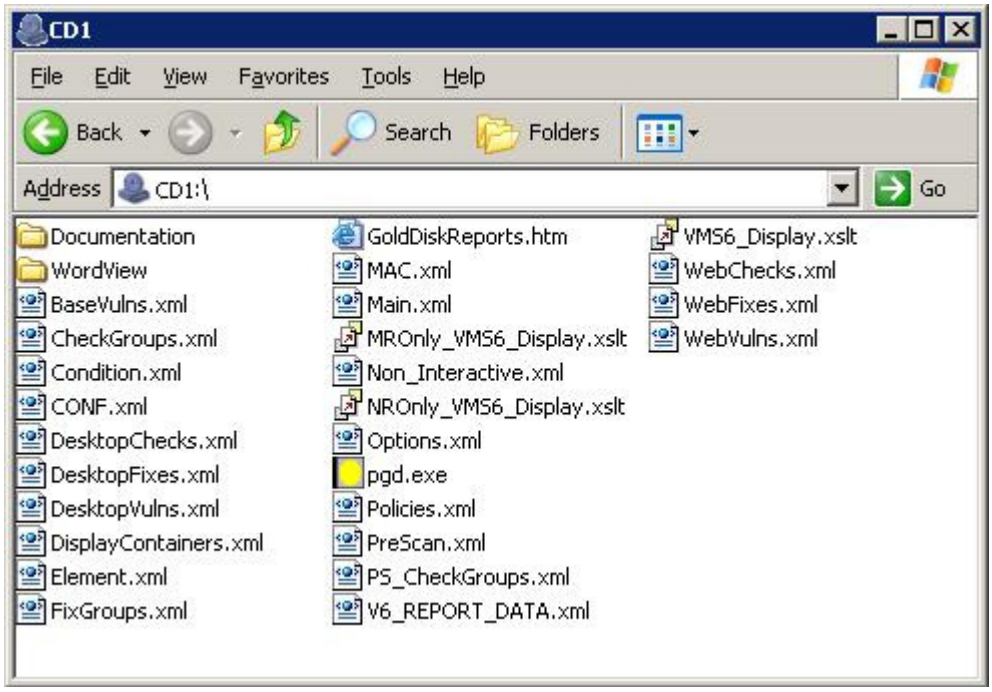


Figure E-9. Explorer Window

Select the following four files and copy them to where you saved the VMS6X.XML file:

- GoldDiskReports.htm
- MROnly_VMS6_Display.xslt
- NROnly_VMS6_Display.xslt
- VMS6_Display.xslt

Launch the GoldDiskReports.htm file, and it will appear in your browser with three buttons at the top. The message shown in Figure E-10 will display at the top of your screen.

Figure E-10. IE Warning Message

Click on the message to launch the pop-up menu shown in Figure E-11.

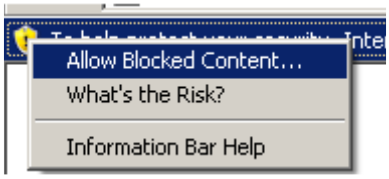


Figure E-11. Message Box

Click Allow Blocked Content. Dialog box will appear as shown in Figure E-12, asking to confirm the operation. Click Yes to proceed.

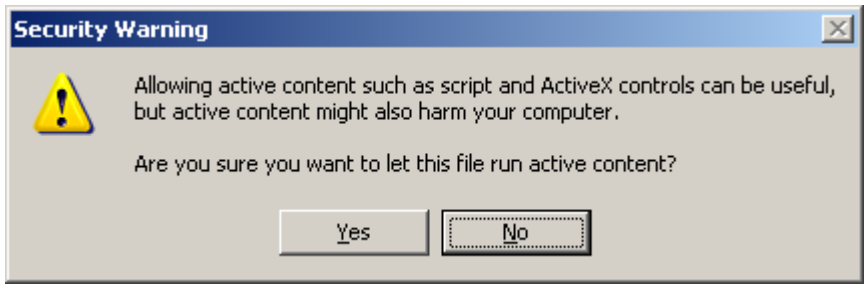


Figure E-12. Dialog Box

Note: This method only allows the content of the page to be unblocked for this session; it will not permanently set anything once the browser is closed. Repeat the process to view the reports again.

Three buttons are presented, as shown in Figure E-13, to allow the user to select a specific report.

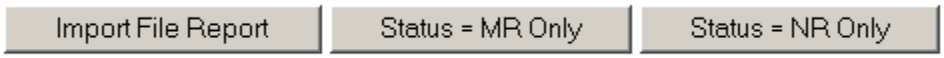


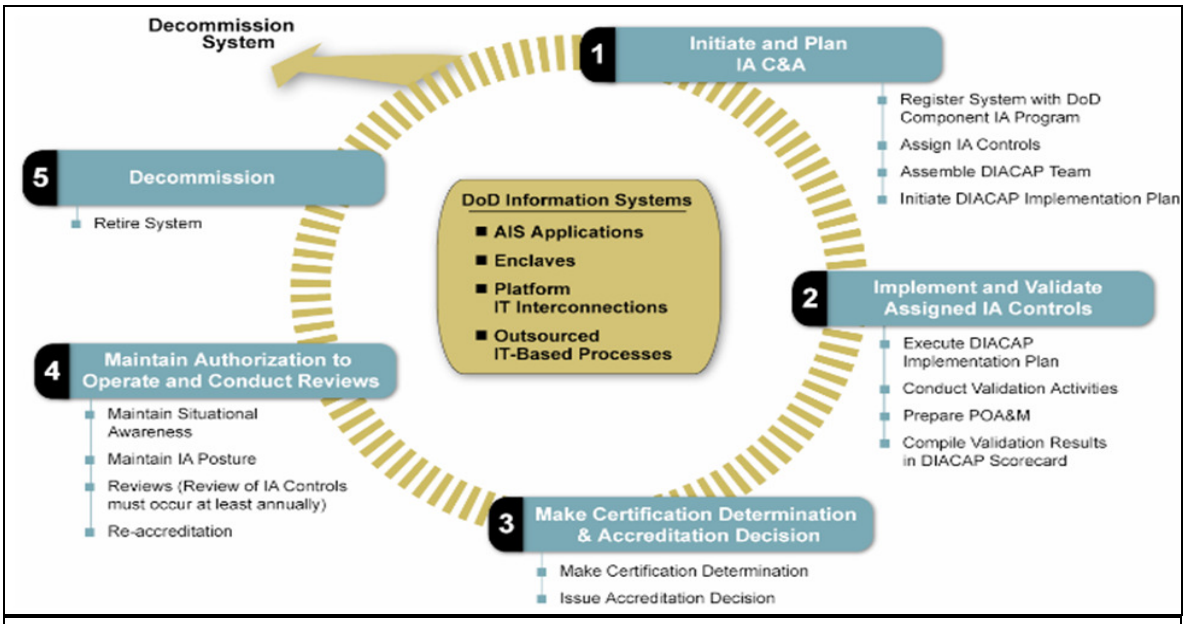
Figure E-13. Reporting Selection Buttons

Each of these buttons corresponds to one of the reports.

E-4.4 Checklists Results. Since this is a manual process, this report is already in a readable format.

E-5 DoD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) PACKAGE

The DIACAP package consists of a product from the beginning of its development until its decommission. The Joint Interoperability Test Command (JITC) IATT will support the DIACAP package through the first two stages of its lifecycle and will prepare site installations for the DIACAP package lifecycle of a vendor's DSN APL product. Figure E-14 shows the DIACAP lifecycle.

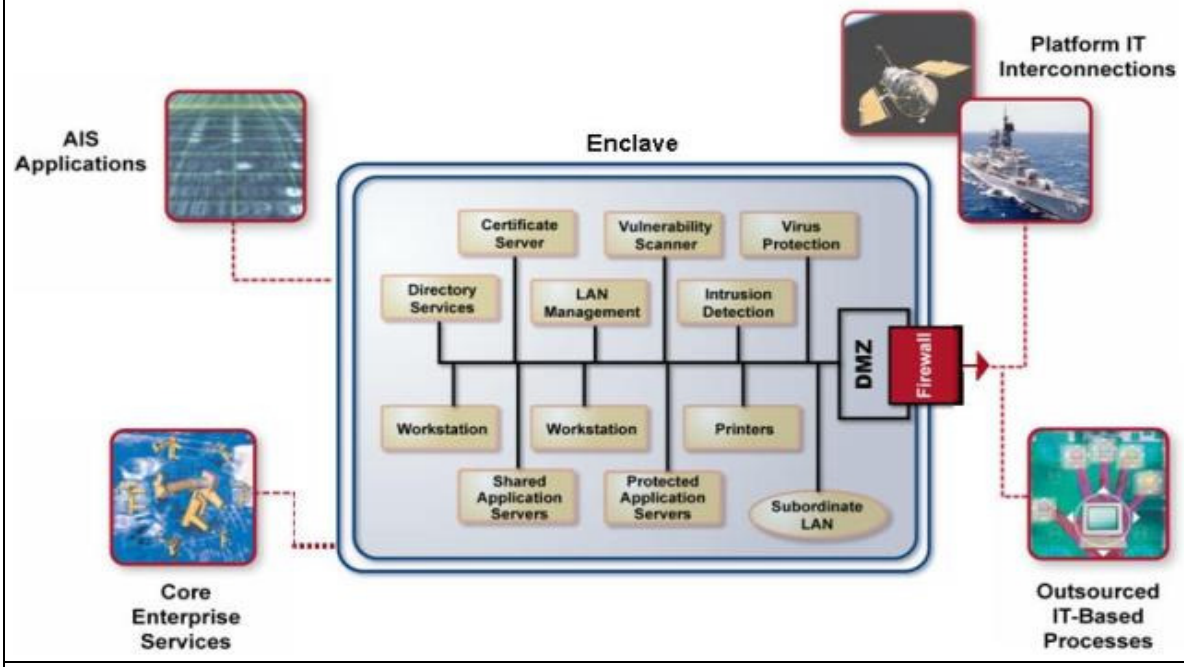


LEGEND:

AIS	Automated Information System	IA	Information Assurance
C&A	Certification and Accreditation	IT	Information Technology
DIACAP	DoD IA Certification and Accreditation Process	POA&M	Plan of Action and Milestones
DoD	Department of Defense		

Figure E-14. DIACAP Lifecycle

E-5.1 DoD Information Systems. All DoD Information Systems are divided into one of four portfolios, as shown in Figure E-15. The JITC IATT supports testing of many elements, either components of a system or complete systems for the warfighter.



LEGEND:

AIS	Automated Information System	IT	Information Technology
DMZ	Demilitarized Zone	LAN	Local Area Network
DoD	Department of Defense		

Figure E-15. DoD Information Systems

E-5.2 Accreditation Steps

E-5.2.1 Initiate and Plan IA Certification and Accreditation (C&A).

The DIACAP registration is the activity by which DIACAP-related elements and system-unique attributes of the DoD information system are made visible to the governing Component IA Program for the purpose of tracking management indicators and for Federal Information Security Management Act (FISMA) reporting. Registration commences a dialog between the DoD information system and the governing DoD Component IA Program that continues until the DoD information system is decommissioned.

The set of information gathered during system registration is referred to as the Sesssion Identification Profile (SIP), which becomes part of the DIACAP Package for the information system and is maintained throughout the system's lifecycle. The SIP identifies the minimum data requirements, plus explanations, for registration. Typically, this information can be found in program/project documentation, such as the initial capabilities document, system requirements/specifications, architecture and design documents, etc.

The DIACAP Implementation Plan (DIP) contains both the strategy for implementation along with the current implementation status of assigned IA Controls for

a system. The plan is part of the DIACAP Package used by both the certifying authority and the designated accrediting authority for accreditation, and it should be consistent with the program schedules.

The DIP should contain the following, minimum information:

- Assigned IA Controls - inherited and implemented
- Implementation Status
- Responsible entities
- Resources
- Estimated completion date for each IA Control.

E-5.2.2 Implement and Validate Assigned IA Controls. Government Accountability Office (GAO) audits, Inspector General (IG) audits, and other reviews or events, such as an annual security review or compliance validation, identifies those DoD information systems that are found to be operating in an unacceptable IA posture with a current Authority to Operate (ATO). The GAO prepares a Plan of Action and Milestones (POA&M). The POA&M identifies tasks to remediate any known vulnerabilities in a program or system. The POA&M addresses the following:

- Why the system needs to operate
- Any operational restrictions imposed to lessen the risk during the interim authorization
- Specific corrective actions necessary to demonstrate that all assigned IA Controls have been implemented correctly and are effective
- The agreed-upon timeline for completing and validating corrective actions
- The resources necessary and available to properly complete the corrective actions

This section provides the instructions for filling out both the System-level Information Technology (IT) security POA&M and the Component-level IT security POA&M.

E-5.2.2.1 IA Controls – Confidentiality. The IA Controls that are applicable to Real Time Services (RTS) Internet Protocol Vulnerability Testing include the following for confidentiality:

- **Specified Robustness (DCSR-2) – Medium.** At a minimum, medium-robustness Commercial-Off-The-Shelf (COTS) IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the Information Assurance Task Force (IATF). Any COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems that are

already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.

- **Individual Identification and Authentication (IAIA-1).** The DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login Identification (ID)) and password. For systems using a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive eight-character mix of uppercase letters, lowercase letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.

- **Encryption for Confidentiality (ECCT-1).** Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using National Institute of Standards and Technology (NIST)-certified cryptography (see also DCSR-2).

- **Conformance Monitoring and Testing (ECMT-1).** Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IA Vulnerability Alerts (IAVA) or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.

- **Physical Security Testing (PEPS-1).** A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.

E-5.2.2.2 IA Controls – Integrity. The IA Controls that are applicable to RTS Internet Protocol Vulnerability Testing include the following for integrity:

- **Non-Repudiation (DCNR-1).** The NIST Federal Information Processing Standard (FIPS) 140-2 validated cryptography (e.g., DoD Public Key Infrastructure (PKI) class 3 or 4 token) is used to implement encryption (e.g.,

Advanced Encryption Standard (AES), 3 Data Encryption Standard (DES), DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g.,Digital Signature Algorithm (DSA), Rivest, Shamir, and Aldeman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and hash (e.g., Secure Hash Algorithm (SHA)-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.

- **Software Quality (DCSQ-1).** Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.

- **Transmission Integrity Controls (ECTM-2).** Good engineering practices with regards to the integrity mechanisms of COTS, Government-off-the-Shelf (GOTS), and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks. Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).

E-5.2.2.3 IA Controls – Availability. The IA Controls that are applicable to RTS Internet Protocol Vulnerability Testing include the following for availability:

- **Ports, Protocols, and Services (DCPP-1).** The DoD information systems comply with DoD ports, protocols, and services guidance. Any Automated Information System (AIS) applications, outsourced IT-based processes, and platform IT identify the network ports, protocols, and services they plan to use as early in the lifecycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.

- **Vulnerability Management (VIVM-1).** A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

E-5.2.3 Make Certification Determination & Accreditation Decision. A Certification Authority (CA) representative determines certification and accreditation. The CA representative is an active member of the DIACAP Team, continuously

assessing and guiding the quality and completeness of DIACAP activities, tasks, and the resulting artifacts. Certification considers the following:

(1) The IA posture of the DoD information system itself. That is, the overall reliability and viability of the information system plus the acceptability of the implementation and performance of IA mechanisms or safeguards that are inherent in the system itself; and,

(2) How the system behaves in the larger information environment, e.g., does it introduce vulnerabilities to the environment, does it correctly and securely interact with information environment management and control services, and is its visibility to situational awareness and network defense services adequate.

E-5.2.4 Maintain ATO and Conduct Reviews. The Information Assurance Manager (IAM) provides an annual written statement to the Designated Approving Authority (DAA) and the CA. The review is based on all IA Controls and testing of selected IA Controls as required by FISMA. The review either confirms the effectiveness of assigned IA Controls and their implementation or recommends changes. The CA and DAA review the IAM statement, consider mission and information environment indicators, and determine a course of action.

E-5.2.5 Decommission. Decommission is defined as a DoD information system is removed from operation. When a system is decommissioned, a number of IA-related events are required. Those events are relative to the disposition of DIACAP registration information, system-related data or objects in Global Information Grid (GIG) supporting IA infrastructures, core enterprise services such as key management, identity management, service management, privilege management, policy management, and discovery, as discussed in DoD Instruction (DoDI) 8500.2.

The program manager should coordinate with DoD governing GIG activities, as appropriate, to identify and apply the necessary decommissioning requirements to eliminate the functional or military capabilities of systems. Decommissioning requirements and procedures change over time as the GIG enterprise information environment changes. The DIACAP Configuration Control Manager maintains and publishes the procedures in the DIACAP Knowledge Service.

E-6 REAL TIME SERVICES IA DERIVED REQUIREMENTS

The following tables are derived from the Defense Information System Network (DISN) Real Time Services Generic System Requirements, Appendix D, Video and Video over Internet Protocol (VVoIP) IA Unified Capabilities Requirements (UCR) document and are provided to assist the reader in understanding the origin of the requirements. Threats and countermeasures for VVoIP IA requirements are a combination of the different functions created to meet the requirements of a particular type of appliance. For the purposes of this UCR 2008, the requirements are levied on the individual appliance, as applicable, to secure the entire system. Features and capabilities are conditional requirements and not considered critical for DoD mission support based on DoD policies. It is understood that the IA Architecture provides a high-level description of how the security services are applied to the system and how the appliances interact in a secure manner. In addition, understanding that the appropriate STIG will further clarify how the IA Architecture and requirements are implemented on the appliance. Table E-6 below shows the appliance types.

Table E-6. Types of Appliance Components Used

Acronym	Appliances
MFSS	Multifunction Softswitch
MFS	Multifunction Switch
EO	End Office
TS	Tandem Switch
LSC	Local Session Controller
SMEO	Small End Office
PBX1	Private Branch Exchange 1
SS	Softswitch
EBC	Edge Boundary Controller
MG	Media Gateway
BC	Border Controller
EI	End Instrument
LS	LAN Switch
R	Router

E-6.1 VVoIP IA Requirements Test Matrix. The information contained in the Tables E-7 through E-13 constitutes the VVoIP IA Requirements Test Matrix. This matrix is used to test products considered for inclusion in the DSN APL.

E-6.2 VVoIP IA UCR. All requirements are derived from the 39 documents and instructions referenced in section 2 of DISN Real Time Services Generic System Requirements, Appendix D, VVoIP IA UCR. The requirements are divided into six sections: General, Authentication, Integrity, Confidentiality, Non-Repudiation, and Availability. The Tables E-7 through E-13 show the requirements for the six sections.

There are two categories for the systems affected by each requirement which are required and conditional.

"REQUIRED" are requirements that have features and capabilities considered necessary for a particular switch type for DoD. The word "REQUIRED" or the term "MUST" or "SHALL" means the definition is an absolute requirement of the product. The phrase "MUST NOT" or "SHALL NOT" means the definition is a complete exclusion of the item. The word "RECOMMENDED" means the reference is given as guidance and will be tested but may not be held against the vendor as a requirement.

"CONDITIONAL" are conditional requirements that have features and capabilities that are not considered critical for DoD or to support DoD policies. However, it should be recognized that such features do have value for some users or for specific operations. To ensure interoperability and consistency of the Assured Services (AS) across all platforms, these features and capabilities are specified with set parameters. If these features and capabilities are provided, the Unified Capabilities (UC) product shall perform and meet the requirements as identified in UCR 2008. The word "CONDITIONAL" or the term "MAY" means an item is optional. The word "RECOMMENDED" means the reference is given as guidance and will be tested but may not be held against the vendor as a requirement.

Table E-7. General Requirements

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
1	**Section:** General **ID:** 1 All IA and IA-enabled IT products shall be capable of being configured in accordance with all applicable DoD approved security configuration guidelines (i.e., STIGs). **Reference:** UCR 5.4.6.2	**Required:** MFSS,MFS, SS, LSC, MG, EBC, R, LS, TS, SMEO, and PBX1	1. Conduct an analysis of the system. 2. Verify accuracy of diagram delineating each component, operating system, firmware version, application version, and test boundaries. 3. Ensure applicable STIG and security requirements have been noted and applied to the system. 4. Note all access points and applications used to manage the system. 5. Evaluate each access point in accordance with the VVOIP IA Requirements Test Plan.	CAT I	
	IA Control: DCAS-1, DCCS-2, DCSD-1, and ECSC-1 **Site Responsibility:** EBCR-1	**Origin:** DoD Directive 8500.1 (4.18, 4.14.3, and 4.17); VoIP STIG (0020, 0103, 0140, 0165, 0250, 0280, 0295, 0330, 0340, and 0360); and DRSN STIG (P43 and 45)			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
2	**Section:** General **ID:** 1a. VVoIP shall be dedicated to VVoIP functions. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, and EBC	Verify that VVOIP appliances are dedicated for VVOIP functions only.	CAT II	
	IA Control: DCHW-1 **Site Responsibility:** EBCR-1	**Origin:** VoIP STIG 0270, NSA 2.3.2, and DRSN STIG 5.1.2			

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
3	**Section:** General **ID**: 1.b VVoIP appliances shall only have applications or routines that are necessary to support VVoIP functions. Note: The disabling or deletion of applications or routines via hardware or software mechanisms shall satisfy this requirement. For example, if an appliance by default is installed with a web browser and the 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. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Ensure that VVOIP appliances contain applications that are used for VVOIP purposes only. 2. If an VVOIP appliance contains applications that are not used for VVOIP purposes, verify it is removed in accordance with VVOIP requirements. 3. Browse to the main folders using the system's folder browser, (e.g., Program Files, /bin, etc.) 4. Using best judgment, question any suspected unnecessary software. If relevant, the files should remain.	CAT II	
	IA Control: DCFA-1	**Origin:** NSA 2.3, 2.3.1, and DRSN STIG 5.1.2			
	Site Responsibility: COEF-2				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
4	**Section:** General **ID:** 1.c Software patches shall only be installed if they originate from the system manufacturer and are applied in accordance with manufacturer's guidance. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	Verify that the patches installed are compliant with the manufacturer's guidance.	CAT II	
	IA Control: DCIT-1, DCMC-1, and DCSL-1	**Origin:** VoIP STIG 0281			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
5	**Section:** General **ID:** 1.c.1 The system shall only accept automatic software updates if they are cryptographically signed by the software vendor. Note: It is assumed that manual updates will be validated and authorized by administrator prior to installation. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Verify that automatic updates to the system are validated before installation. 2. Ensure that the system is required to validate any updates before loading into the system.	CAT III	
	IA Control: DCNR-1 and ECSD-2	**Origin:** NSA 2.3.1 and 2.3.5			

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
6	**Section:** General **ID:** 2 If the system 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 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. **Reference:** UCR 5.4.6.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	If the system uses software that is no longer supported, verify that the system covers the software under the system's warranty.	CAT II	
	IA Control: DCPD-1 and DCMC-1	**Origin:** DRSN STIG and others			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
7	**Section:** General **ID:** 2.a The systems shall only use open source software if all licensing requirements are met. Note: 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. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that the system has a valid license for all software used. 2. Verify that the system has a disclaimer in place on distributed copies of software.	CAT II	
	IA Control: DCPD-1 and DCMC-1	**Origin:** FSO clarification			

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
8	**Section**: General **ID**: 3 The system shall not use mobile code technologies (e.g., Java, JavaScript, VB Script, and ActiveX) unless the mobile code technology is categorized and controlled in accordance with policy. Note: The policy specifying categories and risks associated with mobile code is defined in [5]. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Ascertain if the system complies with all policies associated with the use of mobile code technology. 2. Ensure that the system complies with the IA UCR Reference 4.3.	CAT II	
	IA Control: DCMC-1	**Origin:** DoD Directive 8500.1 4.24 and CJCSI 6510.01D B.8c			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
9	**Section:** General **ID:** 4 If softphones are used in remote connectivity situations, the system shall be capable of supporting a VPN for VVoIP traffic from the PC to Enclave VPN access router/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. **Reference:** UCR 5.4.6.2	**Conditional:** EI	1. If softphones are used for remote connectivity, verify that the system is able to support a VPN for VVOIP traffic from PC to enclave VPN access router or node. 2. If softphones are used, verify data and VVOIP traffic are separated to a VLAN at the earliest point in the path.	CAT I	
	IA Control: EBRP-1 and EBRU-1	**Origin:** VVOIP Core Team and VoIP STIG 0130, 135, 0140, 0150, 0160, and NSA 2.4.6 - CAT I			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
10	**Section:** General **ID:** 5 The system shall be capable of being located in physically secure areas. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system is able to be placed in a secure area.	CAT II	
	IA Control: ECTC-1	**Origin:** VoIP STIG 0050 and NSA 2.1.3			
	Site Responsibility: PEEL-2, PEFD-2, PEFI-1, PEFS-2, PEHC-2, PEMS-1, PETC-2, PETN-1, and PEVR-1				

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
11	**Section:** General **ID:** 5.a The system shall be capable of enabling password protection of BIOS settings. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Determine if the system has the capability to enable a password protection before accessing the BIOS settings. 2. Proceed to BIOS. Ensure that BIOS is password protected.	CAT III	
	IA Control: IAIA-1	**Origin:** NSA 2.3.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
12	**Section:** General **ID:** 5.b The system shall be capable of disabling the ability to boot from a removable media. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Disable the option to boot from a removable media. This could be a setting in the system BIOS or a configuration file. 2. Attempt to boot the system from a removable media. If the system boots from a removable media, the system fails.	CAT III	
	IA Control: COEF-2	**Origin:** NSA 2.3.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
13	**Section:** General **ID:** 6 If the system has a speakerphone, the system shall be capable of disabling the speakerphone microphone. Note: Acceptable methods to meet this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter. **Reference:** UCR 5.4.6.2	**Conditional:** EI	If the system has a speakerphone, verify that it has the capability to disable the speakerphone by either unplugging it, or disabling it, by using a configurable software parameter.	CAT II	
	IA Control: ECND-2	**Origin:** NSA 2.4.1 and DRSN 5.3.1			

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
14	**Section:** General **ID:** 7 If the system is used in a sensitive area where National Security Systems (NSS) are employed and/or within environments where National Security Information (NSI) is stored, processed, or transmitted, then the system shall be certified and accredited in accordance with the (TSG) 6, which is prepared by the (NTSWG). **Reference:** UCR 5.4.6.2	**Conditional:** EI	1. Confirm with the sponsor whether the system is used in a sensitive area where NSS systems are employed or NSI is stored. 2. TSG 6 applies.	CAT I	
	IA Control: DCFA-1 and DCCS-2	**Origin:** DRSN STIG 7.3 Note: Not in March 08 IA UCR. Taken from December 07 IA UCR.			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
15	**Section:** General **ID:** 8 The system shall be capable of using a static Internet Protocol (IP) Address. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	Verify that the system uses a static IP address or is capable of it. 1. Determine the IP address of the system. 2. If DHCP is being used, note the IP address and configure the system with a static IP that was noted.	CAT I	
	IA Control: DCSD-1	**Origin:** NSA 2.4.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
16	**Section:** General **ID:** 9 The system shall only connect to the PSTN or coalition networks using PRI and/or CAS. Note: This precludes the exchange of SS7 or IP VVOIP signaling (and IP VVOIP media) information between the PSTN or coalition networks. **Reference:** UCR 5.4.6.2	**Required:** MFSS, SS, and LSC	Site Responsibility	CAT I	
	IA Control: EBCR-1	**Origin:** VVOIP Core Team Decision			

Table E-7. General Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
17	**Section:** General **ID:** 10 If the system uses a Microsoft Windows based operating system, the system shall support the installation and operation of the DoD mandated Host Based Security System (HBSS). Note: The DoD currently has an enterprise wide license for McAfee's ePolicy Orchestrator (ePO) server, Host Intrusion Prevention System agent, and several associated agent applications. HBSS is being deployed by all C/C/S/As to all Windows based servers and workstations. **Reference:** UCR 5.4.6.2	**Conditional:** MFSS, SS, LSC, MG, EBC, EI	1. Verify the installation and operation of a system HBSS, or at a minimum, verify an enterprise wide HBSS (McAffee ePO agent server).	CAT II	
	IA Control: ECID-1	**Origin:** Windows STIG 1.025			

LEGEND:

AIS	Automated Information System
BIOS	Basic Input/Output System
CAS	Channel Access Signaling
CAT	Category
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COEF	Continuity Identification of Essential Functions
DCAS	Design Configuration Acquisition Standards
DCCS	Design Configuration Configuration Standards
DCFA	Design Configuration Functional Architecture of AIS Applications
DCHW	Design Configuration Hardware Baseline
DCIT	Design Configuration IA for IT Services
DCMC	Design Configuration Mobile Code
DCNR	Design Configuration Non-repudiation
DCPD	Design Configuration Public Domain Software Controls
DCSD	Design Configuration Security Documentation
DCSL	Design Configuration System Library Management Controls
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DRSN	Defense Red Switch Network
EBC	Edge Border Controller
EBCR	Enclave Boundary Defense Connection Rules
EBRP	Enclave Boundary Remote Privileged
EBRU	Enclave Boundary Remote User
ECID	Enclave Computing Intrusion Detection
ECND	Enclave Computing Networking Device
ECSC	Enclave Computing Environment Security Configuration Compliance
ECTC	Enclave Computing Technical Control
EI	End Instrument
FSO	Field Security Officer
HBSS	Host Based Security System
IA	Information Assurance
IAIA	Identification Authentication Individual Identification and Authentication
ID	Identification
IP	Internet Protoco
IT	Information Technology
LS	Local Area Network Switch
LSC	Local Session Controller
MFS	Multi-Function Switch
MFSS	Multifunction Softswitch
MG	Media Gateway
NSA	National Security Agency
NSI	National Security Information
NSS	Network Security Services
NT	New Technology
NTSWG	National Telecommunications Security Working Group
PBX1	Private Branch Exchange 1
PC	Personal Computer
PEEL	Physical Environmental Emergency Lighting
PEFD	Physical Environmental Fire Detection
PEFI	Physical Environmental Fire Inspection
PEFS	Physical Environmental Fire Suppression
PEHC	Physical Environmental Humidity Controls
PEMS	Physical Environmental Master Switch
PETC	Physical Environmental Temperature Controls
PETN	Physical Environmental Control Training
PEVR	Physical Environmental Voltage Regulators
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
R	Router
SMEO	Small End Office
SS	Softswitch
SS7	Signal System 7
STIG	Security Technical Implementation Guidelines
TS	Tandem Switch
TSG	Telephone Security Standard
UCR	Unifed Capabilities Requirements
VB	Visual Basic
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VVoIP	Voice and Video Over Internet Protocol

Table E-8. Authentication

Test Case	Requirement	System Affected	Test Procedure(s)	Risk	Result(s)
18	**Section:** Authentication **ID:** 1 The system shall be capable of having warning banners on all systems management ingress ports accessed by administrators or by users as part of a human-to-machine interface for the purpose of network management. The banner shall function in the following manner: **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	At each ingress, check that a warning banner is displayed at the time of the login. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: ECWM-1	**Origin:** DoDD 8500.1 4.23; CJCSI 6510.01D section 12; OAM&P IA Requirements for public networks M48; IATP GR-815 CORE R-83[51}, R-84[52]; DRSN STIG 6.2.7; Application Security and Development STIG 3.8.8			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
19	**Section:** Authentication **ID:** 1.a At the first point of entry, the system shall have the capability to display a warning message of up to 20 lines by 80 characters (1600 characters) in length. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the warning banner is not hard-coded and that the system has the capability to display a warning message of up to 20 lines by 80 characters in length.	CAT III	
	IA Control: ECWM-1	**Origin:** CJCSI 6510.01D section 12 and IATP GR-815 CORE R-85[53]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
20	**Section:** Authentication **ID:** 1.b As part of delivered software, the system shall be capable of providing an appropriate default message that warns against unauthorized access or use. Note: The default message can be configured during the installation process. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system provides a default message warning against unauthorized access. 2. At each ingress, establish a successful login and check whether there is a display of an appropriate default message that warns against unauthorized access.	CAT III	
	IA Control: ECWM-1	**Origin:** CJCSI 6510.01D section 12 and IATP GR-815 CORE R-86[54]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
21	**Section:** Authentication **ID:** 1.c The system banner shall be capable of being configured by authenticated and authorized personnel. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that authenticated and authorized personnel only may configure the system banner. 2. Login as a lower privileged user and attempt to modify the system banner file. The attempt should fail. 3. Login as administrator. Attempts at modifying the system banner file should succeed.	CAT II	
	IA Control: ECWM-1	**Origin:** CJCSI 6510.01D section 12			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
22	**Section:** Authentication **ID:** 1.d The system shall be capable of displaying the banner to the administrator or user prior to a login attempt to the system. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	At each ingress, check if a warning banner is displayed before the time of the login. If there is no warning banner, the system fails the test.	CAT II	
	IA Control: ECWM-1	**Origin:** CJCSI 6510.01D section 12			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
23	**Section:** Authentication **ID:** 1.e The system shall be capable of requiring that the administrator or user acknowledges the banner after the user login but prior to accessing system processes. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, and EBC	1. Ensure that the administrator or user is required to acknowledge the warning banner after the user has logged in but before accessing system processes. 2. If the acknowledgement to the banner is negative, ensure that the login process is halted and access denied.	CAT III	
	IA Control: ECWM-1	**Origin:** FSO recommendation			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
24	**Section:** Authentication **ID:** 1.e.1 The system shall record the acknowledgement in the audit log with the administrator or user name. Note: If the acknowledgement is an essential step in the successful login process, then it is sufficient to only log the completion of a successful login. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, and EBC	1. Verify in the audit log records the acknowledgement of the warning banner with the administrator or user name. 2. If the acknowledgement is an essential step in the successful login process, verify completion of a successful login. If these procedures are not met, the system fails this requirement.	CAT III	
	IA Control: ECWM-1	**Origin:** Application Security and Development STIG 3.8.8			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
25	**Section:** Authentication **ID:** 1.f The system shall be capable of displaying the following information upon successful access to the system: **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	If the application uses password authentication, try to login to the system Using an incorrect and correct password. Restart the application and login again using the correct password. After a successful login to the application, logout of the application and note the date and times for the last successful and unsuccessful logons. Refer to test cases 26 and 27. If these procedures are not met, the system fails this requirement.	CAT III	
	IA Control: ECAR-2	**Origin:** Application Security and Development STIG 3.15.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
26	**Section:** Authentication **ID:** 1.f.1 The date and time of the administrator's or user's last successful access to the system. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R and LS	Establish a successful login and check whether there is a display of the date and time of the last successful login of the administrator or user. If these procedures are not met, the system fails this requirement.	CAT III	
	IA Control: ECAR-2	**Origin:** Application Security and Development STIG 3.15.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
27	**Section:** Authentication **ID:** 1.f.2 The number of unsuccessful attempts by that user-ID to gain system access to the system (e.g., mistyped password) since the last successful access by that user-ID. **Reference:** UCR 5.4.6.2.1.1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Establish an unsuccessful login then log in correctly. Check whether there is a display of the date and time of the unsuccessful attempts made since the last login. If these procedures are not met, the system fails this requirement.	CAT III	
	IA Control: ECAR-2	**Origin:** Application Security and Development STIG 3.15.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
28	**Section:** Authentication **ID:** 1 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 being connected to. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. At a point of ingress typically used by the administrator, establish a login as the administrator. 2. Print the list of all user-ID attributes (such as role, privilege, etc.) that are not confidential. 3. Verify if there is any recurrence of user-IDs, but differences in other user attributes. If a recurrence is observed, the system fails the test.	CAT I	
	IA Control: IAGA-1, IAIA-1, and ECAD-1	**Origin:** VoIP STIG Vulnerability 12H; GR-815 CORE R3-2[219], R3-54[33], R-21[9]; and DRSN STIG 6.2.8.1.1			
29	**Section:** Authentication **ID:** 1.a The system 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. **Reference:** UCR 5.4.6.2.1.2	MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that passwords are not used as a primary means of granting privileges. 2. Confirm that the system does not use shared passwords between any administrator and user or for any ACL, soft certificate, or privilege.	CAT I	
	IA Control: ECAN-1, ECPA-1, and ECLP-1	**Origin:** CJCSM 6510.01 C-26.3; VoIP STIG Vulnerability 12A, 12D; and GR-815 CORE R3-100[65]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
30	**Section:** Authentication **ID:** 1.b The system shall be capable of ensuring that all users and customer passwords are used in a secure manner. Note: This requirement is for user/customer passwords to include passwords that are used for role-based authentication. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify each user has his, or her, own login and password. 2. Verify that passwords are hidden on the screen during login procedure. 3. As administrator, access the password file(s) of the system and confirm that passwords are stored in an encrypted manner.	CAT I	
	IA Control: IAIA-2	**Origin:** VoIP STIG 0062			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
31	**Section:** Authentication **ID:** 1.b.1 The system shall be capable of automatically suppressing or blotting out the clear text representation of a password on the data entry device. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify displays of control panels suppress password (or other authentication information) during login procedures. If a password is viewable in plaintext, the system fails the test. 2. Attempt to login to every application that requires authentication and verify that the password input is not echoed back to the terminal.	CAT I	
	IA Control: IAIA-1	**Origin:** CJCSM 6510.01 C-A-2.6; OAM&P IA Requirements M52; GR-815-CORE R3-28[16], and DRSN STIG 6.2.8.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
32	**Section:** Authentication **ID:** 1.b.2 The system shall ensure that passwords are safeguarded at the confidential level for Sensitive but Unclassified systems. Note: All components of a system will be at the same sensitivity level. Note: The decision of how to properly safeguard the passwords is determined by the B/P/C/S DAA, but as a minimum, shall consist of encrypting the passwords during transit or while in storage using FIPS 140-2 commercial encryption. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. As administrator, access the password file(s) of the system and confirm that passwords are stored in an encrypted manner. 2. While monitoring (sniffing) the management traffic, confirm that passwords are passed in a secure manner from the control panel to the application. Note: The IPV test team will perform this test.	CAT I	
	IA Control: IAIA-1	**Origin:** CJCSM 6510.01 A.A.7.1.3 and C-A-2.8; VoIP STIG Vulnerability 12H and 121; OAM&P IA Requirements M23; and GR-815 CORE R3-26[14]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
33	**Section:** Authentication **ID:** 1.b.2.a The system shall be capable of storing access passwords (user and administrator) in a one-way encrypted form. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify the file storage of passwords (or other authentication information). If a password is viewable in plaintext, the system fails the test. 2. Create multiple users that have various lengths of passwords (suggest three users with password lengths of 8, 12, and 16 characters). 3. Examine the password file and confirm that the hashed passwords are the same length, indicating a one-way hash was performed on the passwords before storage.	CAT II	
	IA Control: IAIA-1	**Origin:** NSA 2.3.1; GR-815 CORE R3-26[14]; and DRSN STIG 6.2.8.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
34	**Section:** Authentication **ID:** 1.b.3 The system shall be capable of ensuring that passwords are not available in clear text to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords. However, encrypted passwords shall not be available to any other user. Note: It is recognized that it may not be realistic to make the encrypted password file unavailable to administrators. The administrator may be able to view the file's content, but would not be able to decipher the encrypted passwords. **Reference:** UCR 5.4.6.2.1.2	MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify file storage that contains the passwords (or other authentication information) of users are not in plaintext. 2. Confirm acceptable ciphertext and hashing is incorporated. If a password is viewable in plaintext, the system fails the test. 3. Using appropriate tools or utilities, attempt to decode the stored password. Note: The IPV test team will perform this test case.	CAT I	
	IA Control: IAIA-1 and ECCR-1	**Origin:** OAM&P IA Req M52, GR-815-CORE R3-27[15], R3-29[17], NSA 2.3.1, and DRSN STIG 6.2.8.1.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
35	**Section:** Authentication **ID:** 1.b.4 The system shall be capable of providing a mechanism for a password to be user changeable. This mechanism shall require re-authentication of user identity. Note: This requirement applies to factory set, default, or standard user-ID passwords. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Verify that the system provides the capability for each user or administrator to be able to change his or her own password.	CAT II	
	IA Control: IAIA-1	**Origin:** Application and Security Checklist V2r1, Section 3.5.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
36	**Section:** Authentication **ID:** 1.b.4.a The system shall be capable of ensuring that a new user password differs from the previous password by at least four characters. **Reference:** UCR 5.4.6.2.1.2	MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that the system does not allow at least four characters of the previous password to be reused. 2. Attempt to change an existing user password, such that the new password does not differ from the old password by at least four characters.	CAT II	
	IA Control: IAIA-1	**Origin:** Application and Security Checklist V2r1, Section 3.8.4.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
37	**Section:** Authentication **ID:** 1.b.4.b The system shall be capable of having a password history to prevent password reuse. The default shall be configurable and, shall be at least the past eight passwords or 180 days of password history. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Examine the system security configuration file and verify the default for most recently used passwords is a minimum of eight. 2. Login in seven times under the same user-ID with different passwords. On the eighth login, reuse a recently used password. If the system allows the reuse of the password, the system fails this test. 3. Login eight times under the same user-ID with different passwords. On the ninth login, reuse the first password used in the verification process. If the system allows the reuse of the first password, the system passes. 4. The test procedure should verify the reuse limit configured with a minimum default setting of eight and the passwords shall not be able to be reused within a 180-day time period. 5. Verify the system is capable of disallowing password reuse within a 180-day time period by checking the password configuration panel. 6. Attempt to change the password to a password that has been used within the last 180 days. If the system allows reuse of the password, the system fails the test.	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-38[25]; and DRSN STIG 6.2.8.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
38	**Section:** Authentication **ID:** 1.b.5 After a password is assigned to a human user, when that user establishes a session for the first time, the system shall be capable of prompting the user to change the password and deny the session if the user does not comply. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. As administrator, create a new user. 2. Login as the newly created user and confirm that the newly assigned passwords to new users are required to be changed on first login to continue a session. If it is not required to change the new user password on the first login, the system fails the test.	CAT II	
	IA Control: IAIA-1	**Origin:** OAM&P Req M44, GR-815-CORE R3-31[19], and DRSN STIG 6.2.8.1.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
39	**Section:** Authentication **ID:** 1.b.6 The system shall be capable of enforcing a configurable password aging interval (i.e., a password is required to be changed after a specified interval). Note: The exception to these requirements is found in the emergency access requirements in this UCR 2008 Sections 5.4.6, paragraph 1 (l) and (m). **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system provides a password aging setting capability for users and administrators. 2. Assign a specified time interval for password aging beyond the interval. 3. Advance the clock beyond the specifiable time period. 4. Attempt to login as the assigned user. The system should deny the login. If the denial occurs, go to 6. 5. If the denial does not occur, look for an administrative command to assign the password aging interval. If there is no feature for assigning the aging interval, the system fails the test. 6. If the system offers the feature for assigning the default password-aging interval, verify whether the assignment can be individualized on a user-ID basis. If not, the system fails the test. 7. Verify the system enforces a time interval for passwords to be changed. 8. Change the password. The system should have the ability to enforce a time interval password aging; otherwise, the system fails the test. 9. Advance the clock to a time interval beyond the authorized time interval. 10. Verify a warning appears stating that a password change is required within a specified time period not greater than 7 days. 11. Verify that a default is capable of being set and that the default period is not greater than 7 days. 12. Verify the administrator and user is still allowed a specified number of authorized logins before a new password is required.	CAT II	
	IA Control: IAIA-1	**Origin:** OAM&P IA Req. M20, M53, and M54; GR-815-CORE R3-32[20], R3-33[21], R3-34[22], CR3-35[22], CR3-36[23], and CR3-158[125]; VoIP STIG Vulnerability 12F; CJCSM 6510.01 C-A-2.7, and DRSN STIG 6.2.8.1.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
40	**Section:** Authentication **ID:** 1.b.6.a The system shall be capable of defining a system-wide default password aging interval. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system provides a system-wide password aging default setting capability. 2. Assign a specified time interval for password aging beyond the default interval. 3. Advance the clock beyond the specified time period. 4. Attempt to login as a user. The system should deny the login. If the denial occurs, the system passes the test. 5. If the denial does not occur, look for an administrative command to assign the system-wide default password-aging interval. If there is no feature for assigning the default-aging interval, the system fails the test.	CAT III	
	IA Control: IAIA-1	**Origin:** OAM&P IA Req M32 and GR-815-CORE R3-33[21]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
41	**Section:** Authentication **ID:** 1.b.6.b If the system supports long-lived sessions (i.e., two signaling appliances continuously connected), the system shall be capable of providing the capability to set the password ageing interval on a "per-user-ID-basis." Note: If, due to unforeseen circumstances, such as a power failure, the session is interrupted, an expired password may be a hindrance to re-establishing the session, especially if the appliance is not always attended by human users. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG,EBC, R, and LS	1. Verify the system enforces a time interval for passwords to be changed on a per user-ID basis. 2. Change the password. The system should have this feature; otherwise, the system fails the test. 3. Advance the clock to a time interval beyond the authorized time interval. 4. Verify a warning appears stating that a password change is required within a specified time period not greater than 7 days. 5. Verify that a default is capable of being set and that the default period is not more than 7 days. 6. Verify the user is still allowed a specified number of authorized logins before a new password is required. The default number of logins shall not exceed three.	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE CR3-36[22]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
42	**Section:** Authentication **ID:** 1.b.6.c If the system supports users, the system shall be capable of setting the password aging interval on a "per-user-ID" basis. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-34[22]	1. Verify that the system provides a password aging capability on an individualized per user basis. 2. Assign a specified time interval for password aging beyond the default interval. 3. Advance the clock beyond the specifiable time period. 4. Attempt to login as the user. The system should deny the login. If the denial occurs, the system passes the test. 5. If the denial does not occur, look for an administrative command to assign the password-aging interval. If there is no feature for assigning the password-aging interval, the system fails the test.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
43	**Section:** Authentication **ID:** 1.b.6.d The system shall notify the user a specified period of time before the password expiration. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE CR3-36[23]	1. Verify a warning appears stating that a password change is required within a specified time period not greater than 7 days. 2. Verify that a default is capable of being set and that the default period is not greater than 7 days. 3. Verify the administrator or user is still allowed a specified number of authorized logins before a new password is required.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
44	**Section:** Authentication **ID:** 1.b.6.e The system shall notify the user upon password expiration, but allow a specified additional number of subsequent logins within a specified time period before requiring a new password. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG,EBC, R, and LS **Origin:** DRSN STIG 6.2.8.1.1	1. When a user's password expires confirm that a warning appears stating that a password change is required within a specified time period. 2. Verify that a default is capable of being set. 3. Verify the user is still allowed a specified number of authorized logins before a new password is required.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
45	**Section:** Authentication **ID:** 1.b.6.e.1 The default for the number of subsequent logins shall not be greater than three. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** Application and Security Checklist V2r1, Section 3.8.6	1. Confirm that a default for subsequent logins is capable of being set and that the subsequent login allowance is not more than three sessions. 2. Configure a user's password to expire. 3. Login as the expired user. 4. Confirm that a password change warning is issued. Ignore the password change and log out 5. Login as the expired user an additional two times. 6. Confirm the password change warning is issued. Change the user password.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
46	**Section:** Authentication **ID:** 1.b.6.e.2 The default for the specified time period shall not be greater than 30 days. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that a default is capable of being set and that the default period is not greater than 30 days. 2. Create a new user with proper password. 3. Examine the new user security settings. 4. Confirm that the default value for changing the password does not exceed 30 days.	CAT III	
	IA Control: IAIA-1	**Origin:** DSN STIG Section 3.3.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
47	**Section:** Authentication **ID:** 1.b.6.f The system 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 login after password expiration. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system is not hard coded and variable parameters may be set to allow for flexibility in configuration. 2. Examine the system security configuration file and confirm that the password expiration notification parameter is present and changeable.	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-156 [123]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
48	**Section:** Authentication **ID:** 1.b.7 For a user updating a password, the system shall be capable of enforcing a configurable minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password). Note: This requirement discourages password "flipping" and is related to the history requirements stated previously. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Examine the system security configuration file and confirm there is a default minimum waiting period for changing a password.	CAT II	
	IA Control: IAIA-1	**Origin:** OAM&P M19 and M33; GR-815-CORE R3-38[24] and R3-37[24]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
49	**Section:** Authentication **ID:** 1.b.7.a The default for the minimum waiting period shall be 24 hours without administrator intervention. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS **Origin:** DRSN STIG 6.2.8.1.1	Verify the default minimum waiting period for changing a password without administrator intervention is 24 hours. If the system does not have a default capability, the system fails. Attempt to change the password as a regular user account. If the password can be changed the system does not meet the requirement for this check.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
50	**Section:** Authentication **ID:** 1.b.8. The system shall be capable of ensuring that all user-entered passwords meet the following complexity requirements (so it cannot be "easily guessable"): **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, EI and LS **Origin:** NSA 2.3.1 and DRSN STIG 6.2.8.1.1	Attempt to establish a password containing a minimum number of nine characters containing at least two characters from each of the four character sets: upper-case letters, lower-case letters, numbers, and special characters. Note: Password capabilities should be sufficiently robust and flexible to meet the local installation's requirements. The requirements for password complexities are constantly being adjusted to meet higher standards. If these procedures are not met, the system fails this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
51	**Section:** Authentication **ID:** 1.b.8.a The system shall be capable of ensuring that the password consists of a mix of minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters). Note: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.) Note: See the next requirement that is more stringent on certain users. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** Application and Security STIG Section 3.8.4.1	Attempt to establish a password containing a minimum number of 15 characters containing at least two characters from each of the four character sets: upper-case letters, lower-case letters, numbers, and special characters. If these procedures are not met, the system fails this requirement.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
52	**Section:** Authentication **ID:** 1.b.8.b The system shall be capable of ensuring that system security administrators, system administrators, and application administrator passwords consist of a mix of a minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters). NOTE: Special characters are characters on a keyboard typically located above the numbers (i.e., !, @, #, etc.). **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** NSA 2.3.1	1. For system security administrator(s), system administrator (s), and application administrator(s), attempt to establish a password containing a minimum of 15 characters, containing at least two characters from each of the four character sets: upper-case letters, lower-case letters, numbers, and special characters. 2. Verify password cannot be established if password complexity requirements are not met. Note: Password capabilities should be sufficiently robust and flexible to meet the local installation's requirements. The requirements for password complexities are constantly being adjusted to meet higher standards.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
53	**Section:** Authentication **ID:** 1.b.8.c The system shall be capable of ensuring that the password does not contain, repeat, or reverse the associated user-ID. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS **Origin:** NSA 2.3.1	1. Create a new user, "jode" 2. Assign the default password as Jode12345! 3. Confirm that the password assignment failed. 4. Assign a password of 12345Jode! 5. Confirm the password assignment failed. 6. Assign a password of 123Jode!45 7. Confirm the password assignment failed. Note: Password capabilities should be sufficiently robust and flexible to meet the local installation's requirements. The requirements for password complexities are constantly being adjusted to meet higher standards.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
54	**Section:** Authentication **ID:** 1.b.8.d The system shall be capable of ensuring that the password does not contain three of the same characters used consecutively. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS **Origin:** Application and Security Checklist V2r1, Section 3.8.4.1	1. Create a new user called popeye 2. Attempt to assign the password of spinachhh 3. Confirm the password assignment fails. 4. Attempt to assign the password of ssspinach 5. Confirm the password assignment fails. 6. Attempt to assign the password of spinnnach 7. Confirm the password assignment fails. 8. Attempt to assign the password of spinach. 9. Confirm the password assignment passes. Note: Password capabilities should be sufficiently robust and flexible to meet the local installation's requirements. The requirements for password complexities are constantly being adjusted to meet higher standards.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
55	**Section:** Authentication **ID:** 1.b.8.e The system shall be capable of ensuring that a "null" password is not possible. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Login as administrator and create a new user. 2. When prompted for a password to assign, complete the new user creation without a password. 3. Confirm that the new user creation fails.	CAT I	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.2.2.2, R3-16[41]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
56	**Section:** Authentication **ID:** 1.b.9 If passwords are generated by the system, the system passwords shall be capable of meeting the following requirements: **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. If the system does not generate its own passwords, this test is not applicable. 2. Have the system create a password. 3. Confirm that the password rules containing a minimum of 15 characters containing at least two characters from each of the four-character sets: upper-case letters, lower-case letters, numbers, and special characters. 4. Verify that system-generated passwords meet the same security standards for password complexity as self-generated passwords.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-43[30] -			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
57	**Section:** Authentication **ID:** 1.b.9.a System supplied passwords shall be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of system-generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified for user-entered passwords. **Reference:** 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, LS	1. Generate account passwords based off DoD password complexity. 2. Perform Brute Force and other password cracker applications against the system. 3. Mitigate the findings as required. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Application Security and Development STIG 3.8.4, 3.8.4.1, 3.8.4.2, & 3.8.4.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
58	**Section:** Authentication **ID:** 1.b.9.b The generated sequence of passwords shall have the property of randomness, i.e., consecutive instances shall be uncorrelated, and the sequence shall not display periodicity. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Verify that system generated passwords generate passwords in a random pattern. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Application Security and Development STIG 3.8.4, 3.8.4.1 & 3.8.4.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
59	**Section:** Authentication **ID:** 1.b.9.c If the "alphabet" used by the password-generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	If the system-supplied passwords use an alphabet other than English, verify password complexity requirements are enforced and the password does not depend upon the secrecy of the alphabet. Note: Password capabilities should be sufficiently robust and flexible to meet the local installation's requirements. The requirements for password complexities are constantly being adjusted to meet higher standards.	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE CR3-44[31]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
60	**Section:** Authentication **ID:** 1.b.10 The system 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). **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Login as an administrator and create two user-IDs. 2. Assign the same password to both of them. The system should allow this transaction. Otherwise it fails the test.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-25[13]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
61	**Section:** Authentication **ID:** 1.b.11 The system shall not permit passwords to be embedded in system defined access scripts or function keys. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify system cannot be accessed by function keys. 2. Verify that all software that is not essential for running the system does not exist. 3. Use IPV testing to verify that hidden ports are not available to access the system.	CAT II	
	IA Control: IAIA-1	**Origin:** Application and Security Checklist V2r1, Section 3.8.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
62	**Section:** Authentication **ID:** 1.b.12 The system shall have the capability to disable and enable the display of the "username of the last successful logon" feature. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Login as administrator and disable the display of the username of the last successful logon. 2. Login as a normal user and confirm that the display of username's last successful logon is not displayed. 3. As administrator, enable the display of the username of the last successful login. 4. Login as a normal user and confirm that the username of the last successful logon is displayed.	CAT III	
	IA Control: ECAR-1	**Origin:** GR-815-CORE R3-86[54]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
63	**Section:** Authentication **ID:** 1.b.13 The system shall have the capability to disable and enable the last successful logon message feature that tells the user the last successful and unsuccessful logon time and date. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, and MG	1. Login as administrator and disable the display of the last successful or unsuccessful login. 2. Login as a normal user and confirm that the last successful logon message is not displayed. 3. As administrator, enable the display of last successful login. 4. Login as a normal user and confirm that the last successful logon is displayed.	CAT III	
	IA Control: ECAR-1	**Origin:** GR-815-CORE R3-86[54]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
64	**Section**: Authentication **ID**: 1.b.14 If PINs are used for passwords, the system shall have a configurable parameter for the PIN length and the range shall be between four(4) and twenty (20) characters with a default of four (4). Note: All password requirements defined in this section apply to PINs when used as passwords. **Reference**: UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify if the system has the capability to use PINs as an access control measure. 2. Verify the system has configurable parameter to adjust PIN length between four and 20 characters. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Access Control in Support of Information Systems STIG: Section 3.4.3 & 3.5.5; DoDI 8500.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
65	**Section:** Authentication **ID**: 1.b.14.a If PINs are used for passwords, the system shall ensure that only numbers are allowed (i.e., no "#" or "*"). **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Ensure the system has the ability to generate PINs as passwords. 2. Attempt to create a PIN with a alphanumeric character. 3. If the system accepts the newly created PIN, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Access Control in Support of Information Systems STIG: Section 3.4.3 & 3.5.5; DoDI 8500.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
66	**Section:** Authentication **ID:** 1.c If PINs are employed for user identification (versus password), the system shall be capable of ensuring that only one individual is permitted to use an assigned PIN. Note: Since this can conflict with the preceding requirement, PINs (User-ID) must be assigned to users and they shall not be allowed to select their own PIN (User-ID). This requirement only applies when a PIN is used for user Identification without any other credential like a username or phone number. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	As an administrator at the access point, attempt to create two accounts using an identical PIN. If the system allows the creation of two or more identical PINs, the system fails this test.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE CR3-44[31], R3-4[2], OAM&P M43			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
67	**Section:** Authentication **ID:** 1.c.1 If PINs (User-ID) are used for user identification, the system shall have a configurable length between six (6) and twenty (20) characters and the default shall be 6. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify the system uses PINs for user identification. 2. Verify PIN configuration is adjustable between six (6) and 20, and the default is set to six. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Access Control in Support of Information Systems STIG: Section 3.4.3 & 3.5.5; DoDI 8500.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
68	**Section:** Authentication **ID:** 1.c.2 If PINs (User-ID) are used for the user identification, they 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. **Reference:** UCR 5.4.6.2.1.2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify the system uses PINs for user identification. 2. Generate user PIN's with alphanumeric characters. If letters or special characters are accepted, the systems fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** Access Control in Support of Information Systems STIG: Section 3.4.3 & 3.5.5; DODI 8500.2			

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
69	**Section: Authentication** **ID:** 1.d The system shall be capable of ensuring that all authorized users and customers have unambiguous user-IDs, such as MAC addresses or usernames, for identification purposes to support individual accountability, auditability, and access privilege. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	As a user and administrator at the access point, attempt to create a login name that is known to already exist on the system. If the system allows the creation of two or more identical login names, the system fails this test.	CAT II	
	IA Control: IAIA-1	**Original:** GR-815-CORE CR3-44[31], R3-4[2], OAM&P M43			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
70	**Section:** Authentication **ID:** 1.d.1 The system shall be capable of supporting the unambiguity of a user-ID. This implies that the system shall prevent an appropriate administrator from creating (e.g., by mistake) a user-ID that already exists. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	As an administrator at the access point, attempt to create two accounts using an identical login name. If the system allows the creation of two or more identical login names, the system fails this test.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-4[2]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
71	**Section:** Authentication **ID:** 1.e At any given instance of time, the system shall be capable of internally maintaining the identity of all user-IDs logged on at that time. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** ECAT-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-5[3], R3-6[4], and OAM&P M57	1. Establish a login as an administrator. If the system has other points of ingress, establish simultaneous logins as users at the other points of ingress. 2. Execute an appropriate command as the administrator to display the user-IDs that are concurrently logged on at the other ingresses. If the administrator does not have this capability, the system fails the test. 3. Continue by executing appropriate commands as the administrator to display the transactions that are being executed by other users who are concurrently logged on. If the administrator does not have this capability, the system fails the test.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
72	**Section:** Authentication **ID:** 1.e.1 The system shall be capable of associating a process that is invoked by a user or customer with the user-ID of that user. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-6[4]	1. Note the number of applications used on the control panel to manage, maintain, or configure the product. 2. Log on to each application and verify that each application requires a user-ID to log on to the application. 3. Check to see if the application on the control panel interconnects with switches, routers, or other peripherals. 4. If so, check to see that the user-ID and application used are recorded in the security log for each application or device visited. If not, each application, switch, router, or peripheral must require an individual logon procedure. 5. Verify the capability of the system to independently and selectively monitor (in real time) the actions of any one or more users logged in, based on individual user Identity and the application in use.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
73	**Section:** Authentication **ID:** 1.e.2 The system shall be capable of associating a process that is invoked by another process, with the ID of the invoking process. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system's capability to track what processes invoke other processes. 2. Logon to an appliance using a user-ID and password. 3. Note in the security log that access to the appliance in use has been recorded and the user-ID is noted. (Access to a device may be accomplished through an application, CLI, web interface, etc.) 4. If access to an appliance is through an application, select an application and log on using a user-ID and password. 5. Note in the security log that the user-ID and application in use are properly recorded. 6. If the application invokes the use of another application or process (printers, database management servers, web servers, etc.), check in the security log that the use of the application or service is recorded and can be associated with a userID. 7. Check in the security log that the use and activation of supporting applications or services are recorded and traceable to the initiator's user-ID. 8. Use the UNIX command 'ps –ef' or the Windows SysInternal Process Explorer to observe process IDs.	CAT III	
	IA Control: ECAR-2	**Origin:** GR-815-CORE R3-6[4]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
74	**Section:** Authentication **ID:** 1.e.3 The system shall be capable of associating an autonomous process (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. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system's capability to independently and selectively monitor the activities of an autonomous process. 2. Log on to an appliance with a user-ID and password. 3. Ensure that applications associated with the product are not in use (through visual inspection) and verify in the security log that there are no unaccounted applications in use. 4. Note the use of any applications that may be in use. 5. Launch an application that is present on the appliance. 6. Check in the security log that the launch of the new application has been recorded and is associated with a user-ID. 7. Check that the recording of the use of the application is distinguishable from autonomous processes that may be running or may be invoked. 8. If the application invokes the use of another application or process (printers, database management servers, web servers, etc.), check in the security log that the use of the application or service is recorded and can be associated with a User-ID. 9. Check in the security log that the use and activation of supporting applications or services are recorded and traceable to the initiator's user-ID.	CAT III	
	IA Control: ECAR-2	**Origin:** GR-815-CORE Section 3.2.1.1, R3-6[4]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
75	**Section:** Authentication **ID:** 1.f A system shall have the capability to disable (as distinct from deleting) a user-ID after a configurable specified time interval, if that user-ID has never been used during that time interval. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Create a new user-ID with a specifiable period of allowable inactivity. 2. Advance the system's clock beyond the allowable period of inactivity. 3. Verify whether the user-ID is disabled. If the user-ID is not disabled, the system fails the test.	CAT III	
	IA Control: IAAC-1	**Origin:** GR-815-CORE R3-7[220], R3-8[221] and DRSN STIG 6.2.8.1.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
76	**Section:** Authentication **ID:** 1.f.1 This capability shall be either an autonomous disabling of the user-ID by the system, or an alarm/alert generated by the system for an appropriate administrator who then, depending on the policy, may disable the user-ID by using appropriate commands. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Create a new user-ID with a specifiable period of allowable inactivity. 2. Advance the system's clock beyond the allowable period of inactivity. 3. Verify whether the user-ID is disabled. If the user-ID is not disabled, the system fails the test. 4. Verify whether the system has an alarm/alert that notifies an appropriate administer that the user has reached a time interval limitation that qualifies the user to be disabled. 5. Verify that the administrator has the capability to disable the identified user.	CAT II	
	IA Control: IAAC-1	**Origin:** Application and Security Checklist V2r1, Section 3.8.6			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
77	**Section:** Authentication **ID:** 1.f.2 A disabled login ID shall not be re-enabled by the user or another application user. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that only an administrator has the capability to re-enable a disabled user.	CAT III	
	IA Control: IAAC-1	**Origin:** Application and Security Checklist V2r1, Section 3.8.6			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
78	**Section:** Authentication **ID:** 1.g The system shall have the capability to configure the default time interval for disabling a user-ID that has not been used during that time interval. The default time interval shall be 90 days. In addition to disabling the user, the system shall be capable of sending an alert to the system security administrator. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. If the system does not have the capability of establishing a default time interval for user-ID inactivity this test case is not applicable. 2. Verify that default time interval is configurable. 3. Verify that the default time interval is 90 days. 4. Verify that a real-time alarm/alert is sent to the appropriate security administrator.	CAT III	
	IA Control: IAAC-1	**Origin:** GR-815-CORE R3-9[6] and OAM&P IA Req M55, M56			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
79	**Section:** Authentication **ID:** 1.h The system shall be capable of verifying that a specified user (e.g., administrator) is only connected to the system a configurable number of times. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAAC-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** OAM&P IA Req M45, M46	1. Note in the configuration management of the product the number of times a specified user may log onto the system is configurable. 2. Select, in the configuration management of the product, a specified number of times a specified user may be logged onto the system. 3. Logon to the system through a specified application and keep the session activated. 4. Activate another session on the same system and application. Do this until the number of allowed sessions of a specified user is exceeded as dictated by the setup in the configuration management. 5. Verify that when the number of configurable times a user may be connected to a system is exceeded, the system does not allow the new session.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
80	**Section:** Authentication **ID:** 1.h.1 An attempt for a specified user (e.g., administrator) to logon 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. **Reference:** UCR 5.4.6.2.1.2 **IA Control:** IAAC-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.4.5, CR3-87[55]	1. Select, in the configuration management of the product, a specified number of times a specified user may be logged onto the system. 2. Logon to the system through a specified application and keep the session activated. 3. Activate another session on the same system and application. Do this until the number of allowed sessions of a specified user is exceeded as dictated by the setup in the configuration management. 4. Verify that when the number of configurable times a user may be connected to a system is exceeded, the system does not allow the new session. 5. Verify that when the attempt to establish a session exceeds the number of sessions allowed, notification is sent to the NMS. This may be verified through observing the recording of the event in the security log as well as notification on the NMS station through alarms (sound, light, etc.), e-mails, or other applicable alerts.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
81	**Section:** Authentication **ID:** 1.i The system shall be capable of allowing the system security administrator to configure the number of consecutive failed logins for a user before the login procedure shall exit and end the attempted session. The number of times shall be between two and five and the default shall be three. NOTE: The exception to these requirements is found in the emergency access requirements (Sections 5.4.6, paragraph 1 (l) and (m). **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify whether the system security administrator is capable of configuring the number of consecutive failed login attempts before the login procedure shall exit and end the attempted session. 2. Verify the number of failed logon attempts is between two and five. 3. Verify that the default of number of failed login attempts is three. 4. At each ingress, attempt login with incorrect user-ID/authenticator combination. 5. After consecutive attempts, verify whether the system locks the session for a limited time (not more than 10 minutes) based on the configured amount of allowable failed login attempts. If these procedures are not met, the system fails this requirement	CAT II	
	IA Control: ECLO-1	**Origin:** GR-815-CORE, R3-76[44], R3-77[45], Rr3-82[50]; OAM&P IA Req M21, M49, M50, M51, M58; and NSA 2.3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
82	**Section:** Authentication **ID:** 1.i.1 The system shall be capable of immediately notifying the user of a failed login (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 correct). 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." **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. At each ingress, attempt to login with an incorrect user-ID. 2. Repeat the login attempt with a correct user-ID, but incorrect authenticator. 3. Check whether the system responds with a helpful message (e.g., "the user-ID is incorrect," or "the password is incorrect"). If there is a helpful message, the system fails the test.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-18[43], R3-78[46]; and OAM&P IA Req. M49			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
83	**Section:** Authentication **ID:** 1.i.2 The system shall be capable of allowing a locked-out user to be re-enabled by a configurable timer or manually by an application security administrator, a system administrator, or a system security administrator. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1 Verify in the configuration tables that a lockout duration is assignable and not hard-coded. 2. Verify that either the application security administrator, a system administrator, or a system security administrator may configure the timer. 3. At each ingress, attempt to login with an incorrect combination of user-ID and authenticator, if not, the system fails the test. 4. Check whether the system locks the session for a limited time, either on, or before, the second consecutive attempt with incorrect user-ID/authenticator combination, but not longer than the fifth such attempt.	CAT II	
	IA Control: ECLO-1	**Origin:** GR-815-CORE R3-79[47]; OAM&P IA Req. M58; and DRSN STIG 6.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
84	**Section:** Authentication **ID:** 1.i.2.a The default for the lockout duration shall be configurable and the default shall be 60 seconds when the threshold for incorrect user-entered information has been exceeded. (This is because longer delays can be used to temporarily disrupt the service by systematically locking out all input ports). **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Proceed to the software configuration portion of the system. 2. Verify that the system provides for configurable lockout durations. 3. Select a lockout duration interval. 4. Attempt to log on to the system with an improper user-ID or password. Ensure that the number of attempts exceeds the number of allowable logon attempts. 5. Record the interval of lockout duration and verify that it matches the selected time interval. 6. Verify in the system's configuration panel or tables that the default setting is 60 seconds when the threshold for incorrect user-entered information has been exceeded. 7. Ensure that 60 seconds is selected as the default setting. 8. Attempt to log on to the system with an improper user-ID or password. Ensure that the number of attempts exceeds the number of allowable logon attempts. 9. Record the time interval of the lockout and that the lockout duration is 60 seconds.	CAT II	
	IA Control: ECLO-1	**Origin:** GR-815-CORE R3-80[48], R3-81[49], and OAM&P IA Req. M58			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
85	**Section:** Authentication **ID:** 1.i.3 The system shall be capable of providing a mechanism to notify immediately (in real time) an administrator when the threshold for incorrect user-entered information is exceeded. **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Attempt to login with an incorrect user-ID/ authenticator combination, at each ingress. 2. Check whether the system raises an alarm and locks the session for a limited time, either on or before the second consecutive attempt, but not longer than the fifth attempt. 3. Verify the alarm notifies the administrator. If not, the system fails the test.	CAT II	
	IA Control: ECLO-1	**Origin:** GR-815-CORE R3-78[46]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
86	**Section:** Authentication **ID:** 1.i.4 When the threshold for incorrect user-entered information has been exceeded, the system shall not, as a default arrangement, suspend the associated user-ID. (This is because suspension of user-IDs can be used to systematically disable all user-IDs.) **Reference:** UCR 5.4.6.2.1.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Verify that when the threshold for incorrect user-entered information has been exceeded, the system does not, as a default arrangement, disable the associated user-ID.	CAT II	
	IA Control: ECLO-1	**Origin:** GR-815-CORE R3-82[50]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
87	**Section:** Authentication **ID:** 1 The system shall be capable of having different types of user's roles. Note: Section 5.4.5.2.1, User Roles, defines the different types of user roles. A vendor may rename the user roles as long as the requirements are met. The user roles are for the purposes of originating VVOIP sessions and for network management functions. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Confirm that the system can create a hierarchical structure of user privileges. 2. System administrators and users should have multiple privilege levels based on "role."	CAT I	
	IA Control: DCFA-1 and ECLP-1	**Origin:** CJCSI 6215.01B 15; OAM&P IA Req M24, M25; and GR-815-CORE R3-107[72], R3-145[112]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
88	**Section:** Authentication **ID:** 1.a The system shall be capable of having at least five types of user roles: system security administrator, system administrator, application administrator, privileged user, And an application user. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, and LSC	1. Create a new user on the system. The new user shall have, as a minimum, the access and permissions granted to that of an application user. 2. Note that the system is capable of adding or removing access and permissions from the created user default role. 3. Verify that access and permissions do not exceed those of an application user. If multiple applications are present in a system, the default user role must not exceed that of any of the application user roles. 4. Once the default user role has been created, attempt to execute actions beyond that of an application user. The default user role should not be allowed to execute actions beyond the default application user status.	CAT III	
	IA Control: DCFA-1 and ECLP-1	**Origin:** OAM&P IA Req. M25 and NSA 2.3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
89	**Section:** Authentication **ID:** 1.b The system shall be capable of having at least three types of user roles: A system security administrator, a system administrator, and an application administrator. **Reference:** UCR 5.4.6.2.1.3	**Required:** R, LS, EBC, and MG	Verify that the system supports at least three administrative roles to include a system security administrator, a system administrator, and an application administrator.	CAT III	
	IA Control: DCFA-1 and ECLP-1	**Origin:** OAM&P IA Req. M25 and NSA 2.3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
90	**Section:** Authentication **ID:** 1.c The system shall be capable of supporting at least three types of user roles: a system administrator, a privileged application user, and an application user. **Reference:** UCR 5.4.6.2.1.3	**Required:** EI	Verify that the system supports at least three user roles to include a system administrator, a privileged application user, and an application user.	CAT II	
	IA Control: DCFA-1 and ECLP-1	**Origin:** OAM&P IA Req. M25 and NSA 2.3.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
91	**Section:** Authentication **ID:** 1.d The system shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECLP-1	**Required:** EI **Origin:** OAM&P IA Req. M25	1. Verify the EI may be set to a default user precedence setting of ROUTINE for VVoIP session origination. 2. Confirm that the EI with the default user precedence setting of ROUTINE is unable to originate calls of a higher precedence.	CAT I	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
92	**Section:** Authentication **ID:** 1.e The system default user role shall be an application user. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, and EI **Origin:** OAM&P IA Req. M25	1. Create a new user on the system. The new user shall have, as a minimum, the access and permissions granted to that of an application user. 2. Note that the system is capable of adding or removing access and permissions from the created user default role. 3. Verify that access and permissions do not exceed those of an application user. If multiple applications are present in a system, the default user role must not exceed that of any of the application user roles. 4. Once the default user role has been created, attempt to execute actions beyond that of an application user. The default user role should not be allowed to execute actions beyond the default application user status.	CAT I	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
93	**Section:** Authentication **ID:** 1.f The system default user role shall be a limited system administrator. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECLP-1	**Required:** R**,** LS, and EBC **Origin:** OAM&P IA Req. M25	1. Create a new user on the system. The new user shall have access and permissions equivalent to a limited system administrator, as a minimum. 2. Note that the system is capable of adding or removing access and permissions from the created user default role. 3. Verify that access and permissions do not exceed those of a limited system administrator user. If multiple applications are present in a system, the default user role must not exceed that of any of the application limited system administrator user roles. 4. Create the default user role; attempt to execute actions beyond that of a limited system administrator user. The default user role should not be allowed to execute actions beyond the default limited system administrator user status.	CAT I	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
94	**Section:** Authentication **ID:** 1.g The system 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 an application user). **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Verify that the operating system or application provides for the capability to set up a hierarchy of types of users with assignable access and permissions appropriate for their assigned tasks. 2. Create users with specific roles such as system security administrator, system administrator, application administrator, and application user. The users should have access and permissions commensurate with their assigned duties and should not have Super User permissions. 3. Log on as one of the created users. Perform tasks associated with the user's tasks. 4. Attempt to access areas outside of the user's remit. 5. Verify that the user is not granted access to the requested area due to a lack of permission. 6. Log on as a super user. Attempt to access areas requested by the denied user. 7. The super user should have appropriate access and permissions to accomplish assigned responsibilities. 8. Note: In UNIX or UNIX-like systems, where the Super User (root) exists, specific roles may be established (system security administrator, system administrator, application administrator, and application user) through the change mode process, that allow sufficient permissions to accomplish the assigned task without granting Super User access.	CAT II	
	IA Control: IAIA-1 and ECLP-1	**Origin:** OAM&P IA Req. M25			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
95	**Section:** Authentication **ID:** 1.h The system shall support appropriate system administrator function as "separate" from other user functions. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** DCDS-1	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI **Origin:** GR-815-CORE R3-142[107]	1. Log on as a system administrator. 2. Execute tasks related to the system administrator role, such as proper activation and maintenance of user accounts, monitoring network performance, and viewing security log information. Verify that permissions to execute those tasks were granted and accomplished. 3. Log on as an application user. 4. Execute tasks related to the system administrator role such as proper activation and maintenance of user accounts, monitoring network performance parameters, viewing security log information. Task execution should be denied.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
96	**Section:** Authentication **ID:** 1.h.1 The security functions performed by an administrator shall be identified and documented. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** DCDS-1 and ECCD-2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI **Origin:** GR-815-CORE R3-143[110]	1. Note any identified security functions in supporting vendor documentation, which may be performed by administrators. 2. The roles of system administrator and security audit administrator should be separated. 3. Verify that the software supports the ability to separate those administrative roles. 4. The system administrator should not be able to delete any portion of the security log. 5. Log on as a system administrator. 6. Attempt to delete a file in the security log. The system administrator should not be able to write, alter, or delete any item recorded in the security log. 7. Logon as a security audit administrator. 8. Attempt to delete any item recorded in the security log. The security audit administrator should be able to execute the relative command.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
97	**Section:** Authentication **ID:** 1.h.2 If the ability to enable or disable the administrator's account is an option of a system, the systems shall not require that the account be enabled or activated during normal operation. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** IAIA-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI **Origin:** GR-815-CORE R3-144[111]	1. Establish a session as an administrator at installation, and customize the default user-ID and the default password. 2. When the password is established during the installation phase, verify the system does not require that the administrator's account be enabled or activated during normal operation. If the system does not perform this operation correctly, it fails the test. 3. Verify factory default logins, such as "admin," are deleted at the installation. 4. At the installation, attempt to establish sessions at all the points of ingress to ascertain that the appropriate login features have been activated. If the system allows a session without requiring a login with a user-ID and an authenticator, the system fails the test.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
98	**Section:** Authentication **ID:** 1.h.3 The system shall be capable of providing a mechanism for the appropriate administrator to perform the following functions: **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R and LS **Origin:**GR-815-CORE Section 3.6 & Section 3.10	1. Log in as an administrator and perform each of the 29 subsequent requirements (Test Cases 99 – 127).	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
99	**Section:** Authentication **ID:** 1.h.3.a Display all users currently logged onto the system. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.6, R3-145[112]	Verify the system's capability to display all users currently logged on.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
100	**Section:** Authentication **ID:** 1.h.3.b Independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.6.2, O3-126[90]	Verify the capability of the system to monitor independently and selectively (in real time) the actions of one or more users logged in, based on individual user-ID.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
101	**Section:** Authentication **ID:** 1.h.3.c Monitor the activities of a specific terminal, port, or network address in real time. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to monitor independently and selectively the activities of a specific terminal, port, or network address in real time.	CAT III	
	IA Control: ECAR-2	**Origin:** GR-815-CORE Section 3.6.2, O3-126[90]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
102	**Section:** Authentication **ID:** 1.h.3.d Authorize users. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the administrator may authorize users.	CAT II	
	IA Control: ECCD-2	**Origin: :** GR-815-CORE Section 3.10, R3-148[115]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
103	**Section:** Authentication **ID:** 1.h.3.e Revoke users. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the administrator's privileges include the capability to revoke users.	CAT II	
	IA Control: ECCD-2	**Origin:** GR-815-CORE Section 3.10, R3-148[115]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
104	**Section:** Authentication **ID:** 1.h.3.f Lock out and restoring a specific port or interface. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the administrator's capabilities include lock out and restore a specific port or interface.	CAT III	
	IA Control: ECND-2	**Origin:** GR-815-CORE Section 3.10, R3-149[116]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
105	**Section:** Authentication **ID:** 1.h.3.g Identify all resources accessible to any specific user along with the associated privileges required to access them. Note: Resources (i.e., files, applications, processes, etc.) should be denied to users unless specifically authorized access. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the capability of the administrator to identify all resources accessible to any specific user along with the associated privileges required to access them	CAT II	
	IA Control: IAIA-1, ECLP-1, and IAAC-1	**Origin:** GR-815-CORE Section 3.10, R3-150[117]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
106	**Section:** Authentication **ID:** 1.h.3.h Deny the creation of a user-ID that is already in use. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Attempt to create a user-ID that is already in use. If the system allows this action, it fails this test.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-151[118]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
107	**Section:** Authentication **ID:** 1.h.3.i Disable a user-ID after a specific period of time during which the user-ID has not been used. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to disable a user-ID after a specifiable period of inactivity (lack of logon).	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-152[119]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
108	**Section:** Authentication **ID:** 1.h.3.j Reinstate a disabled user-ID. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to disable user-IDs.	CAT III	
	IA Control: IAAC-1	**Origin:** GR-815-CORE Section 3.10, R3-153[120]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
109	**Section:** Authentication **ID:** 1.h.3.k Delete a disabled user-ID. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to delete disabled user-IDs.	CAT III	
	IA Control: IAAC-1	**Origin:** GR-815-CORE Section 3.10, R3-153[120]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
110	**Section:** Authentication **ID:** 1.h.3.l Create or modify a password associated with a user- ID. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to create or modify a password associated with a user-ID.	CAT I	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-154[121]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
111	**Section:** Authentication **ID:** 1.h.3.m Delete a user-ID & password. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to delete a user-ID along with all its attributes, including the password.	CAT I	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-154[121]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
112	**Section:** Authentication **ID:** 1.h.3.n Prevente the retrieval of an existing password in clear text. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as the admin. 2. If the authenticator is a password, enter the "retrieve" command to retrieve the password file on the screen. 3. Execute the print command to print the file. If retrieved or printed passwords are in cleartext, the system fails the test. 4. If the cyphertext passwords are available to the administrator, check if this privilege (i.e., access to cyphertext passwords) can be denied to all other users. If not, the system fails the test. 5. If yes, then confirm this feature by logging on as a user who is not an administrator, repeat the retrieve and print commands for the password file. The system should deny these transactions. If not, the system fails the test. (Note: Plaintext passwords must not be available to any user, including the administrator. Cyphertext passwords may be available to the administrator, but not to any other user.)	CAT I	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-155[122]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
113	**Section:** Authentication **ID:** 1.h.3.o Define a password-aging interval. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system defines a password-aging interval (i.e., the length of time the password will remain valid after being updated).	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.1]			
Test Case	**Requirement**	**System(s) Affected**		**Risk**	**Result(s)**
114	**Section:** Authentication **ID:** 1.h.3.p Define the interval during which an expired password of a user shall be denied being selected again as a new password by the same user. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the interval (or equivalent) during which an expired password shall be denied being selected again as a new password by the same user (to prevent "password flipping").	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.2]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
115	**Section:** Authentication **ID:** 1.h.3.q Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the events that may trigger alarms (e.g., failed login attempts), the levels of alarms (e.g., critical, major, minor), the type of notification (e.g., beep and/or message), and the routing of the alarm (e.g., specific port).	CAT III	
	IA Control: ECAT-2 and ECID-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.3]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
116	**Section:** Authentication **ID:** 1.h.3.r Define the duration of session lockout, which occurs when the threshold on the number of incorrect logins is exceeded. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the duration of session channel lockout. This occurs when the threshold on the number of incorrect logins is exceeded.	CAT III	
	IA Control: IAIA-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.4]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
117	**Section:** Authentication **ID:** 1.h.3.s Specify a customized advisory warning banner that is displayed upon system entry. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can specify an advisory warning banner that is displayed upon valid system entry regarding unauthorized use, and the possible consequences of violating the warning.	CAT II	
	IA Control: ECWM-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.5]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
118	**Section:** Authentication **ID:** 1.h.3.t Define the duration of the time-out interval. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the duration of the time-out interval.	CAT III	
	IA Control: ECLO-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.6]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
119	**Section:** Authentication **ID:** 1.h.3.u Define the privilege of a user to access a resource. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the privilege of a user to access a resource.	CAT III	
	IA Control: ECLP-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.7]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
120	**Section:** Authentication **ID:** 1.h.3.v Define privileges on an interface/port used to access a resource. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system can define the privilege of an interface/port (for a system that has different input channels/ports for different operations functions) to access a resource.	CAT III	
	IA Control: ECLP-1	**Origin:** GR-815-CORE Section 3.10, R3-156[123.8]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
121	**Section:** Authentication **ID:** 1.h.3.w Permit post-collection audit analysis tools for report generation. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-156[123.9]	Verify that the system can define post-collection audit analysis tools for report generation (i.e., the system shall provide an appropriate administrator the capability to customize exception reports, summary reports, detailed reports, etc., on specific system data items, users, or communication facilities).	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
122	**Section:** Authentication **ID:** 1.h.3.x Permit the retrieval, copying, printing, or uploading of the security log. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAN-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-159[126]	1. Note administrators identified security functions in supporting vendor documentation, which may be performed by a tester. 2. System administrator and security audit administrator roles should be separated. 3. Verify that the software supports the ability to separate administrative roles. 4. The system administrator should not have the ability to delete any portion of the security log. 5. Logon as a system administrator. 6. Attempt to delete a file in the security log. The system administrator should not be able to write, alter, or delete any item recorded in the security log. 7. Logon as a security audit administrator. 8. Attempt to retrieve, copy, print, and upload the security log or any portion of the security log. The system, through the security audit administrator role, should be able to execute the relative commands.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
123	**Section:** Authentication **ID:** 1.h.3.y Deny the ability to modify or delete the security log. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECTP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-160[127]	When logged in as an administrator, attempt to modify or delete a security log. If this capability is made available to anyone, other than a designated security system administrator/auditor, the system fails this test.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
124	**Section:** Authentication **ID:** 1.h.3.z Indicate when to upload the security log to avoid an over-write in the buffer. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** ECAT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-161[128]	Confirm that when the security log file should be uploaded, a system-generated notice occurs.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
125	**Section:** Authentication **ID:** 1.h.3.aa Validate the correct operation of the system. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** DCSS-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-163[130]	1. Go to the performance monitor or other available device that monitors the system. 2. Check if the system is functioning within prescribed standards and is properly monitoring system capabilities. 3. Check if notifications, warnings, alerts, or alarms are sent to the system administrator or NMS if the system falls out of prescribed parameters.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
126	**Section:** Authentication **ID:** 1.h.3.bb Monitor the system resources and their availabilities. **Reference:** UCR 5.4.6.2.1.3 **IA Control:** DCSS-2	**Required:** MFSS, SS, LSC, MG, EC, R, and LS **Origin:** GR-815-CORE Section 3.10, R3-164[131]	1. Go to the performance monitor or equivalent device that monitors the system. 2. Check if the performance monitor has the capability of monitoring system resources. 3. Check if the system is capable of distinguishing the resources in the system and their availabilities. 4. Check if notifications, warnings, alerts, or alarms are sent to the system administrator or NMS if the system resources or availabilities fall out of prescribed standards.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
127	**Section:** Authentication **ID:** 1.h.3.cc Provide a capability to detect communication errors above an administrator-defined threshold. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system's capability to detect communication errors above a designated administrator-defined threshold.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815-CORE Section 3.10, R3-165[132]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
128	**Section:** Authentication **ID:** 1.i The system shall be capable of ensuring that a user's role or precedence ability has not changed during the execution or exit from an application. Note: The user shall not be able to use a control sequence mechanism, for example, shell escape to a SUPERUSER mode. Or, if the application fails, it must not leave the user in a different role with more privileges. The user must reauthenticate (re-login) in order to assume a different role. If a system administrator has granted a user role limited root access (e.g., sudo for UNIX) it is part of that person's user role. This primary method to mitigate the threats associated with this requirement is to use industry best practices when developing the system. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, and EBC	1. Log on to an application. 2. Check if the user is able to access permitted areas according to the user's access rights. 3. Check if the user is able to execute applicable permissions according to the user's privilege level (i.e. read write, execute, etc.). 4. When logged in as the user, attempt to elevate access rights and permissions. 5. The user should not be able to elevate any access rights or permissions. Only an administrator should be able to elevate a user's access rights or permissions. 6. Exit the application and log back on as the same user. 7. The same access rights and permissions should be executed as previously noted. 8. Establish a priority precedence IP phone call. 9. Attempt to elevate permissions of the established IP phone call while the session is in progress. 10. A change of phone call precedence (either increased or decreased) should not be possible. 11. Terminate the IP phone call. 12. Re-establish the IP phone call at the same terminal. Check if the user can re-establish the same IP phone with the same precedence. 13. Phones should be assigned precedence permissions by the administrator.	CAT II	
	IA Control: ECCD-2 and ECPA-1	**Origin:** OAM&P M61			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
129	**Section:** Authentication **ID:** 1.j The system shall only transmit passwords that are encrypted. Note: The Backbone Transport Services STIG requires that router administrative passwords are encrypted using MD5. **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify clear-text passwords are not transmitted. This is re-verified during IPV testing. 2. Verify passwords are encrypted using MD5.	CAT II	
	IA Control: IAIA-1	**Origin:** CJCSM 6510.01 C3.14 and VoIP STIG Vulnerability 121			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
130	**Section:** Authentication **ID:** 1.k The system shall be capable of limiting user access based on a time-of-day interval (i.e., duty hours). **Reference:** UCR 5.4.6.2.1.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. If the access point does not have the capability to deny access for requests that fall outside of an authorized time interval, this test case fails. 2. Attempt to perform administration or normal user duties outside the authorized duty hours of the administrator and normal user. 3. Confirm the attempt to perform those duties is prohibited.	CAT III	
	IA Control: DCSR-2 and ECAN-1	**Origin:** GR-815-CORE CR3-11 and DRSN STIG 6.2.8.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
131	**Section:** Authentication **ID:** 1 Systems that use ancillary AAA and SysLog services shall do so in a secure manner. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Verify Required Ancillary Equipment for AAA services are using FIPS140-2. 2. Verify SysLog services are capable of being performed in a secure manner.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Section 13			
	Site Responsibility: EBRU-1				

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
132	**Section:** Authentication **ID:** 1.a Systems that use external AAA services provided by the Diameter Base Protocol shall do so in accordance with RFC 3588. Note: An external AAA service is a service that is extends beyond the boundary of the system. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Determine if the system appears on the NIAP-validated products list. 2. If the product does not appear on the list, note if the product will be tested in the NIAP testing process. 3. Proceed to the AAA configuration tables. 4. Verify that authentication and system data pass to the related device through channels with secure protocols. 5. Confirm that authentication using the AAA device performs to the existing security standards. Note: Protocol traffic and handshake to establish encrypted sessions will be observed during IPV testing. IPV testing will verify that the establish sessions remains encrypted.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** FC 3588 Section 2.8.2			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
133	**Section:** Authentication **ID:** 1.a.1 Systems that act as Diameter Agents shall be capable of being configured as Proxy Agents. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Proceed to the Diameter Agent's configuration panel. 2. Confirm the system's ability to adjust resource usage, provisioning, and forward requests. 3. Intentionally do not conform to the configured parameters of the system. 4. Attempt to login using Diameter services. 5. Confirm that the AAA transaction is rejected.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, EBRU-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Section 2.8.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
134	**Section:** Authentication **ID:** 1.a.1.a Systems that act as Proxy Agents shall maintain session state. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Initiate an active session on the user application. 2. Perform user-initiated actions that require storing and retrieving of values using the initiated application. 3. Confirm that session state is maintained as the user navigates through the application and performs tasks.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Section 2.8.2			
	Site Responsibility: EBRU-1				

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
135	**Section:** Authentication **ID:** 1.a.2 All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Proceed to the Diameter configuration tables. 2. Confirm that there are rules in place to enforce the acceptance or rejection of AVP. 3. Introduce an explicitly excluded AVP into the base Diameter protocol. 4. Confirm that the Diameter implementation ignores the input.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Sections 6.1.8 and 6.2.1			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
136	**Section:** Authentication **ID:** 1.a.3 All Diameter implementations shall provide transport of its messages in accordance with the transport profile described in RFC 3539. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	An LoC may be accepted for this requirement. Note: Interoperability testing will perform interoperability and functionality testing to ensure compliance with RFC 3539.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Section 2.9			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
137	**Section:** Authentication **ID:** 1.a.4 Systems that use the Extensible Authentication Protocol (EAP) within Diameter shall do so in accordance with RFC 4072. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	An LoC may be accepted for this requirement. Note: Interoperability testing will perform interoperability and functionality testing to ensure compliance with RFC 4072. Note: The EAP provides a standard mechanism for support of various authentication methods. RFC 4072 defines the Command-Codes and AVPs necessary to carry EAP packets between an NAS and a back-end authentication server.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 4072			
	Site Responsibility: EBRU-1				

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
138	**Section:** Authentication **ID:** 1.b Systems that use external AAA services provided by the Remote Authentication Dial In User Service (RADIUS) shall do so in accordance with RFC 2865. Note: The use of Diameter is preferred. Future requirement revisions may mandate the use of Diameter. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Note whether the system is able to meet required authentication standards without the use of ancillary equipment. 2. If remote authentication is not required, this test procedure is not applicable. 3. If RADIUS is used, log into the component. 4. Confirm that authentication standards are met in relation to login, password (complexities), and two-factor authentication when required. Note: Authentication requirements and test procedures are noted in this document.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 2865			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
139	**Section:** Authentication **ID:** 1.b.1 Systems that use the Extensible Authentication Protocol (EAP) within RADIUS shall do so in accordance with RFC 3579. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	An LoC may be accepted for this requirement. Note: Interoperability testing will perform interoperability and functionality testing to ensure compliance with RFC 3579. Note: The EAP provides a standard mechanism for support of various authentication methods. The NAS forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3579			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
140	**Section:** Authentication **ID:** 1.b.2 If the systems support RADIUS based accounting, the system shall do so in accordance with RFC 2866. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Confirm that port 1813 is used for RADIUS accounting. 2. Proceed to the NAS and confirm that user accounting information is properly entered and stored. 3. Log into a component that relies on RADIUS for authentication to confirm that the server properly receives the accounting information. Note: IPV testing will ensure that this requirement is tested.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 2866			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
141	**Section:** Authentication **ID:** 1.b.3 If the system 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 2008 (Section 5.4.6, Requirements). **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Proceed to the configuration panel of the RADIUS server. 2. Confirm that IPsec or TLS may be configured using non-null transforms. Note: Observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3588 Section 13			
	Site Responsibility: EBRU-1				

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
142	**Section:** Authentication **ID:** 1.b.4 If the system supports RADIUS and IPsec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements). **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Login to the system and establish a session. 2. Login should use the RADIUS server and IPsec. 3. Confirm that the session is established and maintained. Note: Test certificates are available from the lab SA. Note: Testers will observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 4306			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
143	**Section:** Authentication **ID:** 1.c Systems that use external AAA services provided by the TACACS+ shall do so in accordance with the TACACS+ Protocol Specification 1.78 (or later). Note: The intent is to use the most current specification. The use of Diameter is preferred. Future requirement revisions may mandate the use of Diameter. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Determine whether the system is able to meet authentication standards without the use of ancillary equipment. Note: If remote authentication is not required, this test procedure is not applicable. 2. If TACACS+ is used, log into the component. 3. Confirm that the component meets authentication standards in relation to login, password (complexities), and two-factor authentication when required. Note: Authentication requirements and test procedures are in this document.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin: :** RFC 3588 Section 13			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
144	**Section:** Authentication **ID:** 1.c.1 If the system supports TACACS+, it shall support the use of IPsec and/or TLS using non-null transforms as defined in the confidentiality section of this document (Section 5.4.6, Requirements). **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Proceed to the configuration panel of the TACACS+ server. 2. Confirm that IPsec or TLS may be configured using non-null transforms. Note: Observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin: :** RFC 3588 Section 13			
	Site Responsibility: EBRU-1				

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
145	**Section:** Authentication **ID:** 1.c.2 If the system supports TACACS+ and IPsec, it shall support the use of IKE for key management as defined in the confidentiality section of this (Section 5.4.6, Requirement). **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	1. Login to the system and establish a session. 2. Login should use the TACACS+ server and IPsec. 3. Confirm that the session is established and maintained. Note: Test certificates can be obtained from the lab SA. Note: Observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 4306			
	Site Responsibility: EBRU-1				
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
146	**Section:** Authentication **ID:** 1.d Systems that use external address assignment services provided by the DHCP shall do so in accordance with RFC 2131. Note: An external address assignment service is a service that extends beyond the boundary of the system. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** EI	1. Confirm that the system uses DHCP services. Note: If the system does not use DHCP services, this requirement test procedure is not applicable. 2. Identify the DHCP server. 3. Configure the system to obtain an IP address through dynamic allocation as opposed to automatic or manual allocation. 4. Ensure that the component is connected to the system. 5. Perform functionality checks. Note: IPV testing will confirm that expected traffic is passes between components of the system and that IP addressing is assigned in a secure manner.	CAT III	
	IA Control: DCSP-1	**Origin:** RFC 2131			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
147	**Section:** Authentication **ID:** 1.d.1 Systems 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 are found in RFC 2131. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** EI	1. Attempt a manual connection with a known address. The network should not validate the component. 2. Attempt to use the component with the duplicated IP address in the system. The component should not interact with the system. Note: IPV testing will confirm that properly addressed components were added to the system and that there are no duplicate addresses.	CAT III	
	IA Control: DCSP-1	**Origin:** RFC 2131 Section 2.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
148	**Section:** Authentication **ID:** 1.d.2 Systems 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. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** EI	Note: IPV testing will confirm that components with newly established IP addresses broadcast proper ARP reply announcements.	CAT III	
	IA Control: DCSP-1	**Origin:** RFC 2131 Section 4.4.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
149	**Section:** Authentication **ID:** 1.e Systems that use external AAA services provided by port-based network access control mechanisms shall do so in accordance with IEEE 802.1X-2004 in combination with a secure EAP type (EAP-TLS, EAP-TTLS, or PEAP). **Reference:** UCR 5.4.6.2.1.4	**Conditional:** R, LS, and EI	An LoC may be accepted for this requirement. Note: Interoperability and functionality testing will ensure compliance with RFC 3748. Note: The EAP provides a standard mechanism for support of various authentication methods. The NAS forwards EAP packets to and from the AAA services, encapsulated within EAP-Message attributes.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, EBRU-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3748			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
150	**Section:** Authentication **ID:** 1.e.1 Systems that use external EAP services provided by EAP shall do so in accordance with RFC 3748 and its RFC extensions. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** R, LS, and EI	An LoC may be accepted for this requirement. Note: Interoperability and functionality testing will ensure compliance with RFC 3748. Note: The EAP provides a standard mechanism for support of various authentication methods. The NAS forwards EAP packets to and from the AAA services, encapsulated within EAP-Message attributes.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, EBRU-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3748			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
151	**Section:** Authentication **ID:** 1.e.1.a Systems that support EAP as a minimum shall support authentication using shared secrets. Note: RFC 3748 requires that systems support Identity, Notification, Nak, and MD-5 Challenge Request/ Response exchanges. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** R, LS, EI	An LoC may be accepted for this requirement. Note: Interoperability and functionality testing will ensure compliance with RFC 3748. Note: The EAP provides a standard mechanism for support of various authentication methods. The NAS forwards EAP packets to and from the AAA services, encapsulated within EAP-Message attributes.	CAT II	
	IA Control: IAIA-1, IAGA-1, ECCR-1, ECCT-1, ECLO-1, ECLP-1, IAAC-1, EBRU-1, DCNR-1, IAKM-2, and IATS-2	**Origin:** RFC 3748 Section 5			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
152	**Section:** Authentication **ID:** 1.f Systems that use external sysLog services shall do so in accordance with RFC 3164. Note: It is understood that an Internet Draft is written that will deprecate RFC 3164, but that draft is new and it is unknown whether it will be approved. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Proceed to the SysLog configuration tables. 2. Enter configurations for obtaining desired information from the system. 3. Perform actions on the system to obtain expected data on the SysLog server. 4. Confirm that the information is obtained according to configuration tables.	CAT II	
	IA Control: ECAR-2, ECAT-1, ECAT-2, ECTB-1, and ECTP-1	**Origin:** RFC 3164			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
153	**Section:** Authentication **ID:** 1.f.1 Systems that support SysLog shall use UDP port 514 for the source port of the sender when using UDP for transport. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Proceed to the configuration tables of the SysLog server. 2. Confirm that UDP port 514 is used for receiving data. Note: IPV testing will confirm that expected traffic is properly passing between components of the system using port 514.	CAT III	
	IA Control: ECAR-2, ECAT-1, ECAT-2, ECTB-1, and ECTP-1	**Origin:** RFC 3164 Section 2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
154	**Section:** Authentication **ID:** 1.f.2 Systems that support SysLog shall transmit messages in the format defined by RFC 3164. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	An LoC may be accepted for this requirement. Note: IPV testing will confirm that expected traffic is properly passing between components of the system.	CAT II	
	IA Control: ECAR-2, ECAT-1, ECAT-2, ECTB-1, and ECTP-1	**Origin:** RFC 3164 Section 2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
155	**Section:** Authentication **ID:** 1.f.3 Systems that support SysLog shall have all the parts of the SysLog packet as described in section 4.1 of RFC 3164. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	An LoC may be accepted for this requirement.	CAT II	
	IA Control: ECAR-2, ECAT-1, ECAT-2, ECTB-1, and ECTP-1	**Origin:** RFC 3164 Section 4.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
156	**Section:** Authentication **ID:** 1.f.3.a If the originally formed message has a TIMESTAMP in the HEADER part, then it shall be the local time of the device within its time zone. **Reference:** UCR 5.4.6.2.1.4 **IA Control:** IAKM-2	**Conditional**: MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3164	1. Capture and analyze an originally formed message. 2. Confirm that the system has a timestamp in the header. If the system does not have a TIMESTAMP in the HEADER, this requirement and test procedure does not apply. 3. Note that originally formed messages that do contain TIMESTAMPS in the header use local time within the time zone of the originally created message. Note: IPV testing will capture unencrypted traffic and ensure that traffic is properly passing between components of the system.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
157	**Section:** Authentication **ID:** 1.f.3.b 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. **Reference:** UCR 5.4.6.2.1.4 **IA Control:** IAKM-2	**Conditional**: MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3164	1. Capture and analyze an originally formed message. 2. Note that originally formed message contains a Hostname field. 3. If a hostname field is not present then the original message shall contain an IP address. Note: IPV testing will capture unencrypted traffic and ensure that traffic is properly passing between components of the system.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
158	**Section:** Authentication **ID:** 1.f.3.c If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message. **Reference:** UCR 5.4.6.2.1.4 **IA Control:** IAKM-2	**Conditional**: MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3164	1. Capture and analyze an originally formed message. 2. Confirm that the system has a tag value. If the system does not have a TAG value, then this requirement and test procedure does not apply. 3. Note that if the originally formed messages do not contain a TAG value, it does contain the name of the program or process that generated the message. Note: IPV testing will capture unencrypted traffic and ensure that traffic is properly passing between components of the system.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
159	**Section:** Authentication **ID:** 1.f.4 If systems use TCP for the delivery of SysLog events, then the system shall do so in accordance with the RAW profile defined in RFC 3195. Note: It is understood that an Internet Draft is written that will deprecate RFC 3195, but that draft is new and it is unknown whether it will be approved. **Reference:** UCR 5.4.6.2.1.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	An LoC may be accepted for this requirement. Note: IPV testing will confirm that encrypted traffic is properly passing between components of the system.	CAT II	
	IA Control: IAKM-2	**Origin:** RFC 3195			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
160	**Section:** Authentication **ID:** 1 The system shall be capable of authenticating users and appliances. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	Establish a login at each ingress point. Each ingress should require the user to provide a user-ID and an authenticator (such as a password, a one-time authenticator, etc.). If this requirement is not fulfilled, the system fails the test.	CAT I	
	IA Control: IAIA-1	**Origin:** DoDD 8500.1 4.2; CJSCI 6510.01D B.1.b.1; and GR-815-CORE R3-54			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
161	**Section:** Authentication **ID:** 1.a The system shall only allow authenticated users and appliances to access the system. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	Establish a login at each ingress point. Each ingress should require the user to provide a user-ID and an authenticator (such as a password, a one-time authenticator, etc.). If this requirement is not fulfilled, the system fails the test.	CAT I	
	IA Control: IAIA-1	**Origin:** CJCSM 6510.01 A.C.2; VoIP STIG 0127; and Vulnerability 2A			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
162	**Section:** Authentication **ID:** 1.a.1 The system shall ensure those authentication credentials are not transmitted in the “clear” (i.e., credentials are encrypted end-to-end). Note: The PKI certificate does not fall under this requirement due to the nature of the public key authentication model. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, LS, and EI	Ensure that the communications between nodes is encrypted when PKI is not employed. Note: IPV testing will confirm that encrypted traffic is properly passing between components of the system.	CAT I	
	IA Control: IAIA-1	**Origin:** OAM&P N41			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
163	**Section:** Authentication **ID:** 1.a.2 The system shall be capable of ensuring that system access points that provide remote login facility also provide authentication services that are capable of using authentication mechanisms that are stronger than usernames and passwords (i.e., using two-factor authentication (strong authentication). **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Analyze the system and determine if remote access is used. 2. Record all access points that are that are used for remote access. 3. Verify that all remote access points require two-factor authentication.	CAT II	
	IA Control: EBRP-1, EBRU-1, and DCBP-1	**Origin:** GR-815-CORE CR3-64[R33], R3-19[31], R3-20[34]; DRSN STIG 6.2.8.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
164	**Section:** Authentication **ID:** 1.a.3 The system shall be capable of authenticating the EI using TLS (or its equivalent) (Threshold) and/or with PKI certificates. NOTE: This assumes the EI is served directly by the appliance. **Reference:** UCR 5.4.6.2.1.5	**Required:** LSC	1. Check that the system has encryption enabled. 2. Check that PKI certificates are in place and that the system is capable of using them. 3. Record which method of encryption the IP phone call uses. 4. Establish an encrypted IP phone call. 5. Check that TLS and PKI certificates are being properly used for setup and establishment of the phone call. 6. Check that the established IP phone call is properly encrypted. 7. Note: Observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted. If these procedures are not met, the system fails this requirement.	CAT I	
	IA Control: IAIA-1	**Origin:** Application Security and Development STIG section 3.8.3 PKI Authentication			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
165	**Section:** Authentication **ID:** 1.a.4 The system shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) with PKI certificates. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	1. Check that the system has encryption enabled. 2. Check that PKI certificates are in place and that the system is capable of their usage. 3. Record which method of encryption the LSC is configured for. 4. Establish an encrypted IP phone call and ensure that the LSC is involved in the call set-up. 5. Check that TLS and PKI certificates are being properly used for setup and establishment of the phone call. 6. Check that the IP phone call is properly encrypted. Note: Observe protocol traffic and handshake for establishing encrypted sessions during IPV testing. IPV testing will verify that the established sessions remain encrypted.	CAT I	
	IA Control: IAIA-1	**Origin:** Application Security and Development STIG section 3.8.3 PKI Authentication			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
166	**Section:** Authentication **ID:** 1.b. The system shall be capable of authenticating an appliance using the DoD Public Key Infrastructure (PKI). Note: The EI authentication is excluded from this requirement in FY08. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Confirm that the system can use certificates issued by the DoD PKI and approved external PKIs as appropriate to support authentication, access control, confidentiality, data integrity, and Non-repudiation.	CAT 1	
	IA Control: IAIA-1 and DCNR-1	**Origin:** Application Security and Development STIG section 3.8.3 PKI Authentication			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
167	**Section:** Authentication **ID:** 1.b.1 If the system is PKE, then the system shall use the DoD PKI certificates with the associated public key in the TLS certificate message for authenticating appliance when using AS-SIP. NOTE: Some options considered to meet this requirement include the use of On-line Status Check and certificate trust list as discussed in Section 5.4.5.2.7 paragraph 1(g). **Reference:** UCR 5.4.6.2.1.5	**Conditional**: MFSS, LSC, SS, EBC, and EI	1. Confirm that the system is PKE enabled. 2. Check that PKI certificates are in place and that the system is capable of using them. 3. Check that the DoD PKI certificates are being used with the associated public key in the TLS certificate message for the authenticating appliance when using AS-SIP. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions will be observed during IPV testing.	CAT I	
	IA Control: IATS-2	**Origin:** Vendor Agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
168	**Section:** Authentication **ID:** 1.b.2 If the system supports web browsers and web servers, the system shall be capable of using DoD PKI certificates with the associated public key in the TLS certificate message for authenticating users. **Reference:** UCR 5.4.6.2.1.5	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Confirm whether the system supports web browsers and web servers. 2. Confirm that the system is PKE enabled. 3. Check that PKI certificates are in place and that the system is capable of using them. 4. Check that the DoD PKI certificates are being used with the associated public key in the TLS certificate message for the authenticating between the web browser and web server. 5. Verify encryption of the established session. Note: Protocol traffic and handshake for establishing encrypted sessions will be observed IPV testing. Once the session is established, IPV testing will verify that the established session remains encrypted.	CAT II	
	IA Control: IATS-2	**Origin:** Application Security and Development STIG section 3.8.3 PKI Authentication			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
169	**Section:** Authentication **ID:** 1.c The system shall be capable of ensuring that user authentication of logging in, logging, and auditing of an appliance shall be at least as strong as a user-ID and the appropriate password/PIN entered over a previously established trusted path. Note: The previously established trusted path ensures that the password is not transmitted in the clear. It is acceptable for systems to use RADIUS, TACACS+, or DIAMETER for AAA services. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Establish a session and verify that the system performs logon and authentication services in relation to the requestor and relative authentication service with the use of user-ID and password or a PIN or certificate. Additionally, verify that the system does not allow user-ID, passwords, PINs, or certificates to be transmitted in the clear. 2. Proceed to the security log. 3. Verify that logging and auditing is being recorded is being recorded and that the User-ID and appliance logged into is recorded as appropriate. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** DoDD 8500.1 4.8.1; OAM&P IA Req. M12; and GR-815-CORE R3-9[6]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
170	**Section:** Authentication **ID:** 1.d The system shall not support ways to bypass the deployed authentication mechanism. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Note: The IPV test team will further investigate methods to bypass authentication.	CAT I	
	IA Control: ECAR-2	**Origin:** GIG MA ICD IV.B.6.c.4; and GR-815-CORE R3-10[11]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
171	**Section:** Authentication **ID:** 1.e The system 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 login are covered this section of the UCR 2008. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. At each ingress, attempt to log on, using an incorrect user-ID. 2. Proceed to the security log. 3. Verify that for each logon at each access point an entry appears in the security log. 4. Repeat the logon attempt with a correct user-ID but incorrect authenticator. If the logon procedure is halted, the system fails the test. 5. Verify that for each failed logon at each access point an entry appears in the security log.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-17[42]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
172	**Section:** Authentication **ID:** 1.f The system shall protect (i.e., encrypt) all internal storage of authentication data to ensure confidentiality. Note: This requirement is not meant to preserve session keys during a power cycle. It is primarily meant to ensure that an intruder that gains access to the system is not able to view the authentication information in clear text. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	As administrator, examine all password file(s) and confirm that all passwords are stored in encrypted form.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-11[222]; and VoIP STIG Security Vulnerablity 121			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
173	**Section:** Authentication **ID:** 1.g The system shall be capable of allowing users to place ROUTINE precedence and emergency call without authenticating. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	1. Attempt to place a call using the precedence ROUTINE without entering any authentication credentials. 2. If the call is completed, then the system passes. Otherwise, the system fails this requirement. 3. Attempt to place an emergency call without entering any authentication credentials. 4. If the call is completed, then the system passes. Otherwise, the system fails this requirement.	CAT II	
	IA Control: IAIA-1	**Origin:** VVoIP Core Team Agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
174	**Section:** Authentication **ID:** 1.h The system shall only allow authenticated users to access the system for services above the ROUTINE precedence. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	Attempt to complete calls at all levels of precedence higher than ROUTINE. If the call is completed, then the system fails this requirement.	CAT I	
	IA Control: IAIA-1	**Origin:** VVoIP Core Team Agreement; GR-815-CORE R3-24, NSA 2.3			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
175	**Section:** Authentication **ID:** 1.h.1 The system uses SIP, the system shall use digest authentication as specified in RFC 3261 and/or with PKI certificates for authenticating user credentials to the LSC through the EI. Note: The LSC is responsible for the authentication decisions. The method for authenticating a user with their PKI certificate is a vendor decision (due to the immaturity of the current standards). Vendors may choose to implement user authentication using PKI certificates, as described in RFC 3261 or in RFC 3893. **Reference:** UCR 5.4.6.2.1.5	**Conditional:** LSC and EI	1. Establish an IP phone call between the EI and the LSC. 2. Verify the call is established and is good quality condition. 3. Ensure that encryption method is turned on. 4. Re-establish an IP phone call and ensure that the LSC accepted the digest authentication (via TLS) or PKI certificate. 5. Verify the call is established and is good quality. 6. Proceed to the security log. 7. Ensure that the two calls were recorded in the security log. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: ECNK-1 and IATS-2	**Origin:** Vendor Agreement and NSA 2.3.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
176	**Section:** Authentication **ID:** 1.h.2 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 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. **Reference:** UCR 5.4.6.2.1.5	**Required:** LSC and EI	1. Proceed to the configuration section of the device. 2. Confirm that the tables provide an option to enable or disable authentication.	CAT II	
	IA Control: ECNK-1 and IATS-2	**Origin:** Vendor Agreement and NSA 2.3.5			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
177	**Section:** Authentication **ID:** 1.h.2.a If the system is a Softphone, the system shall provide user authentication by presenting the CAC credentials of the user to the LSC. **Reference**: UCR 5.4.6.2.1.5	EI (Softphone)	1. Access the Softphone authentication settings. 2. Verify that CAC credentials can be configured as form of network authentication.	CAT II	
	IA Control: ECNK-1, IATS-2, and ECLP-1	**Origin:** PCCC (Voice Video Collabration) Section 2.6.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
178	**Section:** Authentication **ID:** 1.h.2.b The system shall only allow 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. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	1. As a normal user, without administrative privileges, attempt to activate a system-administrative process. 2. Confirm that the attempt was denied because of privilege issues.	CAT II	
	IA Control: ECLP-1	**Origin:** VoIP STIG 0060			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
179	**Section:** Authentication **ID:** 1.b The system shall not display configuration information without proper authentication. Note: The minimum requirement for authentication is defined UCR 2008, Section 5.4.6.2.1.5, Authentication Practices, paragraph 1.c. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	Verify that only the appropriate administrator may view configuration information and that the administrator does not have access to that display until properly authenticated.	CAT II	
	IA Control: IAIA-1 and ECLP-1	**Origin:** VoIP STIG 0060			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
180	**Section:** Authentication **ID:** 1.j The system shall be capable of ensuring that all ports on a system that support operation related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Note all access points that support operational or configuration management related commands. All access points of this nature must be on the product's accompanying diagram and in the system description documentation. Verify that two-factor authentication is required to log on at any access point where operational or configuration management related commands might be used.	CAT II	
	IA Control: DCBP-1	**Origin:** GR-815-CORE R3-13[35], R3-24[12]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
181	**Section:** Authentication **ID:** 1.k The system shall be capable of ensuring that all appliances that support connection-oriented communications also support mutual authentication between the requestor and the provider. Note: A connection-oriented communication is a session between two VVOIP appliances where the Transport Layer Protocol sends acknowledgments to the sender regarding incoming data. This type of session usually provides for retransmission of corrupted or lost data. **Reference:** UCR 5.4.6.2.1.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Note all appliances in the system that support connection-oriented communications. 2. Confirm that the system supports mutual authentication between the requestor and the provider. 3. Confirm that once mutually authenticated sessions are established, that the sessions remain up and that information is appropriately passed. Note: IPV testing observes protocol traffic and handshake for establishing of encrypted sessions during IPV testing. IPV testing will verify that the establish sessions remains encrypted.	CAT II	
	IA Control: ECIC-1	**Origin:** GR-815-CORE R3-14[223], R3-15[224], R24[12]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
182	**Section:** Authentication **ID:** 1.l The system shall properly operate when auto-registration is disabled. Note: Auto-registration is typically used during initial installation of large numbers of EIs. It involves the automatic registration of EI 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. **Reference:** UCR 5.4.6.2.1.5	**Required:** EI	1. With auto-registration disabled, perform EI (SIP phone) installation procedures, which include Registration, IP assignment, and other required parameter settings. 2. Establish SIP calls of the newly installed EI and confirm that the calls complete normally.	CAT II	
	IA Control: IAIA-1	**Origin:** VoIP STIG 0065, 0068			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
183	**Section:** Authentication **ID**: 1.m The default authentication mechanism for SNMPv3 shall be HMAC-SHA-96**.** **Reference:** UCR 5.4.6.2.1.5 **IA Control:** ECCT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** Vendor Agreement	1. Confirm if, in the system's configuration tables, the SNMPv3 is used. 2. Note, in the system's configuration tables, that HMAC-SHA-96 is used as the default authentication mechanism. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
184	**Section:** Authentication **ID:** 1 The system shall be capable of meeting the DoD PKE requirements for PKI based authentication. Note: The requirement for an EI to be PKE is conditional for FY 2008, but will be required for FY 12. The condition for FY 2008 is that if the EI is PKE, it shall meet the PKE requirements. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoDD 8500.1 4.8.2; GIG MA ICD IV.B.6.c; CJCSI 6510.01D B.1.b.4.13; JTA 6.7.1; and OAM&P IA Req. for Public Network M7	Verify that the system meets DoD PKE requirements.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
185	**Section: Authentication** **ID:** 1.a The system shall be capable of generating asymmetric (public and private) key pairs and symmetric keys. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2 and IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1 & 4.3.3	1. Confirm that the system is properly equipped to generate symmetric keys. 2. Confirm that the system is properly equipped to generate asymmetric key pairs. 3. Establish sessions that use symmetric keys and asymmetric keys. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
186	**Section:** Authentication **ID:** 1.a.1 The system shall be capable of generating asymmetric keys whose length is at least 1024 for RSA. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2 and IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1.1	1. Proceed to the configuration tables that assign key length parameters. 2. Confirm that the system provides for asymmetric keys whose length is at least 1024 for RSA. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
187	**Section:** Authentication **ID:** 1.a.2 The system shall be capable of generating symmetric keys whose length is at least 128 bits. **Reference:** UCR 5.4.6.2.1 **IA Control:** IAKM-2 and IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, R **Conditional:** EI **Origin:** DoD PKE 4.3.3.2; OAM&P IA Req. M8; and an update from PKI PMO that 3DES is now standard	1. Proceed to the configuration tables that assign key length parameters. 2. Confirm that the system provides for the utilization of symmetric keys whose length is at least 128 bits. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
188	**Section:** Authentication **ID:** 1.a.2.a The system shall be capable of distributing keys used for symmetric encryption out-of-band or by secure cryptographic processes that comply with FIPS 140-2. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** FIPS 140-2 Section 4.7	1. Check if the system is capable of distributing keys used for encryption out-of-band. 2. Check that the system's configuration files comply with symmetric encryption standards. 3. Establish a session, using out-of band encryption, and confirm the quality of the connection. 4. Check if the system is capable of distributing keys used by other acceptable cryptographic processes that comply with FIPS 140-2. (This may include the out-of-band encryption of session set-up, in-band session establishment, or a combination of the two). 5. Note, in the configuration files, that the system adequately complies with symmetric encryption standards. 6. Establish a session using out-of band, In-band, or a combination of the two and ensure that the method of establishment complies with FIPS 140-2. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
189	**Section:** Authentication **ID:** 1.a.3 The system shall be capable of generating keys using a random source algorithm that meets the requirements of FIPS 186. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** FIPS 186	1. Verify that the system is capable of generating random source algorithm PKI keys that are FIPS 186 compliant. 2. Test lab PKI keys may be used to test functionality of the systems capability to generate random source algorithm PKI keys. The test lab will be able to verify that keys are randomly generated. 3. Establish two separate sessions and verify that randomly generated keys were used to establish each session. 4. An LoC with a certificate from the granting certifier is acceptable. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
190	**Section:** Authentication **ID:** 1.b The system shall be capable of storing key pairs and their related certificates. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** ECML-1, ECCR-1, and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1	1. Extract key pairs. 2. Verify that the system is capable of storing key pairs and certificates. 3. Test the functionality of the system using the key pairs and certificates that are in storage.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
191	**Section:** Authentication **ID:** 1.b.1 The system shall be capable of storing certificates for a subscriber. Note: A subscriber may be itself, another appliance, or a user of the system. The certificates may have the same public key and may be associated with different issuers, different uses, or different validity periods. The certificates are stored on the appliance for a variety of reasons including for historical purposes. This requirement is for local authentication of the user and is not meant to obtain the private key of the subscriber. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1	1. Proceed to the certificate storage area for the system. 2. Determine to what extent certificates are used by the system (main appliance, other appliance, or user of the system). 3. Confirm ability of the system to upload and store certificates. 4. Note the systems ability to connect to desired appliances within the system with the use of certificates. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
192	**Section:** Authentication **ID:** 1.b.2 The system shall be capable of protecting the private key from compromise or loss. Note: The requirement may be satisfied by meeting the requirements of FIPS 140-2 for protecting keys. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	Verify that the system is capable of protecting the private keys from exposure, compromise, or loss.	CAT II	
	IA Control: IAKM-2	**Origin:** DoD PKE 4.3.1.2 & 4.3.1; and DRSN STIG 4.7.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
193	**Section:** Authentication **ID:** 1.b.2.a If the certificate shall be used for non-repudiation purposes, the system shall be capable of ensuring that all copies of private keys generated for actual or possible non-repudiation purposes are under the owning entity's sole control. Note: A subsequent requirement mandates that the system is capable of using the certificate for non-repudiation by setting the key usage extension for non-repudiation. An example of a need for non-repudiation is to verify that a user made a malicious configuration change on the platform. **Reference:** UCR 5.4.6.2.1.6	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and EI	Verify that the user's private keys cannot be copied.	CAT III	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
194	**Section:** Authentication **ID:** 1.b.2.b The system shall be capable of meeting the requirements for level 1 of FIPS 140-2 in FIPS Mode (i.e., approved for federal government use as opposed to commercial use). Note: Where the requirements are more secure than FIPS 140-2, UCR 2008 requirements supersedes FIPS 140-2. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, R, and EI	Verify that the system is capable of meeting the level one requirements of FIPS 140-2.	CAT II	
	IA Control: IAKM-2 and DCNR-1	**Origin:** JTA 6.4.2.7.a; DoD PKE 4.3.1.2; NSA 2.3.1 and DRSN STIG 4.7.4			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
195	**Section:** Authentication **ID:** 1.b.2.c If the system performs operations with the unencrypted key in software, the system shall be capable of encrypting or destroying the key as soon as the operation is complete. **Reference:** UCR 5.4.6.2.1.6	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and EI	1. Note if the system performs operations with the unencrypted key in the software. 2. Upon completion of the operation, note that the key has been either encrypted or destroyed. 3. An LoC noting the lab that provided the certification of this specific capability may be accepted. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
	IA Control: IAKM-2 and IATS-2	**Origin:** DoD PKE 4.3.1.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
196	**Section:** Authentication **ID:** 1.b.2.d If passwords are used to protect private keys, the system shall be capable of ensuring that the password is selected from a space of at least 2^{56} possible passwords unless there is a means to detect and protect against deliberate attempts to search for passwords. Note: This requirement is meant to prevent a malicious user from using password guessing to gain access to private keys. The requirement may be met by meeting the requirement defined in requirements section 5.4.5.2, Authentication. **Reference:** UCR 5.4.6.2.1.6	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and EI	1. Note whether passwords are used to protect private keys. 2. If passwords are used to protect private keys, go to the password protect configuration tables and verify that the password complexity can be configured to meet the 2^{56} requirement. 3. An LoC noting the lab that provided the certification of this specific capability may be accepted.	CAT II	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.1.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
197	**Section:** Authentication **ID:** 1.b.2.e The system shall operate with DoD trust points. Note: Trust points are defined in UCR 2008, Appendix A, Definitions, Abbreviations and Acronyms, and References. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1.3	1. Proceed to the certificate management section of the system. 2. Verify that appropriate trust points have been designated. 3. In the lab environment, these trust points will be issued through a test certificate. 4. Establish a session between two components that requires the use of trust points. 5. An LoC noting the lab that provided the certification of this specific capability may be accepted. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
198	**Section:** Authentication **ID:** 1.b.2.f The system shall authenticate up to a trust point. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1.3	1. Proceed to the certificate management section of the system. 2. Verify that appropriate trust points have been designated. 3. In the lab environment, these trust points will be issued through a test certificate. 4. Establish a session between two components that requires the use of trust points. 5. Confirm accepted certificates through the normal operation of the system. 6. An LoC noting the lab that provided the certification of this specific capability may be accepted. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
199	**Section:** Authentication **ID:** 1.b.2.g If the trust point is not established, the system shall authenticate to the root certificate or Certification Authority (CA). **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and EI **Origin:** Vendor agreement - CAT II	1. Verify that the system authenticates to the root certificate or the CA. 2. Search for a locally stored CRL. If it is found, delete it. 3. Remove connection to the PKI directory. 4. Attempt to authenticate. 5. If the system fails to authenticate, then the system passes this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
200	**Section:** Authentication **ID:** 1.c The system shall be capable of protecting certificates that are trust points. Note: Methods used to protect trust points include restricting access to and use of this capability to designated individuals. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and ECPA-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1.3	1. Proceed to the permissions section of the system. 2. Verify that only the appropriate administrator has access to certificate configuration on the system.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
201	**Section:** Authentication **ID:** 1.d The system shall be capable of generating and submitting certificate requests in accordance with methods described in the DoD Class 3 PKI Interface specification. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1.1 and 4.3.2.2	1. Proceed to the certificate management section of the system. 2. Verify that valid certificates are designated for use in the system. 3. In the lab environment test certificates will be issued. 4. Establish a session between two components that requires the use DoD Class 3 PKI. 5. Confirm accepted certificates through the normal operation of the system. 6. An LoC noting the lab that provided the certification of this specific capability may be accepted. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
202	**Section:** Authentication **ID:** 1.d.1 The system shall be capable of using HTTPS to request and obtain certificates for the subscriber. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2 and DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.2.2	1. Verify that web services are used. 2. If web services are used, verify that certificates are exchanged. 3. Upon the establishment of the session, verify in the URL that the HTTPS session is established. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
203	**Section:** Authentication **ID:** 1.d.1.a The system shall be capable of encrypting and decrypting using the TDEA. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.3	1. Check the encryption configuration settings in the SUT. 2. Verify the system's ability to encrypt information using DoD PKI (TDEA/3DES). 3. Verify that the information can be properly decrypted on the receive end by establishing an encrypted session and viewing the decrypted session on the receivers end. (Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted. Also, this cannot be proven by the vendor within the context of AS-SIP.)	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
204	**Section:** Authentication **ID:** 1.e The system shall be capable of importing key pairs, related certificates, and certificate revocation information. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.1	1. Check to see that the system provides the functional capability to provide updating functions. 2. Proceed to the certificate configuration portion on the system. 3. Verify that the system is capable of importing key pairs, related certificates, and certificate revocation information.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
205	**Section:** Authentication **ID:** 1.e.1 The system shall be capable of using the Lightweight Directory Access Protocol (LDAP) or HTTP or HTTPS when communicating with the DoD PKI. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2 and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.2.4	1. Check which protocols the system uses for authentication when using the DoD PKI. 2. Proceed to the configuration tables. 3. If TCP/IP is used, verify that the LDAP protocol properly handles authentication. 4. Verify if web services are used. 5. If web services are used, check that they properly conduct DoD PKI certificate exchanges. 6. Upon establishment of the session, verify in the URL that the HTTPS session is established instead of a standard cleartext HTTP. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
206	**Section:** Authentication **ID:** 1.e.2 The system shall be capable of accepting needed old certificates (i.e., certificates that have expired or been revoked) and CRLs (Certificate Revocation List) (i.e., CRLs whose next update is after the current date) from the DoD PKI archive using HTTPS. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.2.4	1. Proceed to the certificate configuration section. 2. Verify that the system provides the capability to use old certificates and CRLs or to retrieve and receive DoD PKI archived certificates through using HTTPS. 3. Note how old certificates and CRLs are, that are allowed to be used. Note if this method is adjustable and not hard-coded. 4. Advance the system clock beyond the operating time limit of the current certificates. 5. Proceed to the certificate configuration file and configure the system to allow for the operation of the expired certificates. 6. Observe the ability of the system to retrieve DoD PKI archived certificates using HTTPS. 7. An LoC, noting the lab that provided the certification of this specific capability, may be accepted. Note: IPV testing will observe protocol traffic and handshake for establishing encrypted sessions. IPV testing will verify that the established session remains encrypted.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
207	**Section:** Authentication **ID:** 1.e.3 The system shall be capable of requesting and accepting information regarding the status of certificates using CRLs or an On-line Status Check (OSC). **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Origin:** DoD PKE 4.3.2.4	1. Identify a certificate of interest. 2. Cross check the certificates signature with the CRLs and OSCs to ensure validity and usefulness. 3. In the test lab environment, this procedure may be verified using the local test repositories. 4. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
208	**Section:** Authentication **ID:** 1.e.3.a If CRLs are used, the system shall be capable of using a configurable parameter to define the period associated with updating the CRLs. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Conditional:** MFSS, SS, LSC, MG, EBC, and R **Origin:** Vendor agreement	1. Confirm whether CRLs are used in the system. 2. If CRLs are used in the System, proceed to the certificate configuration and management section of the system. 3. Note that the configuration and management of the system provides for a configurable period for updating CRLs.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
209	**Section:** Authentication **ID:** 1.e.3.b If CRLs are used, the default value for the period associated with updating the CRLs shall be 24 hours. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Conditional:** MFSS, SS, LSC, MG, EBC, and R **Origin:** Vendor agreement	1. Proceed to the configuration and management section of the system. 2. Verify that the system default period for CRLs can be set to 24 hours.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
210	**Section:** Authentication **ID:** 1.e.4 If the EI is DoD PKE, it shall support a mechanism for verifying the status of an LSC certificate using a CTL or via the OSC. Note: It is understood that the systems administrator must ensure that the CTL is current to ensure that the status is accurate. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1	**Conditional:** EI **Origin:** Vendor feedback	1. Determine whether the EI is DoD PKE. 2. If the EI is DoD PKE, the EI must be able to verify certificates with a repository or local DoD PKE server to verify if certificates comply with CTLs or OSCs. 3. Note that when a session is established between the EI and LSC, the certificates from both elements are crosschecked against the repository for compliance with the CTLs and OSCs. 4. Note if rejection or non-compliance notification is received from the PKE server or if the session is not established. 5. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
211	**Section:** Authentication **ID:** 1.e.5 If the EI is DoD PKE, the LSC shall verify the status of an EI certificate using the CTL or an OSC. Note: It is understood that the systems administer must ensure that the CTL is current to ensure that the status is accurate. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2	**Conditional:** LSC **Origin:** Vendor feedback	1. Determine whether the EI is DoD PKE. 2. If the EI is DoD PKE, the LSC must be able to verify EI certificates with a repository or local DoD PKE server to verify if certificates are in compliance with CTLs or OSCs. 3. Note that when a session is established between the EI and LSC, the certificates from both elements are crosschecked against the repository for compliance with the CTLs and OSCs. 4. Note if rejection or non-compliance notification is received from the PKE server or if the session is not established. 5. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
212	**Section:** Authentication **ID:** 1.f The system shall be capable of performing public key operations necessary to verify signatures on DoD PKI signed objects (i.e., certificates, CRLs, and OSC responses). **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.3.1	1. Proceed to the section for DoD PKI configuration and management. 2. Verify that settings are enabled providing warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Establish a session using acceptable PKE. 4. Note normal operations. 5. Use an expired or non-compliant certificate. 6. Verify that non-compliance is noted on the system through a warning or lack of session establishment. 7. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
213	**Section:** Authentication **ID:** 1.f.1 The system shall be capable of producing SHA digest of messages to support verification of DoD PKI signed objects. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IATS-2 and DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.3.3	1. Verify that the algorithm takes an input message of arbitrary length and produces an output a 160-bit "fingerprint" or "message digest". 2. Use the digest, SHA1 module, to verify compatibility with the DoD PKI signed objects and DoD PKE server and system. 3. An LoC noting the lab that provided the certification of this specific capability may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
214	**Section:** Authentication **ID:** 1.f.2 The system shall reject all new sessions associated with a revoked certificate. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKI PMO recommendation	1. Proceed to the configuration and management section for DoD PKI settings. 2. Verify that settings are enabled that provide warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Establish a session using acceptable PKE. 4. Note normal operations. 5. Use a revoked (expired or non-compliant) certificate. 6. Verify that non-compliance is noted on the system through a warning or lack of session establishment. 7. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
215	**Section:** Authentication **ID:** 1.f.3 The system shall log when a session is rejected due to a revoked certificate. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Origin: :** DoD PKE 4.3.3 and 4.3.4.2	Examine the system log and verify that the system records session rejections for revoked certificates.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
216	**Section:** Authentication **ID:** 1.g The system 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 either when the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	1. Search the system for stored credentials of entities in the certificate path. 2. If credentials are found locally, archive them, and then remove them. 3. Remove connection to the DoD PKI. 4. Attempt messaging. It should fail. If the messaging is successful, then the system fails this requirement. 5. Restore connection to the DoD PKI. 6. Attempt messaging. If the messaging is successful, then the system passes this requirement.	CAT II	
	IA Control: IAKM	**Origin:** DoD PKE 4.3.3 and 4.3.4.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
217	**Section:** Authentication **ID:** 1.g.1 The system shall be capable of verifying certificate signatures using the certificate issuer's public key. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	1. Proceed to the certificate configuration and management section 2. Configure the system to accept symmetric keys. 3. Establish a session using symmetric certificates between two clients, appliances, or servers. 4. Note if the system successfully establishes the session using the certificate issuer public key. 5. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.4.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
218	**Section:** Authentication **ID:** 1.g.2 The system shall be capable of ensuring that the effective date falls within the certificate's validity period. Note: The effective date is the date when the transaction was initiated. Normally, the effective date should be considered to be the current date unless reliable evidence exists to establish an earlier effective date. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	1. Attempt to login using an expired certificate. If the system allows the use of expired credentials, then the system fails 2. When possible, attempt to login using a certificate that is valid in the future. If the system allows the use of credentials that are not yet valid, then the system fails. Note: The system must have a CAC or web server cert.	CAT II	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.4.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
219	**Section:** Authentication **ID:** 1.g.3 The path process shall fail when a problem that prohibits the validation of a path occur. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.4.2	1. Search the system for stored credentials of entities in the certificate path. 2. If credentials are found locally, archive them, and then remove them. 3. Remove connection to the DoD PKI. 4. Attempt to login. It should fail. If the messaging is successful, then the system fails this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
220	**Section:** Authentication **ID:** 1.g.4 The system shall be capable of ensuring the validity of certificates through a status check. Note: the status check is done at the time the certificate is presented to the appliance. Status checking involves checking the status of certificates in the path to ensure that none are revoked. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.4.2	1. Proceed to the configuration and management section for DoD PKI settings. 2. Verify that settings are enabled that provide warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Establish a session using acceptable PKE. 4. Note normal operations. 5. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
221	**Section:** Authentication **ID:** 1.g.4.a The system shall be capable of verifying the signature using the CRL or the OSC response. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.4.3	Attempt to login with a digital signature that has been revoked. If the login completes without error, then the system fails the requirement.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
222	**Section:** Authentication **ID:** 1.g.4.b If the system uses the OSC to validate a certificate and the system cannot contact the OSCR and backup OSCRs, the system will continue the process, but will log the event and send an alarm to the NMS. **Reference:** UCR 5.4.6.2.1.6	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and EI	1. Remove connection to the OSCR and backup OSCR. 2. Verify that the system allows login. 3. Verify that the system generates an alarm and logs the event.	CAT II	
	IA Control: DCNR-1 and ECAT-2	**Origin:** DoD PKE 4.3.4.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
223	**Section:** Authentication **ID:** 1.g.4.c The system shall be capable of verifying that the CRL has not expired (even if the target certificate has not expired) or shall be capable of verifying that the OSC response indicates the certificate is valid. Note: The intent of this requirement is to ensure that the OSCR or CRL is valid before completing the status check. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	Verify that the system is capable of determining the status of the CRL.	CAT II	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.4.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
224	**Section:** Authentication **ID:** 1.g.4.d The system shall be capable of searching the list of revoked certificates to determine that the target certificate is not included or the revocation date is after the effective date. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, R **Conditional:** EI	1. Proceed to the configuration and management section for DoD PKI settings. 2. Verify that settings are enabled to provide warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Establish a session using acceptable PKE. 4. Note normal operations. 5. Use a revoked /expired certificate. 6. Verify that non-compliance is noted on the system through a warning or lack of session establishment. 7. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
	IA Control: DCNR-1 and IAKM-2	**Origin:** DoD PKE 4.3.4.3			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
225	**Section:** Authentication **ID:** 1.g.4.e The system shall be capable of rejecting expired certificates. NOTE: An example of this case would exist if a certificate's effective date is reliable, but the certificate has since expired. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** DCNR-1 and IAKM-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.4.3 - CAT II	1. Proceed to the configuration and management section for DoD PKI settings. 2. Verify that settings are enabled that provide warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Establish a session using acceptable PKE. 4. Note normal operations. 5. Use a certificate whose effective date is valid, but the certificate has expired. 6. Verify that non-compliance is noted on the system through a warning or lack of session establishment. 7. An LoC, noting the lab that provided the certification of this specific capability, may be accepted.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
226	**Section:** Authentication **ID:** 1.g.4.f The system shall log an event if the certificate is rejected due to a status check. **Reference:** UCR 5.4.6.2.1.6 **IA Control**: IAKM-2 and ECAT-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Origin:** DoD PKE 4.3.4.3	1. Proceed to the configuration and management section for DoD PKI settings. 2. Verify that settings are enabled that provide warnings if certificates are rejected based on non-compliance with CRLs or OSCs. 3. Use a revoked (expired or non-compliant) certificate. 4. Verify that non-compliance is noted on the system through a warning or lack of session establishment. 5. Proceed to the security log. 6. Note that the rejected certificate event is recorded in the security log, due to a status check.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
227	**Section:** Authentication **ID:** 1.g.5 The system shall be capable of ensuring that the intended use of the certificate is consistent with the DoD PKI extensions. **Reference:** UCR 5.4.6.2.1.6 **IA Control:** IAKM-2 and IATS-2	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI **Origin:** DoD PKE 4.3.4.4	1. Review the DoD PKI extensions available to the system. 2. Attempt to have the system use a certificate for an action outside the scope of the extensions. 3. Verify that the action is rejected.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
228	**Section:** Authentication **ID:** 1.g.6 The system shall be capable of ensuring that the key usage extension in the end entity certificate is properly set. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	Verify that the system is capable of ensuring the proper setting of the key usage extension.	CAT II	
	IA Control: IATS-2 and IAKM-2	**Origin:** DoD PKE 4.3.4.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
229	**Section:** Authentication **ID:** 1.g.6.a The system shall be capable of ensuring that the digital signature bit is set for authentication uses. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	Verify that the system is capable of ensuring that the digital signature bit is set for authentication.	CAT II	
	IA Control: DCNR-1 and IAKM-2	**Origin:** DoD PKE 4.3.4.4 - CAT II			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
230	**Section:** Authentication **ID:** 1.g.6.b The system shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses. **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	Verify that the system is capable of ensuring that the non-repudiation bit is set for non-repudiation users.	CAT II	
	IA Control: DCNR-1	**Origin:** DoD PKE 4.3.4.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
231	**Section:** Authentication **ID:** 1.g.6.c The system shall be capable of ensuring that the "common name" and "subject alternate name" fields are populated. Note: The "subject alternate name" should be formatted in accordance with RFC 2459 and should contain as minimum the elements of the "common name." **Reference:** UCR 5.4.6.2.1.6	**Required:** MFSS, SS, LSC, MG, EBC, and R **Conditional:** EI	1. Attempt to login with either a malformed common name or unpopulated common name fields. 2. Attempt to login with either malformed subject alternate name or unpopulated subject alternate name fields.	CAT II	
	IA Control: IATS-2 and IAKM-2	**Origin:** Vendor agreement			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
232	**Section:** Authentication **ID:** 1 The system shall be capable of providing authorization for services accessed on the system. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Verify that the system is capable of providing authorization for services access on the system.	CAT I	
	IA Control: DCNR-1 and PRAS-2	**Origin:** OAM&P IA Req. M42			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
233	**Section:** Authentication **ID:** 1.a The system shall be capable of denying system access to any user unless identified with a user-ID and authenticated. Only authorized users shall be allowed system access. This holds for all users (i.e., persons, processes, or remote systems). NOTE: This requirement applies to multiple access types to include remote login, telephony services, and direct system access. However,911 and emergency service needs may result in this requirement being exempt on some end instruments. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Attempt to access the system with a user that is not identified with a user-ID. Example: Attempt to login with a unknown user-ID	CAT II	
	IA Control: IAIA-1	**Origin:** GIG MA ICD IV.B.2o; VoIP STIG 0067; GR-815 CORE R3-54[33], CR3-11[222], & R3-95[63]; and DRSN STIG 6.2.8.1.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
234	**Section:** Authentication **ID:** 1.b The system shall not allow the user to access a resource unless that user's user-ID has an appropriate privilege to access that resource. Note: Routine and above VVoIP sessions may be authorized for all users of the system and this feature may be disabled if the systems are located in secure facilities for precedence sessions. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	Attempt to access a resource that is not in the user-ID privilege level. A regular user cannot access system logs. If this is attempted, it should cause an error.	CAT I	
	IA Control: IAIA-1 and ECPA-1	**Origin:** GR-815-CORE CR3-55[37], CR3-11[222], R3-95[63], & R3-99[64]; and NSA 2.3.1 - CAT I			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
235	**Section:** Authentication **ID:** 1.b.1 The system 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. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, and LSC	1. Set up the originating EI with permissions not trusted by the destination IP phone number. 2. Set up the destination EI to only have permissions to receive IP phone calls from trusted IP sources. 3. Place the IP phone call from an untrusted source to the destinations phone number. 4. The IP phone call should not be established. Note: Protocol traffic is observed during IPV testing. IPV testing will verify that sessions are established or are dropped.	CAT II	
	IA Control: ECTM-2	**Origin:** DoDD 8500.1.4.4, 4.12; CJCSI 6215.01B A.7; CJCS 6510.01D B.4.b.2; B.9.d, GR-815-CORE R3-61[236] & R3-62[237]; and VoIP STIG 0150			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
236	**Section:** Authentication **ID:** 1.c The system shall be capable of regulating remote access by employing positive technical controls such as proxies and screened subnets. Note: Proxies and screened subnets are provided through the use of border controllers, access control lists, firewalls, and virtual LANs. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	Verify that the system can control remote access by employing proxies and screened subnets.	CAT II	
	IA Control: EBBD-2	**Origin:** DoDD 8500.1.4.4, 4.12; CJCSI 6215.01B A.7; CJCS 6510.01D B.4.b.2; B.9.d, GR-815-CORE R3-61[236] & R3-62[237]; and VoIP STIG 0150			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
237	**Section:** Authentication **ID:** 1.d The system shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for authenticated users and end instruments. Note: Proxies and screened subnets are provided using border controllers, ACLs, firewalls, and virtual LANs. Network service classes are defined by the QoS WG and may consist of voice, video, and data service classes. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	1. Proceed to the systems configuration section. In some cases, this may involve more than one appliance (i.e. EBCs, firewalls, servers, routers, etc.) 2. Note that the system provides for the capability to limit approved network service classes. 3. Note that the system provides for the capability to limit configured traffic levels for authenticated users and end instruments.	CAT II	
	IA Control: EBBD-2	**Origin:** DoDD 8500.1.4.4, 4.12; CJCSI 6215.01B A.7; CJCS 6510.01D B.4.b.2; B.9.d, GR-815-CORE R3-61[236] & R3-62[237]; and VoIP STIG 0150			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
238	**Section:** Authentication **ID:** 1.d.1 The system 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). **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	1. Proceed to the configuration section of the system under test. 2. Note that the system provides for regulation of traffic flow across an interface to the network. 3. Note that traffic flow may be regulated through source and destination IP address. 4. Note that traffic flow may be regulated through source and destination port number. 5. Note that QoS may be implemented through DSCP. 6. Note that traffic flow may be regulated through a protocol identifier ("6 tuple). Note: In-depth functionality and interoperability testing will be accomplished in the IO segment of testing.	CAT II	
	IA Control: EBBD-2	**Origin:** CJCSI 6510.01D B.4.b.2 & B.9.d			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
239	**Section:** Authentication **ID:** 1.d.1.a The system shall have the capability of opening and closing "gates/pinholes" (i.e., packet filtering based on the "6tuple") based on the information contained within the SDP body of the AS-SIP messages. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Proceed to the configuration panel of the system. 2. Note that the system has the capability to open and close gates and pinholes. 3. Note that the system provides for time intervals that the openings may be opened and closed. 4. Note the SDP of the AS-SIP message. Particularly note the instructions and time intervals for opening and closing gates and pinholes. Note: The IPV segment of testing will verify the proper opening and closing of gates and pinholes as well as monitor the AS-SIP packages passing through the system.	CAT II	
	IA Control: EBBD-2	**Origin:** CJCSI 6510.01D B.4.b.2 & B.9.d			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
240	**Section:** Authentication **ID:** 1.d.1.b The system 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. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Proceed to the configuration panel of the system. 2. Note that the system has the capability to open and close gates and pinholes based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP appliances. 3. Note that the system provides for time intervals that the openings may be opened and closed. 4. Note the SDP of the AS-SIP message. Particularly note the instructions and time intervals for opening and closing gates and pinholes. Note: The IPV segment of testing will verify the proper opening and closing of gates and pinholes based on inactivity parameters.	CAT II	
	IA Control: EBBD-2	**Origin:** CJCSI 6510.01D B.4.b.2 & B.9.d			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
241	**Section:** Authentication **ID:** 1.d.1.c The default media inactivity value for closing a session and issuing BYE messages shall be 15 minutes. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Proceed to the configuration panel of the system. 2. Note that the system has the capability to open and close gates and pinholes based on a configurable media inactivity timer and issue a BYE message to upstream and downstream AS-SIP appliances. 3. Note that the BYE message is capable of being sent based on 5 minutes of inactivity. Note: The IPV segment of testing will verify the proper opening and closing of gates and pinholes based on 5 minutes of inactivity.	CAT II	
	IA Control: EBBD-1	**Origin:** CJCSI 6510.01D B.4.b.2 & B.9.d			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
242	**Section:** Authentication **ID:** 1.d.2 The system shall be capable of utilizing VLANs to segregate VVoIP and data traffic. Servers requiring access to multiple VLANs shall be kept in a DMZ connected to the firewall and separating the two VLANs. Note: For the purposes of this UCR 2008, all streams of packets associated with a VTC session are considered video to include voice, video, and data streams. A DMZ in this context may exist between two VLANs within the edge segment. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	1. Verify that the system is capable of using VLANs to segregate VVoIP and non-VVoIP traffic. 2. Verify that servers requiring access to multiple VLANs are kept in a DMZ.	CAT I	
	IA Control: EBCR-1	**Origin:** VoIP STIG 0100; NSA 2.1.1 & 2.1.5; and DRSN STIG 5.1.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
243	**Section:** Authentication **ID:** 1.d.2.a The system shall be capable of supporting a minimum of five (5) distinct VLANs for VVoIP. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	Configure the system to support a minimum of five VLANs.	CAT III	
	IA Control: EBCR-1	**Origin:** VoIP STIG 0101 and NSA 2.1.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
244	**Section:** Authentication **ID:** 1.d.2.b The system shall be capable of ensuring that EIs (that do not contain a multi-port switch) and VVoIP appliances are only connected to switch ports with access to the VVoIP VLAN(s). Note: This requirement is not applicable to an EI with an embedded multi-port switch. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	Verify that the system is capable of ensuring that EIs and VVoIP appliances are only connected to switch ports with access to the VVoIP VLAN(s).	CAT III	
	IA Control: EBCR-1	**Origin:** CJCSI 6215.01C Enclosure C, Para. 2, pg. C-1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
245	**Section:** Authentication **ID:** 1.d.2.c If the system supports a data workstation, then the system shall be capable of supporting 802.1Q trunking to separate VVoIP and data traffic or shall have a separate 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 and to prevent the workstation from accessing the EI for configuration purposes. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** EI	1. Verify that the system supports trunking or has a separate NIC. 2. Examine the system's configuration files and confirm that the voice and data traffic has been separated by VLAN and tagging. 3. Verify that a workstation that is equipped with dual NICs can use one NIC for voice and the second NIC for data.	CAT II	
	IA Control: EBCR-1	**Origin:** VoIP STIG 0110: A concern with this requirement is that the EI does not act as a switch and that it is really a function of the LS, not the EI. The FSO will have to rule on this requirement since they came from the STIG.			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
246	**Section:** Authentication **ID:** 1.d.2.d If the system supports a data workstation, then the system shall be capable of using separate 802.1Q VLAN tags for VVoIP and data or shall use separate NICs for the data and VVoIP interfaces. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** EI	1. Verify that the system supports VLAN tagging by connecting a network sniffer to the network interface. 2. Monitor the traffic and verify that 802.1q tagging is being used to isolate the traffic.	CAT II	
	IA Control: DCPA-1	**Origin:** VoIP STIG 0111 103			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
247	**Section:** Authentication **ID:** 1.d.2.e If the system 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 it involved marking the packet and this requirement was focused on what action to take based on the marking or the output NIC. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** DCPA-1	**Conditional:** EI **Origin:** VoIP STIG 0111	1. Verify that the system supports a data workstation. 2. Set the network interface of the test laptop to the VLAN of the VVoIP systems. 3. Connect a network sniffer and verify that VVoIP only traffic is passed through this VLAN.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
248	**Section:** Authentication **ID:** 1.d.2.f The system shall be capable of configuring the maximum number of MAC addresses that can be dynamically configured on a given switch port (e.g., 1-3). **Reference:** UCR 5.4.6.2.1.7 **IA Control:** DCCS-1	**Required:** R and LS **Origin:** VoIP STIG 0127	1. Verify that the system is able to configure a maximum number of MAC addresses on a given switch port. 2. The vendor should configure the test access port for the maximum number of MAC addresses allowed.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
249	**Section:** Authentication **ID:** 1.d.2.g The system shall be capable of notifying the NMS when MAC addresses tables threshold is reached to avoid an overflow. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** DCCS-1	**Required:** R and LS **Origin:** VoIP STIG	1. Proceed to the MAC address tables. 2. Note the maximum number of MAC addresses that may be assigned. 3. Attempt to add an additional MAC address above the allotted amount. 4. Verify that an alarm or warning is sent to the NMS indicating that MAC addressing threshold has been exceeded.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
250	**Section:** Authentication **ID:** 1.d.2.h The system shall be capable of segregating softphones to a dedicated VLAN. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** DCPA-1	**Required:** R and LS **Origin:** NSA Guidance & 2.4.6; and VoIP STIG 150	Verify that the system is capable of segregating softphones to a dedicated VLAN. (Note: The VoIP STIG requires the laptop containing the softphone configured to a VLAN and requires separate NICs for data and voice. They must be 802.1q compatible NICs. The NSA Security Guide For Deploying IP Telephony Systems contradicts this!) The IPV test team will execute the following test. 1. Confirm that a separate VLAN for softphones was created. 2. Configure the test laptop to a voice VLAN. 3. Verify that test calls can be completed over the VLAN.	CAT I	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
251	**Section:** Authentication **ID:** 1.d.2.i The system shall be capable of segregating signaling appliances to a dedicated VLAN. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	Verify that the system is capable of segregating signaling appliances to a dedicated VLAN.	CAT II	
	IA Control: DCPA-1	**Origin:** NSA 2.1.5 Table			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
252	**Section:** Authentication **ID:** 1.d.2.j The system shall be capable of segregating PSTN gateways to a dedicated VLAN. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	Verify that the system is capable of segregating PSTN gateways to a dedicated VLAN.	CAT III	
	IA Control: DCPA-1	**Origin:** NSA 2.2.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
253	**Section:** Authentication **ID:** 1.d.2.k The system shall be capable of segregating NMS appliances on a separate VLAN. **Reference:** UCR 5.4.6.2.1.7	**Required:** R and LS	Verify the system is capable of segregating NMS appliances on a separate VLAN.	CAT II	
	IA Control: DCPA-1	**Origin:** NSA 2.3.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
254	**Section:** Authentication **ID:** 1.d.3 The system shall have the capability to deploy on a dedicated IP network(s) that use separate address blocks from the normal data address blocks, thus allowing traffic and access control via firewalls and router ACLs. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	Verify that the system has the capability to deploy, on a dedicated IP network that uses separate address blocks, from the normal data address block, thus allowing traffic and access control via firewalls and router ACLs.	CAT I	
	IA Control: DCPA-1	**Origin:** VoIP STIG 0070			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
255	**Section:** Authentication **ID:** 1.d.3.a The system shall be capable of using NAT and NAPT on all VVoIP enclave to WAN connections. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	Verify that the system is capable of using NAT or NAPT on all VVoIP enclave to WAN connections.	CAT II	
	IA Control: DCCS-2	**Origin:** VoIP STIG0190 and NSA 2.2.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
256	**Section:** Authentication **ID:** 1.d.3.a.i The system shall have the capability to deploy using private address space in accordance with RFC 1918. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC and R	1. Verify the system has the ability to use a private address space in accordance with RFC 1918. 2. Verify the system has the ability to use a private address space. 10.0.0.0 (10/8 prefix) 172.16.0.0-(172.16/12 prefix) 192.168.0.0-(192.168/16 prefix).	CAT III	
	IA Control: DCCS-2	**Origin:** VoIP STIG 0080			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
257	**Section:** Authentication **ID:** 1.d.3.a.ii The EBC shall be an AS-SIP intermediary in all WAN signaling sessions. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Calls should be placed from one LSC, through the EBC and terminating at another LSC. 2. Verify that the NAT procedures were performed properly. Also confirm that associated pinholes were opened and closed. Note: This test will be confirmed through the IPV testing.	CAT II	
	IA Control: EBBD-2	**Origin:** VoIP STIG section 2.2, 2.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
258	**Section:** Authentication **ID:** 1.d.3.a.ii.A 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. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. While monitoring (sniffing) the AS-SIP traffic, calls should be attempted that perform media shaping. In addition, call forwarding should be attempted. 2. Verify that the SDP information was modified by the EBC via B2BUA functions. Note: IPV testing will confirm.	CAT II	
	IA Control: EBBD-2	**Origin:** VoIP STIG section 2.2, 2.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
259	**Section:** Authentication **ID:** 1.d.3.a.iii If the system supports H.323 video sessions, the EBC shall be capable of supporting H.323 NAT and NAPT. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** EBC and R	1. Originate an H.323 VTC that traverses the EBC. 2. Confirm that the SDP of the INVITE message reflects the information that NAT or NAPT procedures are in effect. Note: IPV testing will confirm.	CAT II	
	IA Control: EBBD-2	**Origin:** DVS Request			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
260	**Section:** Authentication **ID:** 1.d.3.b The system shall have the capability to be configured to ensure that the data network perimeter (i.e., data edge router or data perimeter firewall) blocks all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space. Note: The VVoIP VLANs may include a softphone VLAN, a non-softphone voice VLAN, and an video VLAN. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	Verify that the system has the capability to be configured to block all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space.	CAT I	
	IA Control: EBBD-2	**Origin:** VoIP STIG 0095			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
261	**Section:** Authentication **ID:** 1.d.3.c The system shall have the capability to limit management appliance access to the IP addresses of appropriate workstations. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R and LS	1. Confirm that the system has the ability to limit management access to specific IP addresses. 2. If not, this test fails. 3. If the system has this capability, remove the IP address of the workstation from this list and attempt a management access. 4. Access should be denied.	CAT I	
	IA Control: EBBD-2	**Origin:** NSA 2.3.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
262	**Section:** Authentication **ID:** 1.d.4 If DHCP is used, the system shall have the capability to deploy different DHCP servers for VVoIP and non-VVoIP components and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R and LS	Verify that, if DHCP servers are used, separate servers are used for VVoIP and non-VVoIP systems.	CAT I	
	IA Control: DCCS-2 and DCPA-1	**Origin:** VoIP STIG 0082			
Test Case	**Requirement**	**System(s) Affected**		**Risk**	**Result(s)**
263	**Section:** Authentication **ID:** 1.d.5 If DHCP is used, DHCP servers shall reside in their respective VVoIP or non-VVoIP address space and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R and LS	Verify that DHCP servers reside in their respective VVoIP or non-VVoIP address space and are located on physically diverse platforms from the routers and LAN switches.	CAT II	
	IA Control: DCPA-1	**Origin:** NSA 2.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
264	**Section:** Authentication **ID:** 1.d.5.a If DHCP is used, the system shall be capable of using 802.1X in combination with a secure EAP (EAP-TLS, EAP-TTLS, or PEAP) residing on the authentication server and within the operating system or application software of the EI in order to authenticate to the LAN. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R, LS, and EI	1. Check to see if DHCP is used. If yes, move on to step 2. 2. Verify that the system is capable of using 802.1 X in combination with a secure EAP.	CAT I	
	IA Control: DCSR-1	**Origin:** FSO clarification. Only the three listed EAP types are allowed. Other types have unacceptable vulnerabilities			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
265	**Section:** Authentication **ID:** 1.d.5.a.i If 802.1X port authentication is used, the system shall ensure that all access ports start in unauthorized state. Note: The system should set AuthControlledPortControl equal to Auto mode for ports that will support VVoIP. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R and LS	Vendor should verify that ports are set to auto mode for ports that will support VVoIP.	CAT I	
	IA Control: ECRC-1	**Origin:** FSO clarification			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
266	**Section:** Authentication **ID:** 1.d.5.a.ii If 802.1X port authentication is used, the system shall ensure that re-authentication occurs every 60 minutes. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R, LS, and EI	1. Connect VVoIP system and verify that port security is enabled. 2. Use a sniffer to verify that port security re-authenticates every 60 minutes.	CAT II	
	IA Control: ECLO-1	**Origin:** FSO clarification			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
267	**Section:** Authentication **ID:** 1.d.5.a.iii If 802.1X port authentication is used, the system shall also use 802.1AE and 802.1AF to ensure a continuation of the authenticated relationship continues after the 802.1X authentication event to prevent parallel attacks. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** R, LS, and EI	Verify that if 802.1X port authentication (port security) is used, 802.1AE (MAC security) and 802.1 AF (MAC Key security) are also used.	CAT II	
	IA Control: DCFA-1	**Origin:** VoIP STIG section 3.5.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
268	**Section:** Authentication **ID:** 1.d.6 The system shall be capable of being configured to ensure that VVoIP and non-VVoIP traffic between their respective VLANs is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services. Note: The EBC used in this case may not have the full feature set of an EBC. For instance, NAT is not required in this instance. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Determine VVoIP and non-VVoIP VLANs. 2. Set testing laptop to tag VVoIP VLAN. 3. Start a network sniffer to verify that only VVoIP traffic passes.	CAT II	
	IA Control: EBBD-2 and ECTM-2	**Origin:** VoIP STIG 0116, 0090, 0115, 0102; and NSA 2.1, 2.1.4, 2.2.1			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
269	**Section:** Authentication **ID:** 1.d.7 The system shall have the capability to deploy VVoIP-aware firewalls at all VVOIP-enclave-to-WAN boundaries. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	Verify that the system has the capability to deploy VVoIP aware firewalls at all VVoIP-enclave-to-WAN boundaries.	CAT II	
	IA Control: EBBD-2	**Origin:** VoIP STIG 0180			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
270	**Section:** Authentication **ID:** 1.d.7.a The system firewalls deployed at the boundaries of the VVoIP enclave shall have the capability to employ stateful packet inspection. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	Verify that the firewall has the ability to perform stateful packet inspection.	CAT II	
	IA Control: EBBD-2	**Origin:** VoIP STIG 0180			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
271	**Section:** Authentication **ID:** 1.d.7.b The system firewalls deployed at VVoIP enclave boundaries shall have the capability to be dedicated to VVoIP traffic. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC	1. Verify that system firewalls are dedicated to VVoIP. 2. Open firewall application and verify that only VVoIP equipment is or can be selected.	CAT III	
	IA Control: EBBD-2	**Origin:** VoIP STIG 0200			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
272	**Section:** Authentication **ID:** 1.d.7.c The system shall be capable of implementing traffic conditioning at all VVoIP enclaves associated with the system. Note: This includes limiting the bandwidth associated with external sessions. **Reference:** UCR 5.4.6.2.1.7	**Required:** R	Verify that the system is capable of implementing traffic conditioning.	CAT III	
	IA Control: EBBD-2	**Origin:** Consistent with VVo IP Appliance Functions and NSA 2.1.4			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
273	**Section:** Authentication **ID:** 1.e The system documentation shall list all of the IP ports and protocols required by the system and the boundaries they transit as defined in the PPS Assurance Category Assignments List and which is maintained by DISA and is described in DoDI 8551.1. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that the system documentation lists all ports and protocols in use by the system. 2. Run a port scan on the system using a system port scanner. 3. Compare results against system documentation. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: DCPP-1	**Origin:** Network STIG section 4.4, NET0910			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
274	**Section:** Authentication **ID:** 1.e.1 The system shall not use deemed IP ports and protocols deemed '"red" as defined by the PPS Assurance Category Assignments List, which is maintained by DISA and described in DoDI 8551.1 **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Run a system port scanner. 2. Review results for ports or protocols deemed "red." If these procedures are not met, the system fails this requirement.	CAT III	
	IA Control: DCPP-1	**Origin:** Network STIG section 4.4, NET0910			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
275	**Section:** Authentication **ID:** 1.f Systems that support critical commands, operational commands, or critical objects shall be capable of establishing access privileges for these objects and commands. Critical objects include authentication data storage. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, BC, R, and LS	1. Verify that systems that support critical commands are capable of establishing access privileges for objects and commands. 2. Check objects and commands to verify that privileges can be set to read and/or write.	CAT II	
	IA Control: ECPA-1	**Origin:** GR-815 CORE CR3-35[22], CR3-36[23], CR3-11[222], R3-98[250], and R3-99[64]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
276	**Section:** Authentication **ID:** 1.f.1 The default policy on a system that supports operations-related or critical commands shall be capable of disallowing command issuance unless the issuer is authenticated and authorized to use that command. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** DCFA-1, ECPA-1, and ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-96[248], R3-97[249], and R3-98[250]	1. Retrieve the database containing user-attributes, and check, whether each user-ID has an assigned code specifying the associated level of privilege. If no such privilege can be assigned to a user-ID, the system fails the test. 2. Retrieve the database containing the operations-related commands and verify whether for any command, a privilege can be assigned to specify the authority levels required of the user-ID to execute that command. If there is any operations-related command to which any specified privilege cannot be assigned, the system fails the test. 3. Establish a login as an administrator. Arbitrarily select a command <C>, and assign a privilege code <P> to that command. 4. Create two user-IDs <U1> and <U2>, assign them privileges <P> and <Q> respectively. 5. Check whether the execution of command<C> is allowed only when U1 and denied to U2. If not, the system fails the test. 6. Establish a login as a user whose privilege is lower than that of an administrator. 7. Attempt the command that enhances the privilege of the user to that of an administrator. If system executes this command and the user is able to elevate his/her privilege to that of the administrator, then system fails the test.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
277	**Section:** Authentication **ID:** 1.f.1.a Assigning passwords to specific actions shall not be used as a primary access method. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECAN-1, ECPA-1, and ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-100[65]	1. Determine if the system has critical type commands associated with it. (e.g., SET for SNMP, reboot, etc.) 2. Attempt to execute one of these critical commands while logged in as an administrator who would normally be authorized to execute these types of commands. 3. Change the password of this administrator and attempt to execute the same command in step 1. There should be no difference. 4. Attempt to execute the same command while logged in as a normal user. The attempt at executing the critical command should be denied.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
278	**Section:** Authentication **ID:** 1.f.2 All ports of the system that accept operations or critical command inputs shall be capable of exercising system-access control. This includes ports that provide direct access, dial-up access, access via a wireless interface, network access, and access via a Data Communications Channel (DCC) as in the case of an Add Drop Multiplexer (ADM) in a Synchronous Optical Network (SONET). **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	This test is associated with privileges associated with specific ports or interfaces into the system. For example, the NM Ethernet port should only handle NM-related commands. 1. Determine all management ingress ports on the system. 2. Confirm that any attempt to access these ports will result in system access controls (i.e., login credentials) being required for access.	CAT I	
	IA Control: DCFA-1, ECPA-1, and ECLP-1	**Origin:** GR-815 CORE R3-96[248]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
279	**Section:** Authentication **ID:** 1.f.2.a Depending on the application, if the system 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 system shall be capable of providing a separate interface/port for such confidential access and shall be capable of ensuring that messages (including login 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. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Determine whether the system provides special administrative access for authorized users whose identity should not be disclosed. 2. If the system does not, then this test is not applicable. 3. Verify that when the system provides for these special administrators, identification and authentication standards, the authorized user information is stored in a separate security log, which is not accessible by other administrators or users.	CAT II	
	IA Control: ECPA-1	**Origin:** GR-815 CORE CR3-102[67]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
280	**Section:** Authentication **ID:** 1.f.2.b The system shall be capable of controlling access to resources over a given interface/port on the basis of privileges assigned to that interface/port. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Confirm that privileges to resources are accessible only through associated privileges granted by the system. 2. If the system uses ACLs as the main access control, confirm that ACLs are in place to control access to ports and resources only to those users/services that require the access.	CAT III	
	IA Control: ECLP-1	**Origin:** GR-815-CORE CR3-104[69]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
281	**Section:** Authentication **ID:** 1.g The system shall have the capability of monitoring the flow of traffic across an interface to the network. **Reference:** UCR 5.4.6.2.1.7	**Required:** EBC, R, and LS	1. On the interface of interest, install an unmanaged hub. 2. Configure a laptop with network sniffing capabilities and interface the laptop using the hub. 3. Monitor traffic as needed. Note: The IPV test team will perform these tests.	CAT II	
	IA Control: ECMT-1	**Origin:** CJCSI 6510.01D B.4.b.2 and B.9.d -			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
282	**Section:** Authentication **ID:** 1.h The system shall have the capability to provide a secure method for allowing automatic interconnections. Note: Automatic interconnection is only allowed between an incoming long-distance DSN call and the local commercial system (off-netting). **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify the system has the capability to provide a secure method for allowing interconnections. 2. If the system supports the DISA feature, make a DISA call. 3. Confirm that the caller is required to use a PIN to access this feature. 4. Verify that the PIN is not sent in the clear. 5. Confirm the fact that this user has made this call. There should be an entry in the event log file.	CAT III	
	IA Control: DCCS-2	**Origin:** CJCSI 6215.01B A.7.b.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
283	**Section:** Authentication **ID:** 1.h.1 Automatic interconnection between DoD IP VVoIP calls and local commercial systems shall only be permitted with proper authorization. Note: The authorization is granted based on successful authentication in combination with an acceptable profile allowing the interconnection. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify that calls between DoD IP VVoIP and local commercial systems are permitted with authorization only. 2. If the system supports the DISA feature, make a DISA call. 3. Confirm that the caller is required to use a PIN to access this feature. 4. Verify that the PIN is not sent in the clear. 5. Confirm the fact that this user has made this call. There should be an entry in the event log file.	CAT III	
	IA Control: DCID-1	**Origin:** CJCSI 6215.01B a.7.b.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
284	**Section:** Authentication **ID:** 1.h.2 The system shall have the capability of identifying all calls made through the automatic interconnection. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify that all calls made through the automatic interconnection can be verified. 2. If the system supports the DISA feature, make a DISA call. 3. Confirm that the caller is required to use a PIN to access this feature. 4. Verify that the PIN is not sent in the clear. 5. Confirm the fact that this user has made this call. There should be an entry in the event log file.	CAT III	
	IA Control: DCFA-1	**Origin:** CJCSI 6215.01B a.7.b.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
285	**Section:** Authentication **ID:** 1.h.3 The system shall be capable of ensuring that all automatic calls are periodically verified by the user. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	Verify that the user is able to verify all automatic calls.	CAT III	
	IA Control: DCFA-1	**Origin:** CJCSI 6215.01B a.7.b.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
286	**Section**: Authentication **ID:** 1.i The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes 24X7 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. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the NMS has the ability to control read-access and write-access to DoD IP VVoIP database tables. 2. The local policy should include management roles and responsibilities.	CAT I	
	IA Control: IAIA-1 and COMS-2	**Origin:** CJCSI 6215.01B A.9.a			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
287	**Section**: Authentication **ID:** 1.j The system shall have the capability to provide an identification system that allows the operators to detect and prevent disruptive fraud, abuse, and compromise within 30 minutes. (Definition or disruptive is found in UCR 2008, Appendix A, Definitions Abbreviations and Acronyms, and references. Note: The threats associated with this requirement are summarized earlier in this UCR 2008. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	1. Authenticate to the system as a trusted user and attempt to access unauthorized information. Observe the behavior. 2. Attempt authentication as an authorized user using invalid passwords as if attempting to guess a user's password and observe the response. 3. Verify that the system has taken action to identify these actions or lock out the account such that Administrator action is taken within the required period. 4. The IPV test section will address this particular requirement by performing session hijacking, corruption of data, and unauthorized access to data. 5. Attempts to replicate those threats mentioned in the IA UCR, table 3.3.2.1-4 will be performed by the IPV test team.	CAT II	
	IA Control: ECTM-2 and ECAT-1	**Origin:** CJCSI 6215.01C 7.f.3.b			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
288	**Section**: Authentication **ID:** 1.j.1 The system shall have an identification system that allows operator to detect a disruptive fraud, abuse, or compromise within 5 minutes. Note: The threats associated with this requirement are summarized in this UCR 2008 section. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, and EBC	1. Authenticate to the system as a trusted user and attempt to access unauthorized information. Observe the behavior. 2. Attempt authentication as an authorized user using invalid passwords as if attempting to guess a users password and observe the response. 3. Verify that the system has taken action to identify these actions or lock out the account such that Administrator action is taken within the required time frame. 4. The IPV test section will address this particular requirement by performing session hijacking, corruption of data, and unauthorized access to data. 5. Attempts to replicate those threats mentioned in the IA UCR, table 3.3.2.1-4 will be performed by the IPV test team.	CAT II	
	IA Control: ECMT-1	**Origin:** CJCSI 6215.01C 7.f.3.b			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
289	**Section**: Authentication **ID:** 1.k The system 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 an SSH session. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, and EBC	1. Confirm that all ports that are not being used or are not needed for the operation of the system are disabled by default. 2. Perform an SSH session to the system. 3. From the NMS, disable the ingress port used for the SSH access. 4. Verify that SSH access is now disallowed.	CAT III	
	IA Control: ECND-2	**Origin:** GR-815 CORE CR3-55[37]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
290	**Section**: Authentication **ID:** 1.l If the system provides an emergency entry port (Emergency Action Interface) with system access control, the system shall have the capability to meet the following requirements: **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Confirm whether the system has an EEP. 2. If not, this test is not applicable. 3. If the system does have an EEP, verify that access to this port must include strong authentication. For example, using either one-time passwords, biometric authentication, or cryptographic authentication.	CAT III	
	IA Control: DCBP-1	**Origin:** GR-815-CORE R3-70[245]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
291	**Section:** Authentication **ID:** 1.l.1 The system shall be capable of using strong authentication. Reference: UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Access the EEP Login procedure. 2. Determine if the system uses strong authentication methods such as two-factor authentication. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: DCBP-1	**Origin:** Access Control STIG 3.4.6 and NET0310			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
292	**Section**: Authentication **ID:** 1.l.2 The system shall log all access attempts in an audit log. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, BC, R, and LS	1. Login at the EEP. 2. Verify the login has been recorded in the security log.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815-CORE R3-71[246]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
293	**Section:** Authentication **ID:** 1.l.3 The system shall be capable of ensuring that at least one, and not more than two, system security administrators cannot be locked out due to login failures. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system is capable of ensuring that at least one, but no more than two, accounts for system security administrators cannot be locked out due to login failures.	CAT II	
	IA Control: IAIA-1	**Origin:** DRSN STIG 6.2.8.1.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
294	**Section:** Authentication **ID:** 1.m If the system provides an emergency entry port without system access control, then the following requirements are met. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Confirm whether an EEP port exists on the system. If not, this test is an not applicable. 2. Determine the use of the EEP and verify that the EEP will not support any additional uses. (e.g., EEP port functionality is strictly for system restart, attempt a non-system restart command.)	CAT II	
	IA Control: COBR-1 and ECND-1	**Origin:** GR-815 CORE CR3-74[39] - CAT II			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
295	**Section:** Authentication **ID:** 1.m.1 The system emergency entry port shall recognize only those commands that performs system restoration (for example, from a disk) and no other operations commands. Reference: UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Logon on the EEP. 2. Verify that the EEP only accepts system restoration commands. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: ECND-2	**Origin:** GR-815 CORE CR3-74[39]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
296	**Section:** Authentication **ID:** 1.m.2 The system shall generate a real real-time alarm/alert when this port is used to gain access to the system and transmit that alarm to the appropriate NOC. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Logon on the EEP. 2. Verify that a real-time alarm is generated; notifying the administrator the EEP has been accessed. Also, verify the access is recorded in the security log.	CAT II	
	IA Control: ECAT-2 and ECND-2	**Origin:** GR-815 CORE CR3-73[38]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
297	**Section:** Authentication **ID:** 1.n The system 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 login request, the system shall not respond. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Install a non-managed hub in a valid SIP signaling interface. 2. Connect the IPV test laptop to the hub. 3. Attempt to access the management webpage or CLI of the system. 4. If access is allowed, this is a finding. The IPV test team will examine this requirement.	CAT II	
	IA Control: DCFA-1	**Origin:** GR-815 CORE R3-75[40]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
298	**Section:** Authentication **ID:** 1.o The system shall be capable of providing a time-out feature for users of the system. This implies that, if during a session, there has not been any exchange of messages for a specified period of time, the system shall lock out that session for subsequent inputs (or re-authenticate user before accepting subsequent inputs). **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. At each ingress, establish a successful login and advance the clock to exceed the timed-out session envelope. If the session is not timed out, the system fails the test. 2. Verify the session can be re-initiated by providing the authenticator. If not, the system fails the test.	CAT II	
	IA Control: PESL-1	**Origin:** GR-815-CORE R3-88[56]; OAM&P IA Req. M59 & M60; and CJCSI 6510.01D A.A.7.b.14			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
299	**Section:** Authentication **ID:** 1.o.1 The default for session inactivity is 15 minutes and shall be configurable. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Determine the access method for management. This could be via CLI, Web Access, Operating System Application, or all of the above methods. 2. For each method that is used in the system, login to the management service. 3. Confirm that the session expires after 15 minutes of inactivity and re-authentication is required to start a new management session.	CAT III	
	IA Control: PESL-1	**Origin:** GR-815 CORE R3-89[57]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
300	**Section:** Authentication **ID:** 1.o.2 If the system uses a keyboard, the system shall be capable of providing a mechanism for user-initiated keyboard locking. When a keyboard is locked, the session time-out feature shall be suspended. The unlocking of a locked keyboard shall require authentication (e.g., entering the password). When the keyboard is unlocked, the session time-out feature shall be resumed. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. At each terminal, verify the mechanism to lock the keyboard. If there is not one, the system fails. 2. Determine the access method for management. This could be via CLI, Web Access, or Operating System Application. 3. Using whichever of the above is used for management (even all three), login to the management service. 4. Perform a user-initiated keyboard lock. Leave the keyboard locked more than 15 minutes. 5. Verify that unlocking the keyboard requires authentication. 6. Also, verify that the management session started in step 3 is still active. If not, this test fails.	CAT III	
	IA Control: PESL-1	**Origin:** GR-815-CORE R3-90[58]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
301	**Section:** Authentication **ID:** 1.o.3 If the system does not use a keyboard (i.e., SSH or other type of remote NMS session), the system shall terminate the session and automatically log the user out after the session inactivity timer has expired. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Connect to the system (via SSH or other remote NMS means). Initiate a NMS session. 2. After waiting for the required time-out period, verify that the system has terminated the session, or logged out the user.	CAT III	
	IA Control: PESL-1	**Origin:** DRSN STIG 6.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
302	**Section:** Authentication **ID:** 1.p The system shall be capable of providing a mechanism to end a user session through a secure logoff procedure. This implies that when a user terminates a session by logging off, the system shall be capable of ensuring that the port drops immediately and the processes running at the time of logoff are terminated. When a subsequent user attempts to log on to that port, the user shall be required to go through the entire login procedure including identification and authentication, and shall not be granted automatic access (i.e., bypassing the login procedure) to any process invoked by the previous user. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Determine the access method for management. This could be via CLI, Web Access, Operating System Application, or all of the these methods. 2. For each method that is used for management in the system, login to the management service. After authentication and authorization completes, perform a process list command on the system and save the results for later use. 3. Perform a secure logoff. 4. Perform another process list on the system and compare the results with the previous list. Confirm that the processes that were associated with the login process are no longer active. 5. Verify attempts to re-establish a session requires the entire logon and authentication procedures.	CAT II	
	IA Control: DCFA-1	**Origin:** GR-815 CORE R3-91[59]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
303	**Section:** Authentication **ID:** 1.q The system shall be capable of dropping a port immediately if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described above shall be required of a subsequent session request. Note: Serial ports must drop the session immediately. A delay in dropping the session may occur with Ethernet connections due the nature of the TCP keep alive capabilities that may appear to keep the session alive. When the disconnected Ethernet connection is attempted to be used to pass data, the connection should drop. If the session drop in not induced by the application, the session should eventually drop on its own once the keep alive fails. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. During each ingress, establish a successful login. 2. Disconnect the cable connecting the workstation to the system. 3. Connect it back again, and check if a login is needed to establish a session. If a login is not needed (i.e., if the previous session did not terminate as a result of the cable disconnection), the system fails the test.	CAT I TDM/Serial or CAT II Ethernet	
	IA Control: DCFA-1	**Origin:** GR-815 CORE R3-92[60]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
304	**Section:** Authentication **ID:** 1.r Depending on the application, if the system employs external modems to perform dial/dial-back, the corresponding modems shall be capable of having the following characteristics: **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	If the system employs an external modem to perform dial/dial-back, verify the modem, after receiving a call from a session requestor, disconnects the line before dialing the authorized number to reestablish the contact.	CAT II	
	IA Control: EBRP-1 and EBRU-1	**Origin:** Network STIG section 5.2.4			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
305	**Section:** Authentication **ID:** 1.r.1 The Modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to reestablish the contact. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Access the remote dial in/dial back configuration, or observe the remote dialing process. 2. Verify that the remote dial back process disconnects the line, before dialing back the authorized number. If these procedures are not met, the system fails this requirement.	CAT II	
	IA Control: ECSC-1, EBRU-1 and EBRP-1	**Origin:** Network STIG Section 5.2.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
306	**Section:** Authentication **ID:** 1.r.2 The dial-back shall be performed over a line different from the line over which the session request arrived at modem. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	If the system employs an external modem to perform dial/dial-back, verify the dial-back is performed over a different line from the line over which the session request arrived at the modem.	CAT II	
	IA Control: EBRU-1 and EBRP-1	**Origin:** DSN STIG section 3.3.12			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
307	**Section:** Authentication **ID:** 1.r.3 A loss of power to the modem shall not cause the modem to fall back to a default password. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	If the system employs an external modem to perform dial/dial-back, verify that a loss of power does not allow the modem to fall back to the default password.	CAT I	
	IA Control: DCCS-1 and DCSS-2	**Origin:** Network STIG section 5.2.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
308	**Section:** Authentication **ID:** 1.r.4 The password file in the modem shall not be readable by a user. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	If the system employs an external modem to perform dial/dial-back, verify that the password file is not stored in clear text.	CAT I	
	IA Control: IAIA-1	**Origin:** Network STIG section 5.2.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
309	**Section:** Authentication **ID:** 1.r.5 The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and authorized for this action. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG,EBC, R, and LS	If the system employs an external modem to perform dial/dial-back, verify the modem does not allow modification of its stored configuration unless the user is properly authenticated and authorized.	CAT I	
	IA Control: IAIA-1	**Origin:** DSN STIG 3.3.3.2			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
310	**Section:** Authentication **ID:** 1.s The system shall be capable of limiting the access to newly created resources in conformance with the privilege of the creator of the resource. This should be the default configuration. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE CR3-103[68]	1. Login to the system as an Administrator. 2. Create a temporary resource. The resource should inherit the privileges of the creator. Confirm the access attributes of the resource (read, write, execute). 3. Log off. 4. Login as a normal user and attempt to access the resource created in step 2. 5. Confirm that a normal user does not have the same access to the resource created by an Administrator because of the privilege level of the creator. If access is possible, this test fails.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
311	**Section:** Authentication **ID:** 1.t If the application requires the system to provide different interfaces/ports for different functions, access to system resources over a given interface/port shall be controlled on the basis of privileges assigned to that interface/port. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-104[69] & R3-107[72]	1. If the application does not require different interfaces/ports for different functions, this test is not applicable. 2. Verify ACLs are in place to control access to ports and resources. 3. Attempt to perform a function on an interface/port that is disallowed due to privilege restrictions on the interface/port.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
312	**Section:** Authentication **ID:** 1.u The system shall be capable of providing a level of granularity such that, for any specified resource controlled by the system (to include precedence calls), it shall be possible to do the following: **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-105[70]	1. Login as administrator and create an grant access privileges for a specific resource for an individual user. 2. Confirm that the individual user has access and privileges to the resource created. 3. Confirm the normal user does not have the same access capabilities to this resource as the creator (admin). 4. Without changing access privileges on the user, move the user into the "Administrator" group. 5. Verify the user now has the ability to access and change the resource.	CAT II	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
313	**Section:** Authentication **ID:** 1.u.1 Grant access rights to a specified user/customer group of users/customers. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-105[70]	1. Verify the ability to deny access rights to a specified user/customer or a group of users/customers. 2. Login as administrator and create an grant access privileges for a specific resource for an individual user. 3. Confirm that the individual user has access and privileges to the resource created. 4. Confirm the normal user does not have the same access capabilities to this resource as the creator (admin). 5. Without changing access privileges on the user, move the user into a group that does not have administrative privileges. 6. Attempt to perform administrative functions on a specified resource. Verify the user does not have the ability to access and change the resource in the manner an administrator would. If these procedures are not met, the system fails this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
314	**Section:** Authentication **ID:** 1.u.2 Deny access rights to a specified user/customer or a group of users/customers. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-105[70]	1. Verify the ability to deny access rights to a specified user/customer or a group of users/customers. 2. Login as administrator and create an grant access privileges for a specific resource for an individual user. 3. Confirm that the individual user has access and privileges to the resource created. 4. Confirm the normal user does not have the same access capabilities to this resource as the creator (admin). 5. Without changing access privileges on the user, move the user into a group that does not have administrative privileges. 6. Attempt to perform administrative functions on a specified resource. Verify the user does not have the ability to access and change the resource in the manner an administrator would.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
315	**Section:** Authentication **ID:** 1.u.3 Grant access rights to a specified interface/port or a group of interfaces/port. **Reference:** UCR 5.4.6.2.1.7 **IA Control:** ECLP-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815-CORE R3-105[70]	1.Verify the ability to grant access rights to a specified interface/port or group of interfaces/ports. 2. Determine an interface or port that is denied access via ACL. 3. Modify the ACL such that access is now granted and verify that the interface/port can now be accessed.	CAT III	

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
316	**Section:** Authentication **ID:** 1.u.4 Deny access right to a specified interface/port or a group of interfaces/ports. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the ability to deny access rights to a specified specified/port or group of interfaces/port. 2. Determine an interface or port that is granted access via ACLs. 3. Modify the ACLs such that access is now denied and verify that the interface/port cannot be accessed.	CAT III	
	IA Control: ECLP-1	**Origin:** GR-815-CORE R3-105[70]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
317	**Section:** Authentication **ID:** 1.u.5 Deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that a hierarchical privilege structure exists to protect data and resource access. 2. Login as a normal “User”. 3. Attempt to execute a command that would cause the system to enter an unstable state (e.g., re-boot) 4. Verify that the attempt was not allowed due to user privilege.	CAT II	
	IA Control: DCFA-1 and ECLP-1	**Origin:** GR-815-CORE R3-106[71]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
318	**Section:** Authentication **ID:** 1.u.6 Deny an interface/port access to potentially damaging processes and transactions that the interface/port does not have to access to be functional. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that a hierarchical privilege structure exists and is enforced to protect data and resource access. 2. Verify ACL are in place to control access to ports and resources.	CAT II	
	IA Control: DCFA-1 and ECLP-1	**Origin:** GR-815-CORE R3-107[72]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
319	**Section:** Authentication **ID:** 1.u.7 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. **Reference:** UCR 5.4.6.2.1.7	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that a hierarchical privilege structure exists and is enforced to protect data and resource access. 2. Verify ACLs are in place to control access to ports and resources.	CAT II	
	IA Control: IAIA-1	**Origin:** GR-815-CORE R3-105[70]			

Table E-8. Authentication (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
320	**Section:** Authentication **ID:** 1.u.8 If the system has its operation database structured on the basis of commands, views, records, and fields, the system shall restrict, on the basis of user-ID, as well as interface/port, the execution of any specifiable command on any specifiable view, record, or field. **Reference:** UCR 5.4.6.2.1.7	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the operational database is structured based on commands, views, records, and fields, the system restricts, because of user-ID, as well as interface/port, the execution of any specifiable view record or field. 2. If the system does not have a database associated with it, this test is not applicable. 3. Create a database user with the rights to view only. 4. Login with the above user and attempt to change or add a field to the database. 5. Confirm that the attempts were denied.	CAT II	
	IA Control: COBR-1 and ECND-1	**Origin:** GR-815-CORE R3-74[39]			

LEGEND:

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADM	Add-Drop Multiplexer
ARP	Address Resolution Protocol
AS SIP	Assured Services Session Initiation Protocol
AVP	Absolute Value Pairs
B	Base
BC	Border Controller
C	Camp
CA	Certification Authority
CAC	Common Access Card
CAT	Category
CALEA	Commission on Accreditation for Law Enforcement Agencies
CLI	Command Line Interface
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COBR	Continuity Backup Restoration
COMS	Continuity Maintenance Support
CRL	Certificate Revocation List
CTL	Certificate Trust List
DAA	Designated Approving Authority
DCBP	Design Configuration Best Practices
DCC	Data Communications Channel
DCCS	Design Configuration Configuration Specification
DCDS	Design Configuration Dedicated Services
DCFA	Design Configuration Functional Architecture
DCID	Detection and Correct Identification Delay
DCNR	Design Configuration Non-Repudiation
DCPA	Design Configuration Partitioning Application
DCPP	Design Configuration Ports Protocols
DCSP	Design Configuration System Plan
DCSQ	Design Configuration Software Quality
DCSR	Design Configuration Specific Robustness
DCSS	Design Configuration System State
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DRSN	Defense Red Switch Network
DSCP	Differentiated Services Code Point
DSN	Defense Switched Network
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
IAKM	Identification Authentication Key Management
IATP	Internet Access and Training Program
IATS	Identification Authentication Token Standards
ICD	Initial Capabilities Document
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IO	Interoperability
IP	Internet Protocol
IPsec	Internet Protocol Security
IPV	Internet Protocol Vulnerability
JTA	Joint Technical Architecture
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LoC	Letter of Compliance
LS	LAN Switch
LSC	Local Session Controller
MA	Mission Area
MAC	Media Access Controller
MFSS	Multifunction Softswitch
MD5	Message Digest 5
MG	Media Gateway
NAS	Network Access Server
NAT	Network Address Translation
NAPT	Network Address Port Translation
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NM	Network Management
NMS	Network Management System
NOC	Network Operations Center
NSA	National Security Agency
OAM&P	Operation, Administration, Maintenance, and Provisioning
OSC	Online Status Check
OSCR	Online Status Check Response
P	Post
PCCC	PC Communication Client
PEAP	Protected Extensible Authentication Protocol
PESL	Physical Environmental Screen Lock
PIN	Personal Identification Number
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PMO	Personnel Management Officer
PPS	Packets Per Second
PRAS	Performance Results Aggregation System
PSTN	Public Switched Telephone Network
QoS	Quality of Service

Table E-8. Authentication (continued)

EAP-TTLS	Extensible Authentication Protocol – Tunneled Transport Layer Security
EBBD	Enclave Boundary Boundary Defense
EBC	Edge Border Controller
EBCR	Enclave Boundary Connection Rules
EBRP	Enclave Boundary Remote Privileged
EBRU	Enclave Boundary Remote User
ECAD	Enclave Computing Affiliation Display
ECAN	Enclave Computing Access Need-To-Know
ECAR	Enclave Computing Audit Record
ECAT	Enclave Computing Audit Trail
ECCD	Enclave Computing Changes to Data
ECCR	Enclave Computing Confidentiality at Rest
ECCT	Enclave Computing Confidentiality at in Transit
ECIC	Enclave Computing Interconnections
ECID	Enclave Computing Intrusion Detection
ECLO	Enclave Computing Logon
ECLP	Enclave Computing Least Privilege
ECML	Enclave Computing Marketing and Labeling
ECND	Enclave Computing Network Device
ECNK	Enclave Computing Need to Know
ECPA	Enclave Computing Privileged Account
ECRC	Enclave Computing Resource Control
ECSC	Enclave Computing Environment Security Configuration Compliance
ECTB	Enclave Computing Trail Backup
ECTM	Enclave Computing Transmission
ECTP	Enclave Computing Trail Protection
ECWM	Enclave Computing Warning Messag
EEP	Emergency Entry Point
EI	End Instrument
FIPS	Federal Information Processing Standard
FSO	Field Security Office
FY	Fiscal Year
GIG	Global information Grid
GR	Generic Requirement
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAAC	Enclave Computing Account Control
IAGA	Identification Authentication Group Authentication
IAIA	Individual Identification and Authentication
R	Router
RADIUS	Remote Authentication Dial-in User Server
RAW	Read after Write
RFC	Request For Comment
RSA	Rivest, Shamir, and Aldeman
S	Station
SA	System Administrator
SDP	Session Description Protocol
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SHA-96	Secure Hash Algorithm-96
SIP	System Identification Profile
SNMP	Secure/Simple Network Management Protocol
SNMPv3	Secure/Simple Network Management Protocol version 3
SONET	Synchronous Optical Network
SS	Soft Switch
SSH	Secure Shell
STIG	Security Technical Implementation Guidelines
TACACS+	Terminal Access Controller Access Control System Plus
TAG	Technical Advisory Group
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDEA	Triple Data Encryption Algorithm
TDM	Time Division Multiplexer/Multiplexing
TLS	Transport Layer Security
UCR	Unifed Capabilites Requirements
UDP	User Datagram Protocol
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VTC	Video Teleconference
VVoIP	Voice and Video Over Internet Protocol
WAN	Wide Area Network

Table E-9. Integrity

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
321	**Section:** Integrity **ID:** 1 The system shall be capable of providing data and system integrity. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Confirm that the system uses TLS v1.0 to secure and maintain the integrity of the system. 2. Verify the cryptographic module is FIPS 140-2 validated. 3. This is possible by examining the system security settings in the configuration file. In addition, sniffing the signaling traffic may reveal the TLS version in use. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies. Note: The IPV test team will perform this test.	CAT I	
	IA Control: DCCS-2	**Origin:** DoDD 8500.1.4.2 and GIG MA ICD IV.B.4e & IV B.6.c7			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
322	**Section:** Integrity **ID:** 1.a The system shall be capable of ensuring the integrity of signaling messages. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, and EI	1. Confirm that the system uses TLS v1.0 to secure and maintain the integrity of the system. 2. Verify the cryptographic module is FIPS 140-2 validated. 3. This is possible by examining the system security settings in the configuration file. In addition, sniffing the signaling traffic may reveal the TLS version in use. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies. Note: The IPV test team will perform this test.	CAT II	
	IA Control: DCNR-1	**Origin:** OAM&P M4 and GR-815 CORE CR3-63[238]			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
323	**Section:** Integrity **ID:** 1.a.1 The system 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. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, and EBC **Conditional:** EI	1. Confirm that the system uses TLS v1.0 to secure and maintain the integrity of the system. 2. Verify the cryptographic module is FIPS 140-2 validated. 3. Examine the system security settings in the configuration file. In addition, sniffing the signaling traffic may reveal the TLS version in use. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies. Note: The IPV test team will perform this test.	CAT II	
	IA Control: DCNR-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
324	**Section:** Integrity **ID:** 1.a.1.a The system shall be capable of using HMAC-SHA1-160 with 160 bit keys. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, and EBC **Conditional:** EI	1. Confirm that the system uses TLS v1.0 to secure and maintain the integrity of the system. 2. Verify the cryptographic module is FIPS 140-2 validated. 3. This is done by examining the system security settings in the configuration file. In addition, sniffing the signaling traffic may reveal the TLS version in use. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies. Note: The IPV test team will perform this test.	CAT III	
	IA Control: DCNR-1	**Origin:** OAM&P M4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
325	**Section:** Integrity **ID:** 1.a.2 If the system uses H.323, the system 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. **Reference:** UCR 5.4.6.2.2	**Conditional:** MFSS, SS, LSC, and EI	1. Verify that the system is capable of using the H.323 protocol. If not, this test is not applicable. 2. If the system is capable of using H.323, verify that the system supports the use of H.235.1 and HMAC-SHA1-96 with 160-bit keys. 3. Verify by examining the system security setting or sniffing the H.323 traffic. Note: The mechanism used for H.323 authentication and key exchange is the IKE protocol.	CAT III	
	IA Control: DCNR-1	**Origin:** OAM&P M4			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
326	**Section:** Integrity **ID:** 1.b The systems shall be capable of protecting data integrity by performing integrity checks and/or data updates. Examples include: **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	Verify the system is capable of protecting data integrity by performing the following integrity check and/or data updates: (16.2a-g)	CAT III	
	IA Control: DCSQ-1 and ECTM-2	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
327	**Section:** Integrity **ID:** 1.b.1 Proper rule checking on data update. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. If the system does not include a database, this test is not applicable. 2. Perform a database operation that requires a data update. Ensure that the data to update is out of range or invalid. 3. Confirm that the data update is refused.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
328	**Section:** Integrity **ID:** 1.b.2 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. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Login as the Administrator. 2. Attempt to perform a system command that could be considered dangerous (e.g., Reboot). 3. Verify that a warning message is presented to the user to optionally cancel the command.	CAT III	
	IA Control: ECCD-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
329	**Section:** Integrity **ID**: 1.b.3 Proper handling of duplicate/multiple inputs. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. In database operations, confirm that duplicate or multiple inputs are rejected by the database system. 2. In management operations, confirm that duplicate or multiple inputs to the management are rejected.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
330	**Section:** Integrity **ID:** 1.b.4 Checking return status. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify the system is capable of protecting data integrity by checking return status. 2. Verify unacceptable message return.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
331	**Section:** Integrity **ID:** 1.b.5 Checking immediate results. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify the system is capable of protecting data integrity by checking intermediate results. 2. Verify data acceptance.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
332	**Section:** Integrity **ID:** 1.b.6 Checking inputs for reasonable values. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	1. During a database operation(s), use data values that are out of range for the specific date. 2. During management operations, use data values that are out of range for the specific data.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
333	**Section:** Integrity **ID:** 1.b.7 The systems shall be capable of protecting data integrity by performing proper serialization of update transactions. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	Verify the system is capable of protecting data integrity by checking proper serialization of update transactions.	CAT III	
	IA Control: DCSQ-1	**Origin:** GR-815 CORE R3-127[101] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
334	**Section:** Integrity **ID:** 1.c The system shall be capable of providing mechanisms or procedures that can be used to periodically validate its correct operation (such as proper functioning of the security log, proper functioning of various trigger mechanisms, etc.). **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	Verify the system provides an alarm that notifies an administrator of a malfunction.	CAT III	
	IA Control: ECAT-2	**Origin:** GR-815 CORE CR3-128[96] and DRSN STIG 4.6.5			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
335	**Section:** Integrity **ID:** 1.d The system shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues). **Reference:** UCR 5.4.6.2.2 **IA Control:** ECAT-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-129[97] and OAM&P IA Req. M35	1. Verify the system provides mechanisms to monitor system resources and their availability (e.g., overflow indication, lost messages, buffer queues). 2. From multiple test laptops, execute the tools that will perform integrity type of testing. This includes the IP Stack Integrity Checker (ISIC) tool, as well as others. 3. Verify the system reports on any anomalies detected during this test. Note: The IPV test team will perform this test.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
336	**Section:** Integrity **ID:** 1.e The system shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold. **Reference:** UCR 5.4.6.2.2 **IA Control:** ECAT-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-130[98]	1. Verify the system provides mechanisms to detect communication errors (relevant to the system) above a specifiable threshold. 2. Confirm that the system has a tunable threshold for detecting communication errors. If not, this is a finding. 3. Attempt to force communication errors by introducing errors during call signaling. The Nemesis tool can be used for this purpose. Note: The IPV test team will perform a portion of this test.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
337	**Section:** Integrity **ID:** 1.f The system shall be capable of providing a mechanism to monitor the integrity of the system 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 system and the IA test team will provide technical advisement to the DSAWG regarding their adequacy. **Reference:** UCR 5.4.6.2.2 **IA Control:** DCCS-2	**Required:** MFSS, SS, LSC, and EBC **Origin:** GR-815 CORE R3-133 [102]; OAM&P M36 & M37 and DRSN STIG 4.6.5	1. Verify the system provides a mechanism to generate a status report detailing the values of all parameters and flags that affect the secure operation of the system. 2. Verify that all security-related parameters are documented and the system has the ability to generate a report on these parameters.	CAT III	

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
338	**Section:** Integrity **ID:** 1.g The system shall be capable of automatically running file or disk integrity checking utilities by vendor-supplied software. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, and EBC	Verify administrator documentation contains recommendations for running, on a regular basis, integrity checking utilities for file systems or disks.	CAT III	
	IA Control: DCSS-2	**Origin:** GR-815 CORE R3-134[103] & CR3-135[104], and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
339	**Section:** Integrity **ID:** 1.h The system shall be capable of providing data integrity of the bearer (Transport) packets. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, MG, and EI	1. Verify that the system is capable of using HMAC-SHA1-32 for the authentication tag with 60-bit key length as the default integrity mechanism for SRTP. 2. If the system has a security configuration file, examine the contents to determine if HMAC-SHA1-32 with 60-bit key is supported. 3. An alternate method would be to sniff and examine the traffic.	CAT II	
	IA Control: DCSQ-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
340	**Section:** Integrity **ID:** 1.h.1 The system shall be capable of using HMAC-SHA1-32 for the authentication tag, with 60-bit key length, as the default integrity mechanism for SRTP packets. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, MG, and EI	1. Verify that the system is capable of using HMAC-SHA1-32 for the authentication tag with 60-bit key length as the default integrity mechanism for SRTP. 2. If the system has a security configuration file, examine the contents to determine if HMAC-SHA1-32 with 60-bit key is supported. 3. An alternate method would be to sniff and examine the traffic.	CAT III	
	IA Control: DCNR-1	**Origin:** Vendor Agreement based on SRTP RFC. It was a tradeoff between "overhead and risk"			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
341	**Section:** Integrity **ID:** 1.h.2 The system 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 use of this protocol is optional, but the capability is required. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, MG, and EI	1. If the system has a security configuration file, examine the contents to determine if HMAC-SHA1-80 with 60-bit key is supported. 2. An alternate method would be to sniff and examine the traffic.	CAT III	
	IA Control: DCNR-1	**Origin:** Vendor agreement based on recommendation in RFC 3711			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
342	**Section:** Integrity **ID:** 1.i Systems that support remote network management functions and/or critical network resources and services shall be capable of providing appropriate standard (FIPS 140-2) cryptography-based data integrity services to protect and detect against unauthorized modification of messages. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the implementation of the SSH2, SSL, IPSeC, AES, SFTP, etc. 2. Verify the cryptographic module is FIPS140-2-validated. (http://csrc.nist.gov/cryptval/140-1/1401vend.htm) Note: Encryption standards for transporting data may be more stringent dependent upon the deployment strategies.	CAT II	
	IA Control: DCNR-1	**Origin:** GR-815 CORE CR3-63[238], CR3-65[240], & CR3-69[224] and DRSN STIG 4.7.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
343	**Section:** Integrity **ID:** 1.j An appliance and its application shall be capable of ensuring that it cannot be made to enter an insecure state because of the operation of non-privileged code. Note: It is understood that systems shall satisfy this requirement using industry best practices and will mitigate any findings associated with this requirement discovered during IA testing. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that the system only allows compatible code and that attempts to intermingle non-compatible code do not lead to an insecure state. This requirement has to do with the stability of the appliance when an application is subject to abnormal usage. 2. For any applications on the system, confirm that the application as well as the system, will remain securely stable when subjected to a thorough IPV test.	CAT III	
	IA Control: DCSQ-1 and ECND-2	**Origin:** GR-815 CORE R3-126[253]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
344	**Section:** Integrity **ID:** 1.k The system 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. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Restart the system and verify that default user-IDs and passwords, previously modified by an administrator, have not reverted to vendor-delivered default user-IDs and passwords. 2. If the user-IDs or passwords reverted back to default this requirement is not met.	CAT I	
	IA Control: IAIA-1	**Origin:** GR-815 CORE R3-167[134] and VoIP STIG Vulnerability 12G			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
345	**Section:** Integrity **ID:** 1.l The system shall be capable of providing mechanisms to ensure the integrity of the data that stored on the appliance and is used to support authentication processes. This includes protecting the information from malicious deletion, modification, or insertion. Note: Examples of the data stored would be private keys or certificates. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, EI, and LS	1. Verify that authentication data essential to running the system may only be accessed by authorized administrators. 2. If session keys, certificates or other authentication data are stored on the system, verify that access to this data is limited to authorized users only.	CAT I	
	IA Control: ECCD-2 and ECCR-1	**Origin:** Access Control STIG 2.1.1.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
346	**Section:** Integrity **ID:** 1.m If the system uses IPsec, the system shall be capable of using HMAC-SHA (class value 2) as the default IKE integrity mechanism as defined in RFC 2409. **Reference:** UCR 5.4.6.2.2	**Conditional:** MFSS, SS, LSC, and MG	1. If the system is using IPsec for H.323, verify that the system is capable of using HMAC-SHA as the default IKE integrity mechanism for IPsec in accordance with RFC 2409. 2. Verify the configuration file associated with the security settings include HMAC-SHA as the IKE mechanism.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 2409 Appendix A			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
347	**Section:** Integrity **ID:** 1.n The entire SNMPv3 message shall be checked for integrity and shall use HMAC-SHA1-96 with 160-bit key length. **Reference:** UCR 5.4.6.2.2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. At the VVOIP NMS, verify that the SNMPv3 is configured to use HMAC-SHA1-96. 2. If SNMPv3 is not using HMAC-SHA1-96, and cannot be configured to use it, this is a finding.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 3414 1.4.2 and DISA SNMPv3 Secure NMS CONOPs			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
348	**Section:** Integrity **ID:** 1.o If the system uses SSHv2, the system shall use HMAC-SHA1-96 with 160 bit key length for data integrity. **Reference:** UCR 5.4.6.2.2	**Conditional:** MFSS, SS, LSC, MG, BC, R, and LS	1. Verify that if the system uses SSH, it is using SSHv2. If not, then this is a finding. 2. If the system is using SSHv2, verify that it is using HMAC-SHA1-96 by inspecting the SSH client ssh_config file for the presence of HMAC-SHA1-96. If this option is not present and cannot be configured, this is a finding.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.4			

Table E-9. Integrity (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
349	**Section:** Integrity **ID:** 1.p If the system uses TLS, the system shall be capable of using TLS (SSLv3.1 or higher) in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for session packets. **Reference:** UCR 5.4.6.2.2 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, BC, and EI **Origin:** OAM&P M4	1. Verify that the system is capable of using TLS. 2. If the system is using TLS, verify that it is capable of using HMAC-SHA1-96 with 160-bit keys to provide integrity for session packets.	CAT III	

LEGEND:

AES	Advanced Encryption Algorithm	ID	Identification
AS-SIP	Assured Services – Sessions Initiation Protocol	IKE	Internet Key Exchange
BC	Border Controllers	IP	Internet Protocol
CAT	Category	IPsec	Internet Protocol Security
CONOPs	Concept of Operations	IPV	Internet Protocol Vulnerability
DCCS	Design Configuration Configuration Standards	LAN	Local Area Network
DCNR	Design Configuration Non-repudiation	LS	LAN Switch
DCSQ	Design Configuration Software Quality	LSC	Local Session Controller
DCSS	Design Configuration System State Changes	MA	Mission Area
DISA	Defense Information Systems Agency	MFSS	Multifunction Softswitch
DoDD	Department of Defense Directive	MG	Media Gateway
DRSN	Defense Red Switch Network	NMS	Network Management System
DSAWG	Defense Information System Network Security Accreditation Working Group	OAM&P	Operations, Administration, Maintenance and Provisioning
EBC	Edge Border Controller	R	Router
ECAT	Enclave Computing Environment Audit Trail, Monitoring, Analysis, and Reporting	RFC	Request for Comments
		SFTP	Secure File Transfer Protocol
ECCD	Enclave Computing Environment Changes to Data	SHA	Secure Hash Algorithm
ECCR	Enclave Computing Environment Encryption for Confidentiality (Data at Rest)	SNMPv3	Simple Network Management Protocol Version 3
		SRTP	Secure Remote Transfer Protocol
ECND	Enclave Computing Environment Network Device Controls	SS	Softswitch
ECTM	Enclave Computing Transmission	SSH	Secure Shell
EI	End Instrument	SSH2	Secure Shell 2
FIPS	Federal Information Processing Standards	SSHv2	Secure Shell version 2
GIG	Global Information Grid	SSL	Secure Socket Layer
GR	Generic Requirements	SSLv3	Secure Socket Layer version 3
HMAC	Hashed Message Authenticated Code	STIG	Security Technical Implementation Guidelines
IA	Information Assurance	TLS	Transport Layer Security
IAIA	Identification Authentication Individual Identification and Authentication	UCR	Unified Capabilites Requirements
		V	Version
ICD	Initial Capabilities Document	VoIP	Voice over Internet Protocol

Table E-10. Confidentiality

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
350	**Section:** Confidentiality **ID:** 1 The system shall be capable of providing data and signaling confidentiality for all VVoIP traffic. **Reference:** UCR 5.4.6.2.3 **IA Control:** ECCT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** VoIP STIG V2r2 3.8	1. Verify that the system can provide data and signaling integrity for all VvoIP traffic. 2. Confirm that all processes that use an encryption algorithm are using a FIPS 140-2 Level 1 cryptographic module. For SSH access, this can be done by verifying the SSH configuration file, or sniffing and examining the SSH traffic. 3. For other processes, examine the security configuration file or attempt to capture traffic that is required to be encrypted.	CAT I	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
351	**Section:** Confidentiality **ID:** 1.a The system shall implement FIPS 140-2 Level I-validated cryptographic hardware modules or software toolkits operated in FIPS mode for all encryption mechanisms. 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 will either purchase an approved FIPS 140-2 cryptographic module for their application or will submit their developed cryptographic module to an approved FIPS 140-2 certification laboratory prior to submitting their 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. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** DoDD E3.2.4.3.3; CJSCI 6510.01D D.13.c; NSA 2.3.1; and DRSN STIG 4.7.4 & 6.2	1. Verify that the system can provide data and signaling integrity for all VvoIP traffic. 2. Confirm that all processes that use an encryption algorithm, are using a FIPS 140-2 Level 1 cryptographic module. For SSH access, this can be done by verifying the SSH configuration file, or sniffing and examining the SSH traffic. 3. For other processes, examine the security configuration file or attempt to capture traffic that is required to be encrypted.	CAT II	

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
352	**Section:** Confidentiality **ID:** 1.b The system shall be capable of providing confidentiality for media streams using SRTP with AES_CM_128 encryption algorithm as the default or [Required FY12] AES 256-bit algorithm. **Reference:** UCR 5.4.6.2.3	**Required:** MG and EI	1. Verify that the system supports SRTP with AES-CM-128 encryption algorithm as the default or AES 256 bit algorithm. 2. Examine the system security configuration file and confirm whether the system supports SRTP with AES-CM-128. 3. While monitoring both the signaling and media stream, confirm that SRTP is being used for the media stream and that AES-CM-128 is the encryption algorithm being used. AES-CM-256 is the ideal choice.	CAT I	
	IA Control: DCNR-1	**Origin:** OAM&P M1 Table 3; JTA and NSA 2.4.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
353	**Section:** Confidentiality **ID:** 1.b.1 The system shall be capable of generating keys using a random source algorithm that meets the requirements of FIPS 186 to support SRTP. **Reference:** UCR 5.4.6.2.3	**Required:** EI	Verify that the system is capable of generating keys using a random source algorithm that meets the requirements of FIPS 186 to support SRTP. Note: An LoC for this requirement will suffice.	CAT II	
	IA Control: DCNR-1	**Origin:** OAM&P M1 Table 3; JTA and NSA 2.4.4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
354	**Section:** Confidentiality **ID:** 1.b.2 The system shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EI	1. Verify that the system is capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages. 2. While monitoring the signaling traffic, place an AS-SIP call. 3. Examine the signaling traffic that was captured and verify that the Master and Salt keys are properly included within the signaling messages. Note: The IPV test team will verify this requirement.	CAT II	
	IA Control: IATS-2	**Origin:** VVoIP IA Core Team			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
355	**Section:** Confidentiality **ID:** 1.b.3 The system shall be capable of distributing the Master Key and the Salt Key in concatenated form. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EI	1. Verify that the system is capable of distributing the Master Key and the Salt Key in concatenated form. 2. While monitoring the signaling traffic, place an AS-SIP call. 3. Examine the signaling traffic that was captured and verify that the Master and Salt keys are properly included within the signaling messages. Note: The IPV test team will verify this requirement.	CAT II	
	IA Control: IATS-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
356	**Section:** Confidentiality **ID:** 1.b.4 The system shall use a Master Key of 128 bits in order to support 128-bit AES encryption. Note: This implies that the Master Salt Key may be null. **Reference:** UCR 5.4.6.2.3	**Required:** EI and MG	1. Verify that the system is capable of using a master key of 128 bits to support 128-bit AES encryption. 2. While monitoring the signaling traffic, place an AS-SIP call. 3. Examine the signaling traffic that was captured and verify that the Master and Salt keys are properly included within the signaling messages. Note: The IPV test team will verify this requirement.	CAT II	
	IA Control: DCNR-1	**Origin:** VVoIP IA Core Team			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
357	**Section:** Confidentiality **ID:** 1.b.5 The Master Key and a random Master Salt Key shall be supported for SRTP sessions. Note: This is in addition to the 256-bit requirement. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Required:** EI and MG **Origin:** VVoIP IA Core Team	1. Verify that the Master Key and a random Master Salt Key shall be supported for SRTP sessions. 2. While monitoring the signaling traffic, place an AS-SIP call. 3. Examine the signaling traffic that was captured and verify that the Master and Salt keys are properly included within the signaling messages. Note: The IPV test team will verify this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
358	**Section:** Confidentiality **ID:** 1.c The system shall be capable of providing confidentiality for signaling messages using TLS or IPsec using the AES 128-bit algorithm or AES 256-bit algorithm. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, and EI **Origin:** OAM&P IA Req M1 & Table 3; JTA; and NSA 2.3.5 & 2.4.4	1. Verify that the system is capable of using TLS or IPSEC using the AES 128-bit algorithm to provide confidentiality for signaling messages. 2. Examine the system security configuration file. 3. Verify that the AES-128 is one of the available encryption algorithms. If not, this is a finding. Note: The IPV test team will verify this requirement.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
359	**Section:** Confidentiality **ID:** 1.c.1 If H.323, MGCP, or H.248 (MEGACO) is used, the system shall be capable of using IPsec to provide confidentiality. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, and EI **Origin:** VoIP STIG 0040	1. Verify that MGCP or MEGACO protocol is in use. 2. If MGCP or MEGACO protocol is in use, verify that the system is capable of using IPsec for confidentiality.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
360	**Section:** Confidentiality **ID:** 1.c.1.a If the system uses H.248 (MEGACO), the system shall be capable of distributing the SRTP Master Key and Salt Key in the Session Description Protocol (SDP) "k=" crypto field when using H.248.15. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, and MG **Origin:** VoIP STIG 3.12 (0040)	1. If the system uses H.248 (MEGACO), verify that the system is capable of distributing the SRTP Master Key and Salt Key in the SDP "k+" crypto field when using H.248.15. 2. Monitor the signaling traffic using WireShark, 2. Make a MEGACO call and confirm that the SDP field of the INVITE message contains the SRTP master and Salt keys. Note: The IPV test team will verify this requirement.	CAT III	

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
361	**Section:** Confidentiality **ID:** 1.c.1.b If H.323 is used, the system shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H.235 KEY as described in H.235.0 and H.235.8. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, and MG	1. If the system uses H.323 (MGCP), verify that the system is capable of distributing the SRTP Master Key and Salt Key in H.235 using the H.235 KEY as described in H.235.0 and H.235.8. 2. During the initiation of an H.323 VTC call that traverses VVOIP enclaves, monitor the signaling using the Wireshark protocol sniffer. 3. Confirm that the H.235 protocol contains the H.235 KEY field and contains the Master and Salt keys. Note: The IPV test team will verify this requirement.	CAT II	
	IA Control: IAKM-2	**Origin:** VoIP STIG 3.12 (0040)			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
362	**Section:** Confidentiality **ID:** 1.c.1.c If IPsec is used, the system shall be capable of using Internet Key Exchange (IKE) for IPsec key distribution. [Required FY 10] IKE version 2 Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. If IPsec is used, verify that the system is capable of using IKE version 1 or version 2 2. The security configuration file should be downloaded. 3. Confirm the version of IKE being used.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
363	**Section:** Confidentiality **ID:** 1.c.1.c.i IKE version 1 **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EI	1. Analyze the IPsec security configuration file. 2. Confirm that IKE version 1 is used.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 5.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
364	**Section:** Confidentiality **ID:** 1.c.1.c.ii IKE version 2 Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EI	1. Analyze the IPsec security configuration file. 2. Confirm that IKE version 1 is used.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 5.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
365	**Section:** Confidentiality **ID:** 1.c.1.c.iii If IPsec is used, the system shall be capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. If IPsec is used, verify that the system is capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication. 2. From the information available in the configuration file, confirm the Revised Mode of public key encryption is being used for ISAKMP negotiation for authentication.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 5.3			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
366	**Section:** Confidentiality **ID:** 1.c.1.c.iv If IPsec is used, the system shall be capable of using the Quick Mode as the default Phase II authentication mechanism. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. If IPsec is used, verify that the system is capable of using the Quick Mode as the default Phase II authentication mechanism. 2. From the information available in the configuration file, confirm the system is able to use the Quick Mode as the default Phase II authentication mechanism.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
367	**Section:** Confidentiality **ID:** 1.c.1.c.v If IPsec is used, the system shall be capable of using interpreting certificate requests for PKCS#7 wrapped certificates as a request for the whole path of certificates. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	If IPsec is used, verify that the system is capable of using interpreting certificate requests for PKCS#7-wrapped certificates as a request for the whole path of certificates. Note: An LoC will suffice for this requirement.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
368	**Section:** Confidentiality **ID:** 1.c.1.c.vi If IPsec is used, the system shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	If IPsec is used, verify that the system is capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation. Note: An LoC will suffice for this requirement.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 2409 5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
369	**Section:** Confidentiality **ID:** 1.c.1.c.vi.a If IPsec is used, the system shall only support the following erroneous messages associated with a certificate request: • Invalid key • Invalid ID • Invalid certificate encoding • Invalid certificate • Certificate type unsupported • Invalid CA • Invalid hash • Authentication failed • Invalid signature • Certificate unavailable **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	If IPsec is used, verify that the system only supports the following erroneous messages associated with a certificate request**:** 1. Create individual certificates with the following characteristics: • Invalid key • Invalid ID • Invalid certificate encoding • Invalid certificate • Certificate type • Unsupported • Invalid CA • Invalid hash • Authentication failed • Invalid signature • Certificate unavailable 2. Using an invalid certificate, confirm that the system rejects the certificate and the calls do not complete.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4306			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
370	**Section:** Confidentiality **ID:** 1.c.1.c.vii If IPsec is used, the system shall be capable of using Oakely Groups 1 and 2 as a minimum. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. If IPsec is used, verify that the system is capable of using Oakely Groups 1 and 2 as a minimum. 2. By examining the configuration file, verify that the system can be configured to use Oakley Groups 1 and 2.	CAT II	
	IA Control: DCNR-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
371	**Section:** Confidentiality **ID:** 1.c.1.d If IPsec is used, the system shall be capable of using AES_128_CBC as the default encryption algorithm. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. If IPsec is used, verify that the system is capable of using AES_128_CBC as the default encryption algorithm. 2. By examining the configuration file, verify that the system can be configured to use AES_128_CBC.	CAT II	
	IA Control: DCNR-1	**Origin:** Vendor agreement; JTA; and OAM&P M1 Table 3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
372	**Section:** Confidentiality **ID:** 1.c.2 The system shall be capable of using TLS to provide confidentiality for the Assured Service- Session Initiation Protocol (AS-SIP). Note: The condition for the EI is the support of AS-SIP. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC,MG, and EBC **Conditional:** EI	1. Verify that the system is capable of using TLS to provide for AS-SIP sessions. 2. By examining the configuration file, verify that the system can be configured to use TLS for AS-SIP sessions.	CAT I	
	IA Control: DCNR-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
373	**Section:** Confidentiality **ID:** 1.c.2.a The underlying protocol for AS-SIP shall be the Transmission Control Protocol (TCP). **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC **Conditional:** EI	Verify that AS-SIP uses TCP as the underlying transmission protocol. Using Wireshark to sniff signaling traffic, confirm that AS-SIP calls use the Transport Control Protocol. Note: The VVOIP IPV test team will verify this requirement.	CAT I	
	IA Control: ECTM-2	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
374	**Section:** Confidentiality **ID:** 1.c.2.b The system shall be capable of using as its default cipher either: [**Conditional**]TLS_RSA_WITH _AES_128_CBC_SHA or [**Conditional**, **Required** FY12] TLS_RSA_WITH_AES_256_CBC_SHA_ **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC **Conditional:** EI	1. Verify that the system is capable of using TLS_RSA_WITH _AES_128_CBC_SHA or TLS_RSA_WITH_AES_256_CBC_SHA_ as its default cipher. 2. Examine the system security configuration log. 3. If the above algorithms cannot be configured, this is a finding.	CAT II	
	IA Control: DCNR-1	**Origin:** Standard TLS encryption algorithm			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
375	**Section:** Confidentiality **ID:** 1.c.2.c The system shall be capable of using a default of no compression for AS-SIP messages. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC **Conditional:** EI	Verify that the system is capable of using a default of no compression for AS-SIP messages.	CAT II	
	IA Control: ECTM-1	**Origin:** Vendor agreement. The size of the message did not make the use of compression necessary			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
376	**Section:** Confidentiality **ID:** 1.c.2.d The system shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC **Conditional:** EI	1. Verify that the system is capable of exchanging AS-SIP TLS messages in single or multiple exchanges. 2. During the initiation of an AS-SIP call, monitor and capture the signaling traffic between the endpoints. 3. Examine the TLS traffic within the signaling and confirm that multiple exchanges of TLS messages are present.	CAT II	
	IA Control: DCCS-2	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
377	**Section:** Confidentiality **ID:** 1.c.2.e The system 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. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC **Conditional:** EI	1. Verify that the system is capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP crypto-field. 2. Confirm that the signaling Path Is being monitored (sniffed) using WireShark. 3. Make an AS-SIP call. 4. Examine the INVITE Message and confirm that the SRTP master and salt keys are present in the SDP crypto field.	CAT II	
	IA Control: DCNR-1	**Origin:** Consistent with Session Description Protocol SDES Internet Drafts			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
378	**Section:** Confidentiality **ID:** 1.c.2.f 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 Network Management-related sessions. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, and SS, LSC, MG, EBC, and EI	1. Verify that TLS resumption is used by examining the security configuration file. If not, this test is not applicable. 2. If TLS resumption is used, verify that session resumption is configurable and that the default shall be 1 hour.	CAT III	
	IA Control: DCNR-1	**Origin:** Session resumption as discussed in RFC 2246			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
379	**Section:** Confidentiality **ID:** 1.c.2.f.i The maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/ confidentiality/authorization process is 1 hour. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC, and EI	1. Verify that TLS resumption is used. If not, this test is not applicable. 2. If TLS resumption is used, verify that session resumption is configurable and that the default shall be 1 hour. If it is not configurable, then this is a finding. 3. For the purpose of this test, configure the session resumption to be 1 minute. Also, monitor the signaling using WireShark. 4. Make an AS-SIP call. 5. Put the called party on hold in preparation for a 3-way call. 6. Establish the 3rd party of the call. 7. After a period of 1 minute has gone by, re-call the original called party establish the 3-way call. 8. Confirm that the Authentication process was repeated.	CAT III	
	IA Control: DCNR-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
380	**Section:** Confidentiality **ID:** 1.c.2.g If AS-SIP is used, the system shall only transmit packets that are secured with TLS and use port 5061. Note: The systems may use other signaling protocols for interfacing to MGs, EIs, etc. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, EBC, and EI	1. Verify that AS-SIP is in use. 2. If AS-SIP is in use, verify that the system secures packets with TLS over port 5061. Note: The IPV test team will confirm this requirement.	CAT III	
	IA Control: DCNR-1 and ECCT-2	**Origin:** VoIP STIG 3.7.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
381	**Section:** Confidentiality **ID:** 1.c.2.h The system shall reflect all received AS-SIP packets associated with port 5061 that are not secured with TLS. Note: This ensures that the system does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, EBC, and EI	1. Verify that the system reflects all AS-SIP associated with port 5061 that are not secured by TLS. 2. Configure an unmanaged hub on the AS-SIP signaling interface. 3. Attempt to inject a properly constructed AS-SIP INVITE message toward the system. 4. Confirm that this message is rejected by the system. Note: The IPV test team will perform a portion of this test.	CAT III	
	IA Control: DCNR-1	**Origin:** VoIP STIG 3.7.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
382	**Section:** Confidentiality **ID:** 1.c.2.i The system shall only accept and process AS-SIP packets that arrive on port 5061. Note: The system should discard AS-SIP packets that arrive on a different port. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, and EBC	1. Verify that the system only processes AS-SIP packets that are received by the system on port 5061. 2. Use a tool such as SiVus or another tool capable of injecting SIP messages. 3. Attempt to inject an AS-SIP INVITE message on port 5060. 4. Confirm that the message is ignored by port 5060. 5. Repeat step 2 but choose a port that is open and performing a service. The message should be ignored. Note: The IPV test team will perform a portion of this test.	CAT III	
	IA Control: DCCS-2	**Origin:** VoIP STIG 3.7.2.2			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
383	**Section:** Confidentiality **ID:** 1.d If the system uses web browsers or web servers, the system web browsers and web servers shall be capable of supporting TLS (Secure Socket Layer SSL v3.1) or higher for remote configuration of appliances. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Verify that the system has web servers or web browsers in use. 2. Analyze the web server or web browser security configuration to determine if TLS (SSLv3) can be supported.	CAT II	
	IA Control: DCNR-1	**Origin:** VoIP STIG 0290 & 0210; OAM&P IA Req. M2; JTA 6.4.1.1a; GR-815-CORE CR3-67[242] & CR3-68[243]; and NSA 2.3.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
384	**Section:** Confidentiality **ID:** 1.e The system shall be capable of using SSHv2 or TLS (SSLv3.1) or higher for remote configuration of appliances. Note: EIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system is capable of supporting SSHv2 or TLS (SSLv3.1) for remote configuration management. 2. Confirm that the SSH and TSL configuration files are set up for SSHv2 and TLS 1.0 (SSLv3) respectively.	CAT II	
	IA Control: DCNR-1	**Origin:** VoIP STIG 0290, 0210 & 0350; OAM&P IA Req M2; GR-815 CORE R3-66[241]; NSA 2.3.5 (EI); and DRSN STIG 6.2 & 6.2.2			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
385	**Section:** Confidentiality **ID:** 1.f If the system uses TLS, the system shall do so in a secure manner, as defined by the following subtended requirements. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Verify that the system is capable of using TLS. 2. If the system is using TLS, verify that it does so in a secure manner as required.	CAT II	
	IA Control: DCNR-1	**Origin:** VoIP STIG 0290, 0210 & 0350; GR-815 CORE R3-66[241];			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
386	**Section:** Confidentiality **ID:** 1.f.1 If the system uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA or TLS_RSA_WITH_AES_256__CBC_SHA_ [Required FY12] as its default cipher. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Verify that the system is capable of using TLS. 2. If the system is using TLS, verify that it is capable of using TLS_RSA with AES 128 CBC SHA or TLS_RSA with AES 256 CBC SHA. 3. Examine the security configuration file. 4. Verify that the system is using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher algorithm.	CAT III	
	IA Control: DCNR-1	**Origin:** VoIP STIG 0290, 0210 & 0350; GR-815 CORE R3-66[241];			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
387	**Section:** Confidentiality **ID:** 1.f.2 If the system uses TLS, the system shall be capable of using a default of no compression. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Verify that the system is capable of using TLS with a default of no compression. 2. Examine the TLS or security configuration file and verify that TLS is defaulted to “no compression.”	CAT III	
	IA Control: DCNR-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
388	**Section:** Confidentiality **ID:** 1.f.3 If the system uses TLS, the system shall be capable of exchanging TLS messages in a single exchange or in multiple exchanges. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	Verify that the system is capable of exchanging TLS messages in a single or in multiple exchanges.	CAT II	
	IA Control: DCCS-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
389	**Section:** Confidentiality **ID:** 1.f.4 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 Network Management-related sessions. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EBC	1. Verify that TLS resumption is used. If not, this test is not applicable. 2. If TLS resumption is used, verify that session resumption is configurable and that the default shall be 1 hour.	CAT III	
	IA Control: DCNR-1	**Origin:** Session resumption as discussed in RFC 2246			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
390	**Section:** Confidentiality **ID:** 1.f.4.a 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. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, and EBC **Origin:** Vendor agreement	1. Verify that TLS resumption is used. If not, this test is not applicable. 2. If TLS resumption is used, verify that session resumption is configurable and that the default shall be 1 hour. If it is not configurable, then this is a finding. 3. For the purpose of this test, configure the session resumption to be 1 minute. Also, monitor the signaling using WireShark. 4. Make an AS-SIP call. 5. Put the called party on hold in preparation for a 3-way call. 6. Establish the 3rd party of the call. 7. After a period of 1 minute has gone by, re-call the original called party to establish the 3-way call. 8. Confirm that the authentication process was repeated.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
391	**Section:** Confidentiality **ID:** 1.g If the system uses SSH, the system shall do so in a secure manner, as defined by the following subtended requirements. Note: EIs remote manual configurations shall not be enabled and all no automatic processes shall be performed locally. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-66[241];	Verify that the system uses SSH in a secure manner, as defined by the following requirements.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
392	**Section:** Confidentiality **ID:** 1.g.1 If the system uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** OAM&P Table 3	1. Verify that the system is capable of supporting the RSA 2,048-bit key algorithm. 2. Examine the SSH configuration file to determine what key algorithm is in use. 3. If the algorithm is something other then RSA 2,048 bit, verify whether it can be changed to RSA 2,048 bit.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
393	**Section:** Confidentiality **ID:** 1.g.2 If the system uses SSH, the system shall use SSH in a secure manner. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-66[241];	1. Verify that the system uses SSH in a secure manner. 2. Verify that Private/Public keys are securely stored and assessable only by those with the need.	CAT II	

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
394	**Section:** Confidentiality **ID:** 1.g.2.a If the system 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. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that a client closed the session if it receives a request to initiate an SSH session whose version is less than 2.0. Note: The IPV test team will attempt to establish an SSH session, using an SSH version 2.0.	CAT II	
	IA Control: DCNR-1	**Origin:** None			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
395	**Section:** Confidentiality **ID:** 1.g.2.b If the system uses SSH, SSH sessions shall re-key at a minimum of every 2^{31} of transmitted data or every 60 minutes, whichever comes first. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the SSH sessions re-key at a minimum of every 2^{31} of transmitted data or every 60 minutes, whichever comes first 2. While sniffing the traffic of an SSH session, perform a data transfer from client to host. Ensure that the total size of the transmitted data transferred exceeds the 2^{31} packet limit. 3. Verify that the re-keying traffic can be seen in the captured traffic. 4. While sniffing the traffic for a SSH session, advance the clock by 58 minutes. 5. Once the 60-minute mark has elapsed, confirm that the captured traffic contains the re-keying sequence traffic. Note: The IPV test team will perform this test.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4344 3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
396	**Section:** Confidentiality **ID:** 1.g.2.c If the system uses SSH, SSH sessions shall transmit less than 2^{32} packets after a key exchange has occurred. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that SSH sessions shall transmit less than 2^{32} packets after a key exchange has occurred. Note: An LoC will suffice.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4344 3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
397	**Section:** Confidentiality **ID:** 1.g.2.d If the system uses SSH, SSH sessions shall re-key at a minimum after receiving 2^{31} packets or every 60 minutes, whichever comes first. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that, SSH sessions shall re-key at a minimum after receiving 2^{32} packets or every 60 minutes, whichever comes first. 2. While sniffing the traffic for a SSH session, advance the clock by 58 minutes. 3. Once the 60-minute mark has elapsed, confirm that the captured traffic contains the re-keying sequence traffic. Note: The IPV test team will perform this test.	CATIII	
	IA Control: DCNR-1	**Origin:** RFC 4344 3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
398	**Section:** Confidentiality **ID:** 1.g.2.e If the system uses SSH, SSH sessions shall accept less than 2^{32} packets after a key exchange has occurred. Note: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept ($2^{(L/4)}$ where L is the key length – 128 bits). **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that SSH sessions shall accept less than 2 upper 32 packets after a key exchange has occurred. Note: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept (2 upper L/4 where L is the key length – 128 bits). Note: An LoC will suffice.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4344 3.1			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
399	**Section:** Confidentiality **ID:** 1.g.2.f If the system uses SSH, SSH sessions shall use as the default encryption algorithm either: AES 128-CBC or [conditional FY12] AES256-CBC. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that SSH sessions shall use AES 128-CBC (Threshold) or AES256-CBC (Objective) as the default encryption algorithm. 2. Initiate an SSH session, while monitoring the traffic. 3. Examine the captured SSH traffic and confirm that AES-128-CBC is being used.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.3 and OAM&P Table 3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
400	**Section:** Confidentiality **ID:** 1.g.2.g If the system uses SSH, SSH sessions shall use TCP as the underlying protocol. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system uses TCP as the underlying protocol. 2. Confirm that the captured SSH traffic in test case 273 shows that the TCP protocol was used.	CAT II	
	IA Control: ECTM-2	**Origin:** RFC 4253 6.3 and OAM&P Table 3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
401	**Section:** Confidentiality **ID:** 1.g.2.h If the system uses SSH, the SSH packets shall have a configurable maximum uncompressed payload and the default shall be of 32, 768 bytes. This does not preclude the system from automatically sizing the MTU if it is less than 32,768. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the SSH packets shall have a configurable maximum uncompressed payload and the default shall be of 32,768 bytes. This does not preclude the system from automatically sizing the MTU if it is less than 32,768. 2. Examine the security configuration file. 3. Verify that the maximum uncompressed payload default is 32,768.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
402	**Section:** Confidentiality **ID:** 1.g.2.h.i If the system uses SSH, SSH packets shall have a maximum packet size of 35,000 bytes including the packet_length, padding_length, payload, random padding, and mac. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that SSH packets have configurable maximum packet size and the default shall be 35,000 bytes, including the packet length, padding length, payload, random padding, mac. 2. Examine the security configuration file. 3. Verify that the maximum packet size is configurable and the default size is 35,000, If it is not configurable, this is a finding.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
403	**Section:** Confidentiality **ID:** 1.g.2.h.ii If the system uses SSH, the appliance shall discard SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system discards SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks. 2. Initiate an SSH session and attempt to send an SSH packet that is larger then 35,000. 3. Confirm that SSH has discarded the packet. 4. Confirm that the SSH session is not disrupted. Note: The IPV test team will perform a portion of this test.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.1			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
404	**Section:** Confidentiality **ID:** 1.g.2.h.iii If the system uses SSH, SSH packets shall use random bytes if packet padding is required. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that SSH packets use random bytes if packet padding is required. Note: An LoC will suffice.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
405	**Section:** Confidentiality **ID:** 1.g.2.i If the system 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. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that, the system treats 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. 2. During the monitoring of an SSH session using Wireshark, confirm that the captured traffic indicates the IV has been passed from the end of one packet to the beginning of the next. Note: The IPV test team will perform a portion of this test	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4253 6.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
406	**Section:** Confidentiality **ID:** 1.g.2.j If the system uses SSH, the system shall use Diffie-Hellman-Group2-SHA1 as the default key exchange mechanism for SSH. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system uses Diffie-Hellman-Group2-SHA1 as the default key exchange mechanism for SSH. 2. Examine the SSH configuration file. 3. Verify that Diffie-Hellman-Group2-SHA1 is set as the default key exchange algorithm.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4344			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
407	**Section:** Confidentiality **ID:** 1.g.2.k If the system uses SSH, the system using SSH shall be PKE and shall use the PKI to authenticate. **Reference:** UCR 5.4.6.2.3	**Conditional FY12 :** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system is PKE and uses the PKI to authenticate. 2. Examine the SSH configuration file and confirm that the system is PKE and is using the PKI to authenticate sessions.	CAT II	
	IA Control: DCNR-1	**Origin:** This is consistent with the PKE requirements shown elsewhere RFC 4253 6.6			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
408	**Section:** Confidentiality **ID:** 1.g.2.k.i If the system uses SSH, the system server using SSH shall have a host key. **Reference:** UCR 5.4.6.2.3	**Conditional FY12:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Manually verify that the system server uses a host key. 2. Obtain the system SSH host key. 3. Attempt to SSH into the system for the first time. 4. Confirm that the host key the system sends back is the same as the host key obtained in step 1.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4253			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
409	**Section:** Confidentiality **ID:** 1.g.2.k.ii If the system uses SSH, the system shall certify and validate a server's host key using the DoD PKI before connecting with an SSH session. **Reference:** UCR 5.4.6.2.3	**Conditional FY12:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system certifies and validates a server's host key using the DoD PKI before connecting with an SSH session .	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4253			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
410	**Section:** Confidentiality **ID:** 1.g.2.k.iii If the system uses SSH, the system shall certify and validate a server's host key prior to connecting with a SSH session. **Reference:** UCR 5.4.6.2.3	**Conditional FY12:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system disconnects if the number of failed authentication attempts for a single session exceeds a configurable parameter and the default shall be three attempts. Note: An LoC will suffice.	CAT II	
	IA Control: IAIA-1 and ECAR-2	**Origin:** RFC 4253			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
411	**Section:** Confidentiality **ID:** 1.g.2.l If the system uses SSH, the system shall disconnect a session if the authentication has not been accepted within 10 minutes. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system shall disconnect a session if the authentication has not been accepted within 10 minutes. Note: An LoC will suffice.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4252 Section 4			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
412	**Section:** Confidentiality **ID:** 1.g.2.m If the system uses SSH, the system shall disconnect if the number of failed authentication attempts for a single session exceeds a configurable parameter and the default shall be three attempts. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system disconnects if the number of failed authentication attempts for a single session exceeds a configurable parameter and the default shall be three attempts. 2. At the CLI prompt, execute the SSH command three times, each time using an invalid password. 3. Verify the session is disconnected. 4. Confirm that a tunable parameter exists for the number of invalid attempts before disconnect. 5. Repeat this test with a value other than 3 (e.g. 5).	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 4252 Section 4			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
413	**Section:** Confidentiality **ID:** 1.h The system shall be capable of using SNMPv3 for all SNMP sessions. Note: If the system 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 system has also developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system uses SNMP. 2. If the system uses SNMP, verify that the system is capable of using SNMP v3 for all SNMP sessions. If the system uses a version of SNMP that is <v3, this is a CAT III finding. 3. If SNMP versions 1 or 2 are found to be in use, verify that all security patches have been applied to mitigate existing security issues with version 1 and 2.	CAT II	
	IA Control: DCCS-2	**Origin:** Network Infrastructure STIG and NSA 2.3.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
414	**Section:** Confidentiality **ID:** 1.h.1 The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the security level for SNMPv3 is authentication with privacy ~ snmpSecurityLevel=authPriv 2. From the system management console, confirm that the SNMP variable snmpSecurityLevel = authPriv	CAT I	
	IA Control: IAIA-1	**Origin:** Vendor agreement			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
415	**Section:** Confidentiality **ID:** 1.h.2 The SNMPv3 architecture 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. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. From the management console, verify that the system is capable of manual configuration of the snmpEngineID by a systems administrator. 2. If a default snmpEngineID is applied, verify that it is manually configurable.	CAT III	
	IA Control: IAAC-1	**Origin:** RFC 3411 5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
416	**Section:** Confidentiality **ID:** 1.h.3 The security model for SMMPV3 shall be User-Based Security Model – snmpSecurity Model =3. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the SNMPv3 security model is user based – snmpSecurity Model -3. 2. From the management console, verify the SNMP variable snmpSecurity Model is set to 3.	CAT I	
	IA Control: DCCS-1	**Origin:** Consistent with SNMPv3 USM RFCs 3414, 3411,			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
417	**Section:** Confidentiality **ID:** 1.h.3.a If the system recieves SNMP responses, the system shall conduct a timeliness check on the SNMPv3 message. **Reference:** UCR 5.4.6.2.3 **IA Control:** ECRC-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 1,4,2	Verify that a timeliness check is conducted on SNMPv3 messages. Note: An LoC will suffice for this test.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
418	**Section:** Confidentiality **ID:** 1.h.3.b An SNMPv3 engine shall perform time synchronization using authenticated messages. **Reference:** UCR 5.4.6.2.3 **IA Control:** IAIA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that the SNMPv3 engine performs time synchronization using authenticated messages. 2. Enable sniffing on the subnet of a SNMP operation. 3. Perform the SNMP action and 4. verify the captured traffic contains the SNMP transaction. 5. Verify the captured traffic contains the synchronized packets as well as the authenticated messages. 6. If the system does not use SNMP v3, then this is a finding because as SNMP v1 and v2 do not have acceptable authentication capabilities.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
419	**Section:** Confidentiality **ID:** 1.h.4 The message processing model shall be SNMPv3 – snmpMessage ProcessingModel=3. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCCS-2	**Required:** MFSS, SS, LSC, MG,EBC,R,LS **Origin:** RFC 3414 11.1	1. Verify that the SMNPv3 processing model is SNMPv3-snmpMessageProcessingModel=3 2. Examine the SNMP configuration file and confirm that the snmpMessageProcessingModel is set to three.	CATIII	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
420	**Section:** Confidentiality **ID:** 1.h.5 The default encryption cipher for SNMPv3 shall be CBC-DES-128 – usmDESPrivProtocol – CBC-DES_128. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that the default encryption cipher for SNMPv3 is CBC-DES-128 usmDESPrivProtocol-CBC-DES-128. 2. Examine the SNMP configuration file and verify that the default encryption cipher CBC-DES-128 is being used.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
421	**Section:** Confidentiality **ID:** 1.h.6 If the system recieves SNMP response messages, the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that the SNMPv3 engine discards all response messages that do not correspond to any current outstanding request messages. 2. Verify that the system is capable of using 160-HMAC-SHA1 as the default integrity mechanism for SRTP.	CAT III	

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
422	**Section:** Confidentiality **ID:** 1.h.7 If the system recieves SNMP responses, the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCFA-1	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that an SNMPv3 Command Generator Application discards any Response Class PDU for which there is no outstanding Confirmed Class PDU. 2. Verify that a crafted response PDU injected will be ignored. 3. Verify subsequent valid request message is responded to properly.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
423	**Section:** Confidentiality **ID:** 1.h.8 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. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCFA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that when the system uses msgID for correlating response messages to outstanding request messages, the SNMPv3 engine uses different msgIDs in all such request messages that it sends out during a configurable 150-second Time Window and has a default of 150 seconds. 2. While monitoring the SNMP traffic, perform basic SNMP requests on the system from the NMS. 3. Examine the SNMP traffic and confirm that the msgIDs are different.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
424	**Section:** Confidentiality **ID:** 1.h.9 An SNMPv3 command Generator or Notification Originator Application shall use different request-ids in all Request PDU that it sends out during a Time Window. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCFA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that an SNMPv3 command Generator or Notification Originator Application uses different request-IDs in all request PDUs that it sends out during a configurable period and has a default of 150 seconds. 2. While monitoring (sniffing) SNMP traffic, cause the system issue multiple Request PDU SNMP commands. 3. Examine the SNMP traffic and confirm that the request-IDs are different in all of the “Request” PDUs.	CAT III	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
425	**Section:** Confidentiality **ID:** 1.h.10 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. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCFA-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** RFC 3414 11.1	1. Verify that an SNMPv3 command Generator or Notification Originator Application uses different request-IDs in all Request PDUs that it sends out during a configurable period and has a default of 150 seconds. 2. From the NMS, attempt to send the system an SNMP message, but before the system responds, send another SNMP message. 3. Verify that the second SNMP message was not sent until a response from the first message was received.	CAT III	

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
426	**Section:** Confidentiality **ID:** 1.h.11 The appliance using SNMPv3 shall implement the key-localization mechanism. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system uses the key-localization mechanism for SNMPv3. 2. Verify that there exists a secret key shared between the user and the SNMP engine.	CAT III	
	IA Control: IAKM-2	**Origin:** RFC 3414 11.3			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
427	**Section:** Confidentiality **ID:** 1.i The system shall be capable of ensuring confidentiality by protecting one user's resource from being accessed by others who do not have such authorization. Note: An instance of this is if the system is accessed by users (including third-party service providers) who need confidentiality of their respective resources (which may contain proprietary, confidential, or sensitive information) from one another or from unauthorized personnel. Note: If resource control mechanisms such as command control, object control, record control, and field control, fail to provide the required confidentiality, it may be necessary to partition the system database to protect on user's data from being accessed by another user. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, and EBC	1. Verify that the system is capable of ensuring confidentiality by protecting one user's resource form being accessed by others who do not have such authorization. 2. Login to the system as a "normal user." 3. Create a temporary file or some other user resource. 4. Change the security attributes on the file or resource such that only the creating user can access it. 5. Login as another "normal user" and attempt to access the file or resource created in step 2. 6. Verify that access to the file or resource was denied.	CAT II	
	IA Control: IAIA-1 and ECPA-1	**Origin:** GR-815 CORE CR3-102[67] & CR3-103[68];			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
428	**Section:** Confidentiality **ID:** 1.j The system shall be capable of using a separate interface for management traffic. Note: The separate interface may be a logically or physically separate interface. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system is capable of using a separate logical or physical interface for management traffic. 2. Confirm that any attempt to access the management control panel through any VLAN except the management VLAN is not possible. 3. If access to the management function is physically separated by an interface, confirm that other interfaces cannot access the management function(s).	CAT II	
	IA Control: DCSP-1	**Origin:** Network STIG v7r1			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
429	**Section:** Confidentiality **ID:** 1.j.1 The system shall be capable of protecting the management interface using filters. Note: Within a router, the filters may be achieved using ACLs. Within an appliance, the filters may include internal routing procedures to the different physical interfaces or VLAN tagging. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system can apply filters (ACLs) to isolate traffic on the management interface. 2. Verify that a router or switch can institute an ACL to prevent unauthorized access to the interface. 3. Depending on the system, also confirm whether internal routing procedures protect the management Interface.	CAT II	
	IA Control: DCSP-1	**Origin:** Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
430	**Section:** Confidentiality **ID:** 1.j.2 The system shall be capable of using VLANs to segregate management traffic from other types of traffic, where feasible. Note: The R and LS will implement the VLAN, but the other appliances will have to tag the packets with the correct VLAN tag. **Reference:** UCR 5.4.6.2.3	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the system is capable of using VLANs to isolate management traffic from other types of traffic where possible. 2. The configuration file should be inspected to ensure that voice, data, and management traffic is isolated by the use of VLANs. 3. Confirm that VLAN tagging is also being used.	CAT II	
	IA Control: DCSP-1	**Origin:** Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
431	**Section:** Confidentiality **ID:** 1.k If the system uses IPsec, the system shall be capable of using 3DES-CBC (class value 5) as the default IKE encryption algorithm **[Threshold]** AES-CBC **[Objective].** **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, and MG	1. Verify that the system is capable of using 3DES-CBC (class value 5) as the default IKE encryption algorithm (Threshold), AES-CBC (Objective). 2. From the maintenance security control panel, confirm that the 3DES-CBC algorithm can be selected. Alternately, the configuration file can be inspected to confirm 3DES-CBC is present. 3. During security key negotiation, monitor the traffic and confirm that minimally, the 3DES-CBC algorithm is used. Note: Protocol traffic and handshake for the establishment of encrypted sessions will be observed during IPV testing. IPV testing will verify that the establish session is using the correct algorithm.	CAT III	
	IA Control: DCNR-1	**Origin:** RFC 2409 Appendix A RFC 2409 Appendix A			

Table E-10. Confidentiality (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
432	**Section:** Confidentiality **ID:** 1.l If the system uses different signaling protocols, (i.e., H.323 and AS-SIP), then the system shall be capable of translating/transferring the bearer keys between the different signaling protocols. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Conditional:** MFSS, SS, LSC, and MG **Origin:** Vendor agreement	1. Verify that the system is capable of translating/transferring the bearer keys between different signaling protocols. 2. Originate calls between two EIs: One that does support AS-SIP and one that does not support AS-SIP (e.g., an H.323 VTC device calls a SIP VTC device.). 3. Verify that the keys are translated and transferred between both the supporting and non-supporting protocols. Note: The IPV test team will address this requirement during the IPV testing phase.	CAT I	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
433	**Section:** Confidentiality **ID:** 1.m The system shall re-key each encrypted session once the session has transmitted a maximum of $2^{L/4}$ blocks of data. 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. **Reference:** UCR 5.4.6.2.3 **IA Control:** DCNR-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** VVoIP Core Team	1. Verify that the system rekeys each encrypted session once the session has transmitted a maximum of $2^{L/4}$ blocks of data. L is the block length in bits (e.g., 128 for AES_128) and shall be configurable. 2. Verify that the "Block Length" is configurable by examining the Administration control panel for security and that the actual configuration file contains the tunable block length. 3. If testing the re-keying process is unreasonable, an LoC with a certificate from the granting certifier is acceptable. Note: The IPV test team will address this requirement during the IPV testing phase.	CAT III	

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
434	**Section:** Confidentiality **ID:** 1.n If the system 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 re-keying. Note: The re-keying 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 they would be able to eavesdrop on the forwarded session. LSCs, MFSSs, and SSs may act as a B2BUA for an EI and would, therefore, originate the AS-SIP session on behalf of the EI. **Reference:** UCR 5.4.6.2.3	**Conditional:** MFSS, SS, LSC, MG, and EI	1. Upon completion of the forwarding, confirm that the originating party no longer has information available about the forwarding party, either by monitoring the traffic with a sniffer, or by using a specific tool. 2. Confirm from the originating party that re-keying has occurred. Note: The IPV test team will address this requirement during the IPV testing phase.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
435	**Section:** Confidentiality **ID:** 1.o If the EI acts as a bridge or an MCU, it shall establish a unique key for each EI connection. **Reference:** UCR 5.4.6.2.3	**Conditional:** EI	Verify that if the EI acts as a bridge or an MCU, it shall establish a unique key for each EI connection. Note: The IPV test team will address this requirement during the IPV testing phase.	CAT II	
	IA Control: DCNR-1	**Origin:** RFC 4306			

Table E-10. Confidentiality (continued)

LEGEND:	
3DES	Triple Data Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Algorithm
AS-SIP	Assured Services – Sessions Initiation Protocol
CA	Certificate Authority
CAT	Category
CBC	Cipher Block Chaining
CLI	Command Line Interface
DCCS	Design Configuration Configuration Standards
DCFA	Design Configuration Functional Architecture of AIS Applications
DCNR	Design Configuration Non-repudiation
DCSP	Design Configuration Security Support Structure Partitioning
DES	Data Encryption Standard
DoD	Department of Defense
EBC	Edge Boundary Controller
ECCT	Enclave Computing Environment Encryption for Confidentiality (Data in Transit)
ECPA	Enclave Comuting Privilege Account
ECRC	Enclave Computing Environment Resource Control
ECTM	Enclave Computing Transmission
EI	End Instrument
FIPS	Federal Information Processing Standard
GR	Generic Requirements
HMAC	Hashed Message Authentication Code
IA	Information Assurance
IAAC	Enclave Computing Account Control
IAIA	Identification Authentication Individual Identification and Authentication
IAKM	Identification Authentication Key Management
IKE	Internet Key Exchange
ID	Identification
IPsec	Internet Protocol Security
IPV	Internet Protocol Vulnerability
ISAKMP	Internet Security Association and Key Management Protocol
IV	Initialization Vector
JTA	Joint Technical Architecture
LoC	Letter of Compliance
LoC	Loss of Carrier
LS	LAN Switch
LSC	Local Session Controller
LSC	Local Session Controller
MFSS	Multifunction Softswitch
MCU	Multipoint Control Unit
MEGACO	Gateway Control Protocol
MG	Media Gateway
MGCP	Media Gateway Control Protocol
MTU	Maximum Transmission Unit
NSA	National Security Agency
OAM&P	Operations Administration Maintenance and Planning
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standard
PKE	Public Key Encryption
PKI	Public Key Infrastructure
R	Router
RFC	Request for Comment
RSA	Rivest, Shamir, and Adelman
RTS	Real Time Services
SCTP	Stream Control Transmission Protocol
SDES	Session Descriptions
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	System Identification Profile
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SRTP	Secure Real-Time Transport Protocol
SS	Softswitch
SSH	Secure Shell
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guidelines
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UCR	Unified Capabilites Requirements
UDP	Universal Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing
VVoIP	Voice and Video over Internet Protocol

Table E-11. Non Repudiation

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
436	**Section:** Non-Repudiation **ID:** 1 The system shall be capable of providing non-repudiation and accountability services. Note: This assumes that authentication has already occurred as required previously. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the system provides a security log that records actions by users according to user-ID, date, time, and event.	CAT I	
	IA Control: DCNR-1	**Origin:** DoDD 6510.01D 4.2; CJCSI 6510.01D B.1.b.1; GR-815 CORE CR3-110[91]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
437	**Section:** Non-Repudiation **ID:** 1.a For user-accessible resources in the system that are created or modified by a user-ID via standard operations and maintenance procedures, the system shall be capable of providing a mechanism to identify the said user- ID, date, and time associated with the said resource creation or modification. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system provides a security log that records users' actions in relation to creation or modifications of resources, and records user-ID, date, time, and event. 2. Based on a "User's" authorization to create or change a resource, verify that any creation or change to a system resource is logged. Also, confirm that the system administrator's actions are logged.	CAT II	
	IA Control: DCFA-1	**Origin:** GR-815 CORE R3-91[59] and NSA 2.3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
438	**Section:** Non-Repudiation **ID:** 1.b The system shall be capable of auditing at the operating system and Database Management System (DBMS) levels and shall have a security log that contains information to support after the fact investigation of loss or impropriety and appropriate management response. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system has a robust security log that captures operating system and database management data. 2. If the system contains a database, verify that when the database administrator logs on to the system, the fact that he did log on is recorded in the security log. 3. If the database administrator performs a security-related change to the database, verify that the change is recorded in the security log (e.g., changing the permissions on table entries). Note: Capture any alteration of the system's configuration files that implement the overall security policy in the security log.	CAT I	
	IA Control: ECAT-2	**Origin:** GR-815 CORE R3-11[75]; OAM&P 123A; NSA 2.3.1; and DRSN STIG 4.6.5 & 6.2.8.3			

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
439	**Section:** Non-Repudiation **ID:** 1.b.1 The security log entry of any request or activity that is invoked by a user-ID shall be capable of including that user-ID so it becomes possible to establish user accountability. Note: The term "user-ID" shall be interpreted for this requirement to include users as well as processes. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the user-ID appears in the security log for any activity or request. 2. Confirm that the correct "User" information is recorded in the log file when the User initially logs on to the system, including user- ID, date and time. 3. Verify that the system logs any resource activity by the "User."	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815-CORE R3-112[76]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
440	**Section:** Non-Repudiation **ID:** 1.b.2 The security log shall be capable of protecting itself from unauthorized access or destruction. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that only the designated administrator and auditor may view the security log. 2. Verify that only the designated auditor may alter or destroy the security log.	CAT I	
	IA Control: ECTP-1	**Origin:** GR-815 CORE R3-114[78] & R3-115[79]; and NSA 2.3.1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
441	**Section:** Non-Repudiation **ID:** 1.b.2.a The security log protection, at a minimum, shall be capable of providing access control based on user privileges and interface (logical or physical) privileges. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that only the designated administrator and auditor the may view the security log. 2. Log into the system as the auditor. 3. Verify that the security file can be viewed. 4. Log into the system as the administrator. 5. Verify that the security log can be viewed, but not modified or deleted.	CAT II	
	IA Control: DCNR-1	**Origin:** GR-815 CORE Section 3.6.1 R3-114[78]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
442	**Section:** Non-Repudiation **ID:** 1.b.2.b The appliance shall have no mechanism for any external user (human or machine), including the administrator, to modify or delete the security log. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Confirm that no user, administrator, or auditor can edit or delete the security. 2. Log on as each of the following and attempt to delete the security log file: administrator, normal user, and auditor.	CAT II	
	IA Control: ECTP-1	**Origin:** GR-815 CORE Section 3.6.1 R3-115[79]			

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
443	**Section:** Non-Repudiation **ID:** 1.b.3 The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest). **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the security log is constructed in such a way as to allow continuous recording. 2. Verify that only appropriate designated personnel are able to print, copy, and upload the security log to ensure proper business continuity precautions.	CAT II	
	IA Control: ECAT-2 and ECTP-1	**Origin:** GR-815 CORE R3-116[80]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
444	**Section:** Non-Repudiation **ID:** 1.b.3.a The system shall be capable of generating a security log alarm base upon specific conditions (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload, disk space used). The alarm may necessitate uploading the security log (typically to some remote facility or other facility for long-term storage) to avoid an overwrite in the buffer. This upload may be automatically performed by the system or by an appropriate administrator. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the system has the capability to properly alert appropriately designated personnel that the security log is preparing to overwrite.	CAT III	
	IA Control: ECAT-2	**Origin:** GR-815 CORE Section 3.6.1 R3-115[79]; R3-116[80]; R3-117[81] & R3-118[82]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
445	**Section:** Non-Repudiation **ID:** 1.b.4 Only the system security administrator role shall have the ability to retrieve, print, copy, and upload the security log(s). **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the security log(s) may only be viewed by the designated administrator and auditor. 2. Verify that retrieval, printing, copying, and uploading of the security log(s) may only be conducted by the system security administrator (auditor). 3. Verify there is a separate user-ID (Auditor) that can perform this duty.	CAT III	
	IA Control: ECAT-2	**Origin:** GR-815 CORE R3-117[81] & R3-118[82]			

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
446	**Section:** Non-Repudiation **ID:** 1.b.4.a The system 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. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that a downloaded security log records and maintains time sequentially and records all records up to the time when copying starts.	CAT III	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-118[82]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
447	**Section:** Non-Repudiation **ID:** 1.b.5 The system security log shall survive system restart (e.g. via reloading). **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Initialize the system (restart the system) and test whether the history files retain the records. If the records do not survive a system restart, the system fails the test. 2. Confirm the current information in the Security log. 3. Perform a hard restart on the system. 4. Confirm that the information in the Security log before the restart is the same.	CAT II	
	IA Control: ECTP-1	**Origin:** GR-815 CORE R3-119[83]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
448	**Section:** Non-Repudiation **ID:** 1.b.6 The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console) to include the following events by default as a minimum: **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS		CAT II	
	IA Control: ECAR-2	**Origin:** CJCSM 6510.01 C-A-4.9; VoIP STIG Vulnerabilities 123B, 23A, 23B, 23C, 23D, 23E, 3A, 3B, 3D; and GR-815-CORE R3-120[84], CR3-121[85]			

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
449	**Section:** Non-Repudiation **ID:** 1.b.6.a Invalid user authentication attempt. **Reference:** UCR 5.4.6.2.4.	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator with an invalid password. 2. Verify the security log reflects an invalid authentication attempt. 3. Login as a normal user, using an invalid password. 4. Verify the security log reflects an invalid authentication attempt.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
450	**Section:** Non-Repudiation **ID:** 1.b.6.b Unauthorized attempts to access system resources. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Attempt to access resources with unauthorized login credentials. 2. Confirm all unauthorized attempts are recorded in the security log.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
451	**Section:** Non-Repudiation **ID:** 1.b.6.c Changes made in a user's security profile and attributes. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator. 2. Change the security profile of a normal user. 3. Confirm that this change is recorded in the security log.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
452	**Section:** Non-Repudiation **ID:** 1.b.6.d Changes made in security profiles and attributes associated with an interface/port. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator. 2. For the system, attempt to edit a security attribute associated with an interface and/or port. 3. Confirm that this action is recorded in the system security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
453	**Section:** Non-Repudiation **ID:** 1.b.6.e Changes made in access rights associated with resources (i.e., privileges required of a user and an interface/ports to access). **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Changes made in access rights associated with resources.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
454	**Section:** Non-Repudiation **ID:** 1.b.6.f Changes made in system security configuration. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator 2. Make a change in the system security configuration file. 3. Verify that the change is recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
455	**Section:** Non-Repudiation **ID:** 1.b.6.g Creation and modification of the system resources performed via standard operations and maintenance procedures. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator. 2. Perform a modification of the system resource(s) as would be done during normal operations and maintenance procedures. 3. Verify that the changes were recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
456	**Section:** Non-Repudiation **ID:** 1.b.6.h Disabling a user profile. **Reference:** UCR 5.4.6.2.4	MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator and perform a disabling of a normal user profile. 2. Verify that this was recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1R3-120[84]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
457	**Section:** Non-Repudiation **ID:** 1.b.6.i Events associated with privileged users. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. If the system does not support privileged users, this test is not applicable. 2. For those events that can be performed by a "Privileged User", confirm that those events are recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6.1 CR3-121[85]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
458	**Section:** Non-Repudiation **ID:** 1.b.6.j If the system contains resources that are deemed mission critical (for example, a risk analysis classifies it critical), then the system should log any events associated with access to those mission critical resources. **Reference:** UCR 5.4.6.2.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. If the system does not contain mission critical resources, this test is not applicable. 2. Attempt to remove or modify the mission critical resource. 3. Verify the action is recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6 1 R3-112[85]			

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
459	**Section:** Non-Repudiation **ID:** 1.b.6.k Successful login attempts. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the Administrator and Normal User successful logins are recorded in the security log file.	CAT I	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6 1 R3-112[76]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
460	**Section:** Non-Repudiation **ID:** 1.b.6.l Failed login attempts to include the following: **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that the Administrator and Normal User unsuccessful logins are recorded in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE Section 3.6 1 R3-112[76]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
461	**Section:** Non-Repudiation **ID:** 1.b.6.l.i Failed login attempt due to an excessive number of logon attempts. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Login as administrator with an invalid password four times. 2. Confirm that an entry in the security log indicates the Administrator was temporarily locked out because of excessive number of attempts.	CAT II	
	IA Control: ECAR-2	**Origin:** UNIX STIG Section 3.16 GEN002720			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
462	**Section:** Non-Repudiation **ID:** 1.b.6.l.ii Failed logon attempt due to blocking or blacklisting of a user-ID. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Failed logon attempt due to blocking or blacklisting of a user-ID.	CAT II	
	IA Control: ECAR-2	**Origin:** Database STIG Section 3.3.2 DG0146			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
463	**Section:** Non-Repudiation **ID:** 1.b.6.l.iii Failed logon attempt due to blocking or blacklisting of a terminal. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Confirm that a failed logon attempt due to blocking or blacklisting of a terminal is logged in the security log file.	CAT II	
	IA Control: ECAR-2	**Origin:** Database STIG Section 3.3.2 DG0146			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
464	**Section:** Non-Repudiation **ID:** 1.b.6.l.iv Failed logon attempt due to blocking or blacklisting an access port. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC,MG, EBC, R, and LS	Confirm that a failed logon attempt due to blocking or blacklisting of a access port is logged in the security log file.	CAT III	
	IA Control: ECAR-2	**Origin:** Database STIG Section 3.3.2 DG0141			

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
465	**Section:** Non-Repudiation **ID:** 1.b.7 The security log event record shall be capable of including at least the following information: **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as administrator. 2. Remove a resource from service. 3. Verify that the removal of the resource, along with a time and date stamp, is recorded in the security log file. 4. Place the resource back in service. 5. Verify the date and time of the resource being placed back in service is recorded in the security log file.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
466	**Section:** Non-Repudiation **ID:** 1.b.7.a Date and time of the event (both start and stop). **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as administrator. 2. Verify date and time is recorded in the system security log file for start and stop time.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
467	**Section:** Non-Repudiation **ID:** 1.b.7.b User-ID including associated terminal, port, network address, or communication device. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as a normal user. 2. Confirm that the security log contains the associated terminal/port, IP address, or communication device used.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
468	**Section:** Non-Repudiation **ID:** 1.b.7.c Event type. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as administrator. 2. Create a temporary file. 3. Verify the security log contains an entry for the file creation. 4. Delete the above file. 5. Verify the security log contains an entry for the file deletion.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
469	**Section:** Non-Repudiation **ID:** 1.b.7.d Names of resources accessed. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as administrator. 2. Attempt to access a system resource (e.g., disable an interface). 3. Confirm that the disable, as well as the interface, name is recorded in the security log file.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
470	**Section:** Non-Repudiation **ID:** 1.b.7.e Success or failure of the event. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAR-2	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE Section 3.6 1 R3-122[86]	1. Login as administrator. 2. Attempt to access a system resource (e.g., disable an interface). 3. Confirm that the disable, as well as the interface, name is recorded in the security log file. 4. Confirm that the Success or Failure is indicated in the security log file.	CAT II	

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
471	**Section:** Non-Repudiation **ID:** 1.b.8 The system shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate Networks Operations Center (NOC) if the security log fails to record the events that are required to be recorded. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-123[87]	1. Test if the system generates an alarm when the history files malfunction. If there is no provision for such an alarm, the system fails the test. 2. Configure the log files such that it is not possible to write to by the system. This could be by temporarily changing permissions on the file, removing the file, or changing the threshold percentage to 100%. 3. Verify that an attempt by the system to write the log file fails and an appropriate alert is generated.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
472	**Section:** Non-Repudiation **ID:** 1.b.9 The system shall not record actual or attempted passwords in the security log. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECAT-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** GR-815 CORE R3-124[88]	1. Verify that clear text passwords are not recorded in the security log. 2. Using all methods of access to the system, including CLI, Web Access and/or operating system application, log into the system. 3. Verify that the password used for access is not recorded in the security log.	CAT I	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
473	**Section:** Non-Repudiation **ID:** 1.b.10 The system shall ensure that security and audit logs are maintained separate from other audit logs (history or CDR audit logs). **Reference:** UCR 5.4.6.2.4 **IA Control:** ECRR-1	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS **Origin:** Suggestion from FSO	1. Verify the system security and audit logs are maintained separate for other audit logs. 2. Confirm that any security related activities (e.g., changing permissions on objects or changing authentication data) are recorded in a separate log file from the System log or other logs being used in the system.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
474	**Section:** Non-Repudiation **ID:** 1.b.11 The system shall be capable of transmitting all logs to a remote log server in a secure manner. Note: Secure manner may be accomplished by using industry best practices to ensure the confidentiality and integrity of the logs during transfer. **Reference:** UCR 5.4.6.2.4 **IA Control:** ECTM-2	**Required:** MFSS, SS, LSC, MG, EBC, R, LS **Origin:** NSA 2.3.1 and FSO clarification	Verify that the system is capable of transmitting all logs to a remote log server in a secure manner. Note: Remote transmission must meet encryption and transport requirements.	CAT II	

Table E-11. Non Repudiation (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
475	**Section:** Non-Repudiation **ID:** 1.c If the system accesses other systems to pass on a request or activity that has a user-ID associated with it, the system 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. **Reference:** UCR 5.4.6.2.4	**Conditional:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify that the user-ID is traceable to the other systems and events are recorded in the security log of this system as well as the other systems that were accessed. 2. For a SIP call, if authentication is required, the authentication user data should be sent to the SIP server. It should be recorded there. Note: If the system does not have the capability of granting access to other systems, this test is not applicable.	CAT II	
	IA Control: ECAR-2	**Origin:** GR-815 CORE CR3-113[77]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
476	**Section:** Non-Repudiation **ID:** 1.d The system 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. **Reference:** UCR 5.4.6.2.4	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify that a post-collection audit analysis tool is supported by the system. This data-mining tool needs to be able to provide typical reports in regard to recorded activity in the security log.	CAT III	
	IA Control: ECRG-1	**Origin:** GR-815 CORE R3-125			

LEGEND:

AIS	Automated Information System
CAT	Category
CDR	Compact Disk Recordable
CLI	Command Line Interface
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
DBMS	Database Management System
DCFA	Design Configuration Functional Architecture (of AIS Applications)
DCNR	Design Configuration Non-repudiation
DoDD	Department of Defense Directive
DRSN	Defense Red Switch Network
EBC	Edge Border Controller
ECAR	ECE Audit Record Content
ECAT	ECE Audit Trail, Monitoring, Analysis, and Reporting
ECE	Enclave Computing Environment
ECRG	ECE Audit Reduction and Report Generation
ECRR	ECE Audit Recording Retention
ECTM	ECE Transmission Integrity Controls
ECTP	ECE Audit Trail Protection
FSO	Field Security Office
GR	Generic Requirement
IA	Information Assurance
ID	Identification
IP	Internet Protocol
LAN	Local Area Network
LS	LAN Switch
LSC	Local Session Controller
MFSS	Multifunction Softswitch
MG	Media Gateway
NOC	Network Operations Center
NSA	National Security Agency
OAM&P	Operations Administration Maintenance and Planning
R	Router
SIP	System Identification Profile
SS	Softswitch
STIG	Security Technical Implementation Guidelines
UCR	Unified Capabilites Requirements
VoIP	Voice over Internet Protocol

Table E-12. Availability

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
477	**Section:** Availability **ID:** 1 The VVoIP system (MFSS, LSC1, etc.) shall meet the availability requirements as stated in the UCR 2008, Section 5.3.2.2.3.8, System Quality Factors. There are additional IA specific IA availability requirements specified below that are not covered in the System Quality Factors section of this UCR. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify business continuity procedures are in place for the system under test to include back-up capabilities for the system.	CAT I	
	IA Control: DCAR-1, DCCT-1, DCHW-1, DCSD-1, DCSW-1, ECSC-1, ECVP-1, EBCR-1, EBVC-1, PEEL-2, PEFD-2, PEFI-1, PEFS-2, PEHC-2, PEMS-1, PETC-2, PETN-1, PRRB-1, COAS-2, COBR-1, CODB-3, CODP-3, COEB-2, COED-2, COEF-2, COMS-2, COPS-3, COSP-2, COSW-1, COTR-1, VIIR-2, and VIVM-1	**Origin:** CJCSI 4.a and GIG CRD IV.B.4k, IV.B.4n			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
478	**Section:** Availability **ID:** 1.a The system shall have robustness through the maximum use of alternative routing, backup. Note: From a vendor's perspective, this requirement is associated with meeting the reliability numbers for the system. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Interoperability and functionality checks to include alternative routing, alternate power supplies, and redundancy are tested during interoperability testing.	CAT II	
	IA Control: COBR-1	**Origin:** CJCSI 4.a; GIG CRD IV.B.4k, IV.B.4n & GR-815 CORE CR3-138[106			

Table E-12. Availability (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
479	**Section:** Availability **ID:** 1.b The system shall have mechanisms to allow "secure recovery" to reduce vulnerability due to failure or discontinuity making it vulnerable to security compromise. Note: This requirement will ensure that as a system is reestablished, it does not reboot in an unsecured mode such as with factory set configurations. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the system is capable of executing procedures or mechanisms that provided for a secure recovery. 2. Confirm all of the user-IDs as well as application IDs and passwords. 3. Perform a re-boot on the system. 4. Verify a secure recovery occurred by confirming the User-IDs and Applications have the same passwords before the re-boot occurred.	CAT III	
	IA Control: COTR-1	**Origin:** GR-815 CORE CR3-138[106]			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
480	**Section:** Availability **ID:** 1.c The system shall have the capability to rebuild the system to a base version and subsequent vendor modification of that version, if that version and modification are currently in use. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	Verify the capability to rebuild a base version and subsequent vendor modifications (e.g., patches) of the version through uploading of the latest backed up state of the system.	CAT III	
	IA Control: DCSW-1	**Origin:** GR-815 CORE R3-139[107] and DRSN STIG 4.6.5			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
481	**Section:** Availability **ID:** 1.d The system shall have the capability to provide adequate checkpoints in a process flow of the software system so that, upon detection of service deterioration, a recovery to an acceptable level is facilitated. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Ideally, some test traffic should be running on the system during the execution of this test procedure. 2. Attempt to cause service disruptions and service deterioration. This could be by either of the following: momentarily removing power from the system, or removing circuit packs, or pulling cables. 3. Upon restoration of service, verify that the test traffic and service is at an acceptable level.	CAT III	
	IA Control: DCSS-1	**Origin:** GR-815 CORE R3-140[108]			

Table E-12. Availability (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
482	**Section:** Availability **ID:** 1.e The system shall have a capability to define a threshold e.g., percentage full by new entries since last upload, time interval elapsed since last upload to initiate a warning before a security log buffer overflow. **Reference:** UCR 5.4.6.2.5	**Required:** MFSS, SS, LSC, MG, EBC, R, and LS	1. Verify the capability of a warning alerting an administrator when buffer overflow occurs. 2. If the system does not have the ability to set a threshold percentage before sending warning of log buffer overflow, then this is a finding. 3. Determine the log files current percentage of being full. 4. Set the threshold percentage to current percentage plus one percent. 5. Cause additional log information to be recorded, so that the new information will cause the log file to exceed the threshold. 6. Verify that a warning was generated.	CAT III	
	IA Control: ECAT-2	**Origin:** GR-815 CORE R3-141[81]			

LEGEND:

CAT	Category	ECVP	Enclave Computing Environment Virus Protection
CJCSI	Chairman of the Joint Chiefs of Staff Instruction	GIG	Global Information Grid
COAS	Continuity Alternate Site	GR	Generic Requirement
COBR	Continuity Backup Restoration	IA	Information Assurance
CODB	Continuity Data Backup	ID	Identification
CODP	Continuity Disaster Recovery and Planning	LS	LAN Switch
COEB	Continuity Enclave Boundary Defense	LSC	Local Session Controller
COED	Continuity Scheduled Exercises and Drills	MFS	Multifunction Softswitch
COEF	Continuity Identification of Essential Functions	MG	Media Gateway
COMS	Continuity Maintenance Support	PEEL	Physical Environmental Emergency Lighting
COPS	Continuity Power Supply	PEFD	Physical Environmental Fire Detection
COSP	Continuity Spare Parts	PEFI	Physical Environmental Fire Inspection
COSW	Continuity Software	PEFS	Physical Environmental Fire Suppression
COTR	Continuity Trusted Recovery	PEHC	Physical Environmental Humidity Controls
CRD	Capstone Requirements Document	PEMS	Physical Environmental Master Switch
DCAR	Design Configuration Procedural Review	PETC	Physical Environmental Temperature Controls
DCCT	Design Configuration Compliance Testing	PETN	Physical Environmental Environmental Control Training
DCHW	Design Configuration Hardware Baseline	PRRB	Personnel Rules Responsible Behavior
DCSD	Design Configuration IA Documentation	R	Router
DCSS	Design Configuration System State Changes	SS	Softswitch
DCSW	Design Configuration Software	STIG	Security Technical Implementation Guidelines
DRSN	Defense Red Switch Network	UCR	Unified Capabilities Requirements
EBC	Edge Border Controller	VIIR	Vulnerability Incident and Incident Response
EBCR	Enclave Boundary Defense Connection Rules	VIVM	Vulnerability Incident and Vulnerability Management
EBVC	Enclave Boundary VLAN Controls	VLAN	Virtual Local Area Network
ECAT	Enclave Computing Environment Audit Trail	VVoIP	Voice and Video Over Internet Protocol
ECSC	Enclave Computing Environment Security Configuration Compliance		

Table E-13. IPv6 Requirements

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
1	**Section:** System Requirements **ID:** 1 The system shall support dual IPv4 and IPv6 stacks as described in RFC 4213. NOTE: The tunnel requirements are only associated with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers. **Reference:** UCR 2008 5.3.5.3	Required: SS, NA, EBC, R, LS, – Conditional: EI	1. Conduct an analysis of the system configurations. 2. Verify traffic generated is accepted in IPv4 and IPv6 format. 3. If tunneling is utilized verify that the tunnel is able to transmit IPv6 to IPv4 and also IPv4 to IPv6. 4. Verify that if tunneling is utilized that it is able to process correct decapsulation checks to discard any IPv6 packets with IPv4 compatible addresses in IPv6 header field.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 4213 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
2	**Section:** System Requirements **ID:** 1.1 If the system supports routing functions, the system shall support the manual tunnel requirements as described in RFC 4213. **Reference:** UCR 5.3.5.3	Conditional: R, LS	1. Verify that the administrator has the ability to manually configure tunnel requirements. 2. Ensure that changes are successful to allow for secure traffic. 3. Verify that IPv6 packets are transported over IPv4 correctly.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 4213 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
3	**Section:** System Requirements **ID:** 2 The system shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. **Reference:** UCR 2008 5.3.5.3	Required: SS, NA, EBC, R, LS, EI	1. Verify that all IPv6 addresses are constructed per the IPv6 format in section 3. of RFC 2460. 2. Ensure the IPv6 format of the address is updated according to RFC 5095 which removes the use of the IPv6 “extension header” called Routing Header.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5095 and Network STIG v7r1			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
4	**Section:** System Requirements **ID:** 3 The system shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented. **Reference:** UCR 2008 5.3.5.3	Required: SS, EBC, R, LS, EI	1. Verify that the system is able to transmit IPv6 packets over the network. 2. Verify the Address Token in the packet is not the node's 48-bit MAC address per RFC 1972, but is replaced by the Interface Identifier per RFC 2464. EXAMPLE: The Organizationally Unique Identifier of the Ethernet address (the first three octets) becomes the company_id of the EUI-64 (the first three octets). The fourth and fifth octets of the EUI are set to the fixed value FFFE hexadecimal. The last three octets of the Ethernet address become the last three octets of the EUI-64. For example, the Interface Identifier for an Ethernet interface whose built-in address is, in hexadecimal, 34-56-78-9A-BC-DE would be 36-56-78-FF-FE-9A-BC-DE.	CAT III	
	IA Control: ECSC-1	**Origin:** RFC 2464 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
5	**Section:** MTU **ID:** 4 The system shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981). **Reference:** UCR 2008 5.3.5.3.1	Required: EBC, R, LS, EI (Softphone only)	1. Ensure that when the system sends out a large sized IPv6 packet that it has the ability to break up those packets into smaller packets on the network. 2. Verify that if a node receives a packet too big message the node attempts to reduce the size of the original packet sent according to RFC 1981.	CAT I	
	IA Control: ECSC-1	**Origin:** RFC 1981 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
6	**Section:** MTU **ID:** 5 The system shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095). NOTE: Guidance on MTU requirements and settings can be found in UCR 2008, Section 5.3.3.10.1.2 Layer 2- Data Link Layer. **Reference:** UCR 2008 5.3.5.3.1	Required: SS, NA, EBC, R, LS, EI	1. Verify that the NIC MTU size is set to 1280 bytes. 2. Create packets that are smaller than that of the minimum MTU of 1280 bytes and ensure that a fragment header is appended to the packet it to allow it to meet the minimum MTU size of 1280 bytes.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5095 and Network STIG v7r1			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
7	**Section:** MTU **ID:** 6 If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the system shall ignore the request for the smaller MTU and shall include a fragment header in the packet. NOTE: This is to mitigate an attack where the path MTU is adequate, but the Packet Too Big messages are used to make the packet so small it is inefficient. **Reference:** UCR 2008 5.3.5.3.1	Conditional: SS, NA, EBC, R, LS, EI	1. Verify that the NIC MTU size is set to 1280 bytes. 2. Create packets that are smaller than that of the minimum MTU of 1280 bytes and ensure that a fragment header is appended to the packet it to allow it to meet the minimum MTU size of 1280 bytes. 3. Ensure that the traffic is passed correctly with the appended header.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5095			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
8	**Section:** Flow Label **ID:** 7 The system shall not use the Flow Label field as described in RFC 2460. **Reference:** UCR 2008 5.3.5.3.2	Required: SS, NA, EBC, EI	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send the packet to a host or router that does not support the flow label field as described in 2460. 3. Observe the packet as it passes through that host or router and ensure that it ignores the field when receiving the packet.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2460 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
9	**Section:** Flow Label **ID:** 7.1 The system shall be capable of setting the Flow Label field to zero when originating a packet. **Reference:** UCR 2008 5.3.5.3.2	Required: SS, NA, EBC, EI	1. Attempt to create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send out the IPv6 packet on the network. 2. Ensure that the flow label field on the packet is set to zero.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2460 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
10	**Section:** Flow Label **ID:** 7.2 The system shall not modify the Flow Label field when forwarding packets. **Reference:** UCR 2008 5.3.5.3.2	Required: SS, NA, EBC	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Attempt to send out the IPv6 packet through the system tested host or router. 3. Ensure that the Flow Label field set in the header of the IPv6 packets created when passed through the host or router on the network are not modified.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2460 and Network STIG v7r1			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
11	**Section:** Flow Label **ID:** 7.3 The system shall be capable of ignoring the Flow Label field when receiving packets. **Reference:** UCR 2008 5.3.5.3.2	Required: SS, NA, EBC, EI	1. Create IPv6 packets with the flow label field set in the IPv6 header. 2. Send out the IPv6 packet on to the system under test. 3. Ensure that the Flow Label field is ignored and that the system does not process the packet according to the Flow Label Field in the IPv6 header.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2460 and Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
12	**Section:** Address **ID:** 8 The system shall support the IPv6 Addressing Architecture as described in RFC 4291. NOTE: The use of "IPv4 Mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities. **Reference:** UCR 2008 5.3.5.3.3	Required: SS, NA, EBC, R, LS, EI	1. Verify the system is capable of communication through IPv6. 2. Ensure that the system follows the IPv6 Addressing Architecture in RFC 4291. 3. Ensure that the system does not use IPV4 mapped IPv6 addresses due to improper handling by some IPv4 devices.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4291 and Network STIG v7r1			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
13	**Section:** DHCP **ID:** 10 If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 system, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315. NOTE 1: UCR 2008, Section 5.4, Information Assurance, requires that the voice or video DHCP servers are not to be located on the same physical appliance as the voice or video LAN switches and routers in accordance with the Security Technical Implementation Guides (STIGs). Also, the VoIP STIG requires (in VoIP 0082) separate DHCP servers for (1) the phone system in the phone VLAN(s) and (2) the data devices (PCs) in the data VLAN(s). NOTE 2: There is no requirement that separate DHCP servers be used for IPv4 and for IPv6. **Reference:** UCR 2008 5.3.5.3.4	Conditional: SS, NA EI, R, LS	1. Confirm that the system is capable of utilizing DHCP Note: If the system does not use DHCP services, this requirement test procedure is not applicable. 2. Determine the Identify of the DHCP server. 3. Configure the system to obtain an IP address through dynamic allocation as opposed to automatic or manual allocation. 4. Ensure the system attempts to connect to the DHCP server and that the traffic passed between the systems and the IP addressing is processed securely. 5. Perform functionality checks to verify that it is capable of communication with the new address.	CAT II	
	IA Control: DCCS-2 and DCPA-1	**Origin:** RFC 3315			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
14	**Section:** DHCP **ID:** 10.1 If the system is a DHCPv6 client, the system shall discard any messages that contain options that are not allowed, which are specified in Section 15 of RFC 3315. **Reference:** UCR 2008 5.3.5.3.4	Conditional: SS, NA, EI	1. Verify that DHCP is currently in use. 2. Attempt to send a DHCP message to the client with an improper option set for the message. (e.g., an Identity Association option in an Information-Request message). 3. Observe the actions of the host to ensure that the message is discarded.	CAT II	
	IA Control: DCBP-1 ECSC-1	**Origin:** RFC 3315			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
15	**Section:** DHCP **ID:** 10.2 The system shall support DHCPv6 as described in RFC 3315. NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the end instrument. It is not expected that other UC appliances will use DHCPv6. **Reference:** UCR 2008 5.3.5.3.4	Required: EI	1. Confirm that the system is capable of utilizing DHCP Note: If the system does not use DHCP services, this requirement test procedure is not applicable. 2. Configure the system to obtain an IP address through dynamic allocation as opposed to automatic or manual allocation. 3. Verify that the system supports the ability of obtaining a new IP address from the DHCP server. 4. Observe the traffic between the host and the DHCP server to insure that it is correctly processing the DHCP requests per RFC 3315.	CAT III	
	IA Control: DCSP-1 and ECSC-1	**Origin:** RFC 3315			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
16	**Section:** DHCP **ID:** 10.2.1 If the system is a DHCPv6 client, and the first Retransmission Timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall continue with a client-initiated message exchange by sending a Request message. **Reference:** UCR 2008 5.3.5.3.4	Required: EI Conditional: SS, NA	1. Verify that DHCP is currently in use. 2. Send a solicit message from the system under test. 3. Ensure that an Advertise message with a preference value of 255 is sent to the host. 4. Once the host receives the advertise message observe traffic between the host and the DHCP server 5. Verify that the client initiates a request message.	CAT II	
	IA Control: DCBP-1 and ECSC-1	**Origin:** RFC 3315			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
17	**Section:** DHCP **ID:** 10.2.2 If the system is a DHCPv6 client and the DHCPv6 message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs. NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds. **Reference:** UCR 2008 5.3.5.3.4	Required: EI Conditional: SS, NA	1. With the system under test attempt to initiate a message exchange to a DHCPv6 server 2. Ensure that the message exchange between the system under test and the DHCP server fails. 3. After the failure of the message exchange fails attempt to restart the process through user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event. 4. Verify that the reconfiguration process restarts and the client attempts to communicate with the server.	CAT II	
	IA Control: DCBP-1 and ECSC-1	**Origin:** RFC 3315			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
18	**Section:** DHCP **ID:** 10.2.3 If the system is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server. **Reference:** UCR 2008 5.3.5.3.4	Required: EI Conditional: SS, NA	1. With the system being tested initiate an information request message to the DHCPv6 server 2. Attempt to send an information request without a Client Identifier and ensure that the system is unable to be authenticated to the DHCPv6 server 3. Attempt to send an information request with a Client Identifier and ensure that the system is now able to be authenticated to the DHCPv6 server.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3315			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
19	**Section:** DHCP **ID:** 10.2.4 If the system is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself. **Reference:** UCR 2008 5.3.5.3.4	Required: EI Conditional: SS, NA	1. Prepare the system under test to request an address from the DHCPv6 server. 2. Ensure that the server attempts to assign the system an address that is already in use by another client. 3. Observe the actions of the system to ensure that it sends a decline message back to the DHCP server to inform it that the address assigned is already in use.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3315			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
20	**Section:** DHCP **ID:** 10.2.5 If the system is a DHCPv6 client, it shall log all reconfigure events. **Reference:** UCR 2008 5.3.5.3.4 **IA Control**: ECSC-1	Required: EI Conditional: SS, NA **Origin:** RFC 3315	1. Complete a configuration change to the DHCP server to ensure that it will send out a reconfigure message to the system under test. 2. Ensure that once the client receives the reconfigure message that the message is logged. 3. Confirm the logging of the reconfigure message by the client.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
21	**Section:** DHCP **ID:** 10.3 If the system supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC systems and log the event. NOTE: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication. **Reference:** UCR 2008 5.3.5.3.4 **IA Control:** DCBP-1 and ECSC-1	Conditional: SS, NA, EI, R, LS **Origin:** RFC 3315	1. Send out an Advertise message from the DHCP server without authentication information included. 2. Ensure that the system under test receives the message and discards the message due to it being unauthenticated. 3. Confirm the logging of the unauthenticated advertise message by the client.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
22	**Section:** Neighbor Discovery **ID:** 11 The system shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (FY2010). **Reference:** UCR 2008 5.3.5.3.5 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4861	1. Connect the system under test to a properly configured test network. 2. Once the system is connected to the network view traffic from the host to ensure that it properly attempts to use the proper protocols for Neighbor Discovery defined in RFC 2461. (e.g. *Router Discovery* to locate routers on their local network, *Parameter Discovery* to determine link parameters such as the link MTU, also *Duplicate Address Detection* to determine that an address the host wishes to use is not already in use.)	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
23	**Section:** Neighbor Discovery **ID:** 11.1 The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. **Reference:** UCR 2008 5.3.5.3.5 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS **Origin:** RFC 4861	1. Attempt to send a neighbor advertisement message from the host. (e.g. *Neighbor Solicitation*: Sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address. Neighbor Solicitations are also used for Duplicate Address Detection. *Anycast addresses:* Anycast addresses identify one of a set of nodes providing an equivalent service, and multiple nodes on the same link may be configured to recognize the same anycast address. Neighbor Discovery handles anycasts by having nodes expect to receive multiple Neighbor Advertisements for the same target. All advertisements for anycast addresses are tagged as being non-Override advertisements. A non-Override advertisement is one that does not update or replace the information sent by another advertisement. *Proxy advertisements*: A node willing to accept packets on behalf of a target address that is unable to respond to Neighbor Solicitations can issue non-Override Neighbor Advertisements. Proxy advertisements are used by Mobile IPv6 Home Agents to defend mobile nodes' addresses when they move off-link. However, it is not intended as a general mechanism to handle nodes that, e.g., do not implement this protocol.) 2. Ensure that the override flag bit is not set in the advertisement message which in turn does not overwrite previous information identified in past messages.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
24	**Section:** Neighbor Discovery **ID:** 11.2 The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. **Reference:** UCR 2008 5.3.5.3.5 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS **Origin:** RFC 4861	1. Attempt to send a Neighbor Advertisement message by the host to a specified target system that sends a Neighbor Solicitation message to start the communication process. 2. In response to the Neighbor Solicitation message the system under test will set the override flag bit to "1" in the Neighbor Advertisement message sent back to the target address. (Proper setting of the Override flag ensures that nodes give preference to non-proxy advertisements, even when received after proxy advertisements, and also ensures that the first advertisement for an anycast address "wins".)	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
25	**Section:** Neighbor Discovery **ID:** 11.3 If a valid neighbor advertisement is received by the system and the system neighbor cache does not contain the target's entry, the advertisement shall be silently discarded. **Reference:** UCR 2008 5.3.5.3.5 **IA Control:** ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4861	1. Attempt to send a Neighbor Advertisement message to the system under test with a preconfigured test client on the network in which the system under test will not have the address for the client in its neighbor cache which is used to inform the system of neighbors on the network in which traffic has been initiated with. 2. Verify that when the system under test receives the neighbor advertisement from the client the advertisement is discarded.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
26	**Section:** Neighbor Discovery **ID:** 11.4 If a valid neighbor advertisement is received by the system and the system neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the system shall silently discard the received advertisement. **Reference:** UCR 2008 5.3.5.3.5 **IA Control**: ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4861	1. Attempt to send a Neighbor Advertisement message to the system under test when its neighbor cache is an INCOMPLETE state. (i.e. INCOMPLETE: Address resolution is in progress and the link-layer address of the neighbor has not yet been determined.) 2. Verify that when the system under test receives the neighbor advertisement while in INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included that the message is discarded.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
27	**Section:** Neighbor Discovery **ID:** 11.5 If address resolution fails on a neighboring address, the entry shall be deleted from the system's neighbor cache. **Reference:** UCR 2008 5.3.5.3.5 **IA Control:** ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4861	1. Initiate address resolution for a neighboring address on the network. 2. Ensure that the system under test creates an entry in the INCOMPLETE state and initiates the address resolution process. 3. Verify that the address resolution process fails and that the entry for the client is deleted from the system's neighbor cache. (i.e. The entry is deleted so that subsequent traffic to that neighbor invokes the next-hop determination procedure once again to allow for the system to attempt to find an alternate route to communicate with the host.)	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
28	**Section:** Redirect Messages **ID:** 11.6 The system shall support the ability to configure the system to ignore redirect messages. **Reference:** UCR 2008 5.3.5.3.5.1 **IA Control**: ECSC-1	Required: SS, NA, EBC, EI **Origin:** RFC 4890	1. Configure the system under test to ignore redirect message. 2. Generate a redirect message from a router on the test network to inform the system under test of an alternate route to take for traffic. 3. Verify that the system receives the redirect message from the router and that the system ignores the message.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
29	**Section:** Redirect Messages **ID:** 11.7 The system shall only accept redirect messages from the same router as is currently being used for that destination. NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a redirect message from router X for packets destined for location A to be sent to router Z. **Reference:** UCR 2008 5.3.5.3.5.1 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 2461	1. Attempt to send a packet from the system under test to a pre-determined router configured on the test network. 2. Then attempt to send a redirect message to the system from a different router on the test network in which the original packet generated must travel through to reach its destination. 3. Verify that the system receives the redirect message from the router and that the system ignores the message.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
30	**Section:** Redirect Messages **ID:** 11.7.1 If redirect messages are allowed, the system shall update its destination cache in accordance with the validated redirect message. **Reference:** UCR 2008 5.3.5.3.5.1 **IA Control**: ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 2461	1. Attempt to send a packet from the system under test to a pre-determined router configured on the test network. 2. Attempt to send a redirect message from the router on the test network in which the system is using to relay its packet to the destination. 3. Verify that the system receives the validated redirect message (per Section 8.1 RFC 4861) from the router and that the system updates its destination cache for future traffic.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
31	**Section:** Redirect Messages **ID:** 11.7.2 If the valid redirect message is allowed and no entry exists in the destination cache, the system shall create an entry. **Reference:** UCR 2008 5.3.5.3.5.1 **IA Control:** ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 2461	1. Send the system under test a valid redirect message from a router set to process traffic for the host in which the redirect message contains a new address for which the system is unaware of. 2. Verify that when the system receives the redirect message that it updates its destination cache to include the new address contained in the redirect message.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
32	**Section:** Router Advertisements **ID:** 11.8 If the system sends router advertisements, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements. **Reference:** UCR 2008 5.3.5.3.5.2 **IA Control**: ECSC-1	Required: R Conditional: LS, EBC **Origin:** RFC 4861	1. Configure a router on the test network to send out an inconsistent router advertisement to the system under test. (i.e. Information to determine what makes a router advertisement a valid advertisement can be found in section 6.2.7. Router Advertisement Consistency of RFC 4861.) 2. Ensure that when the system receives the router advertisement it attempts to validate it and when it fails that the inconsistent router advertisement is logged.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
33	**Section:** Router Advertisements **ID:** 11.8.1 The system shall prefer routers that are reachable over routers whose reachability is suspect or unknown. **Reference:** UCR 2008 5.3.5.3.5.2 **IA Control:** ECSC-1	Required: SS, NA, EBC, EI **Origin:** RFC 4861	1. Configure the system under test to send out packets through neighboring routers. 2. On the closest router to the system for the test ensure that the connection is unreliable for the system under test. 3. On the next router on the network verify that it has a good connection to send traffic on. 4. Send out a packet to a destination on the network and verify the system attempts to reference a previous reachability confirmation to send the packet through the router that it knows is accessible and that it does not attempt to first send the packet through the router on the network configured with an unreliable connection.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
34	**Section:** Router Advertisements **ID:** 11.9 If the system sends router advertisements, the system shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861 (FY2010). **Reference:** UCR 2008 5.3.5.3.5.2 **IA Control**: ECSC-1	Required: R Conditional: LS, EBC **Origin:** RFC 4861	1. Attempt to send a router advertisement message with the system under test. 2. Verify that the router advertisement message contains the MTU value for that link. (i.e. MTU values should be included in router advertisements to verify that they are in fact valid advertisements. Information used to determine that a router advertisement is in fact valid can be found in section 6.2.7 Router Advertisement Consistency in RFC 4861.)	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
35	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12 If the system supports stateless IP address autoconfiguration, the system shall support IPv6 Stateless Address Auto-Configuration (SLAAC) for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (FY2010). **Reference:** UCR 2008 5.3.5.3.6 **IA Control:** ECSC-1	Required: R, LS, EI (Softphone only) Conditional: SS, NA, EBC, EI **Origin:** RFC 4862	1. Connect the system under test to the test network without an address specified for the specific interface. 2. Once connected to the network verify that the system begins the auto-configuration process by generating a link-local address for the interface. 3. The system will then attempt to send out a Neighbor Solicitation message to ensure that the address for the interface is not already in use on the network. 4. Next ensure the system attempts to receive a router advertisement message to determine what routers if any are available on the network.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
36	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.1 The system shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration. NOTE: The objective of this requirement is to prevent a system from using stateless auto configuration. **Reference:** UCR 2008 5.3.5.3.6	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system is configurable to have the "managed address configuration" flag and the "other stateful configuration" flag to always be set (i.e. A "managed address configuration" flag indicates whether hosts should use stateful autoconfiguration to obtain addresses. An "other stateful configuration" flag indicates whether hosts should use stateful autoconfiguration to obtain additional information (excluding addresses.) 2. Configure the flags to be set to prevent stateless auto-configuration. 3. Connect the system to the network and verify that it does not attempt to start the stateless auto-configuration process as defined in Section 4 of RFC 2462.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
37	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.2 The system shall support manual assignment of IPv6 addresses. **Reference:** UCR 2008 5.3.5.3.6	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system under test is capable of being configured to allow for the manual input of an IPv6 address. 2. Assign an address to the system that will allow for it to communicate on a test network. 3. Connect the system to the network and verify connectivity of the system.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
38	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.3 The system shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE). NOTE: This requirement is associated with the earlier requirement for the EI to support DHCPv6. **Reference:** UCR 2008 5.3.5.3.6	Required: EI	1. Configure the system under test to have the ManagedFlag value set to TRUE. (The Default setting for the ManagedFlag value on a system is set to FALSE.) 2. Connect the system to the network and verify that it does not attempts to start the stateless auto-configuration process, as stateful auto-configuration is used to assign an address manually to the system	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
39	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.3.1 If the system sends router advertisements, the system shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented. **Reference:** UCR 2008 5.3.5.3.6 **IA Control:** ECSC-1	Required: R Conditional: LS, EBC **Origin:** RFC 2462	1. Verify that the system under test is configurable to allow for the "managed address configuration" flag and the "other stateful flag" to be set to TRUE 2. Attempt to send out a router advertisement from the system under test to a target host on the network. 3. Verify that the router advertisement contains the "managed address configuration" flag and the "other stateful flag" set to TRUE. (i.e. In addition, when the value of the ManagedFlag is TRUE, the value of OtherConfigFlag is implicitly TRUE as well. It is not a valid configuration for a host to use stateful address autoconfiguration to request addresses only, without also accepting other configuration information.)	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
40	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.4 If the system supports a subtended appliance behind it, the system shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the system and does not cause the system to attempt to change its IP address. NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address. **Reference:** UCR 2008 5.3.5.3.6 **IA Control**: ECSC-1	Conditional: EI **Origin:** RFC 3756	1. Configure a phone system on the test network with a hub or switch interface in which the system may connect to the network through. 2. Connect the system to the switch interface of the phone system on the test network. 3. Verify the system is able to obtain an IP address on the network to allow for connectivity. 4. Once the system has obtained its IP address and it is capable of communicating on the network ensure that the configuration of the phone system is unchanged and that it retained it's original IP address.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
41	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.5 If the system supports IPv6 SLAAC, the system shall have a configurable parameter that allows the function to be enabled and disabled. **Reference:** UCR 2008 5.3.5.3.6	Conditional: SS, NA, EBC, EI	1. Verify that the system under test is configurable to allow for the SLAAC to be enabled or disabled. (e.g. Per RFC 2462 Hosts maintain the following variables on a per-interface basis: ManagedFlag: Copied from the M flag field (i.e., the "managed address configuration" flag) of the most recently received Router Advertisement message. The flag indicates whether or not addresses are to be configured using the stateful autoconfiguration mechanism. It starts out in a FALSE state. OtherConfigFlag: Copied from the O flag field (i.e., the "other stateful configuration" flag) of the most recently received Router Advertisement message. The flag indicates whether or not information other than addresses is to be obtained using the stateful autoconfiguration mechanism. It starts out in a FALSE state. In addition, when the value of the ManagedFlag is TRUE, the value of OtherConfigFlag is implicitly TRUE as well. It is not a valid configuration for a host to use stateful address autoconfiguration to request addresses only, without also accepting other configuration information.) 2. Enable SLAAC on the system and connect it to the network and ensure that it begins the stateless auto-configuration process. 3. Disable SLAAC on the system and connect it to the network and ensure that it does not begin the stateless auto-configuration process.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
42	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.6 If the system supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPsec capable systems shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6. **Reference:** UCR 2008 5.3.5.3.6	Conditional: EI (Softphones only)	1. Configure the system under test to allow the use of IPsec and to . 2. Connect the system to the test network and verify that it attempts to create a new randomized interface identifier. (i.e. A new interface identifier can be created by a few different methods which are explained in Section 3 of RFC 4941.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4941			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
43	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.7 If the system supports stateless IP address autoconfiguration, the system shall support a configurable parameter to enable or disable manual configuration of the site-local and Global addresses (i.e., disable the "Creation of Global and Site-Local Addresses" as described in Section 5.5 of RFC 2462). **Reference:** UCR 2008 5.3.5.3.6	Required: R, LS, EI (Softphone only) Conditional: SS, NA, EBC, EI	1. Verify that the system under test is configurable for the enabling and or disabling of manual configuration of site-local and Global addresses. 2. Configure the system under test with a site-local address and attempt to have a host in a separate network reach the system in the test network 3. Verify that the system with the site-local address is unreachable from the host on a separate network. 4. Configure the system under test with a Global routing prefix and attempt to have a host in a separate network reach the system in the test network 5. Verify that the system with the Global routing prefix is reachable by the host on a separate network.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2462			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
44	**Section:** Stateless Address Autoconfiguration and Manual Address Assignment **ID:** 12.8 All IPv6 nodes shall support link-local address configuration, and the Duplicate Address Detection (DAD) shall not be disabled in accordance with RFC 2462 and RFC 4862 (FY2010). **Reference:** UCR 2008 5.3.5.3.6	Required: SS, NA, EBC, R, LS, EI	1. Attempt to connect the system under test to the test network. 2. Verify that the system attempts to assign a link-local address to its interface. 3. Once the system attempts to assign a link-local address verify that it attempts to perform Duplicate Address Detection to ensure that it is not using an address that is already assigned to a separate host on the network.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4862			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
45	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14 The system shall support the Internet Control Message Protocol for IPv6 (ICMPv6) as described in RFC 4443. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Conduct an analysis of the system configuration. 2. Verify that ICMPv6 is implemented as the IPv6 messaging protocol. 3. Ensure that the protocol is configured properly per Section 2 of RFC 4443.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
46	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.1 The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Confirm that the system is capable of configuring rate limiting. 2. Verify that you have the ability to set the parameter for rate limiting to a desired rate. 3. After you have configured rate limiting to a determined rate generate ICMP traffic that would surpass the rate limiting parameter you previously configured and ensure that the traffic is either dropped or delayed on that interface.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
47	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.2 The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable Destination Unreachable Messages. 3. Configure a host on the test network to not allow ICMP traffic through a firewall. 4. Verify that the system has the ability to generate the Destination Unreachable message. 5. Send an ICMP packet to the system setup to not allow ICMP traffic and ensure that a Destination Unreachable message is returned.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
48	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.3 The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast/anycast address. NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable Echo Reply Messages. 3. Verify that the system tested first has Echo Reply disabled then send an Echo Request from a host on the test network and ensure that no Echo Reply is received. 4. Verify that the system tested has Echo Reply enabled then send an Echo Request from a host on the test network and ensure that an Echo Reply is received.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
49	**Section:** Internet Control Message Protocol (ICMP) **ID:** 14.4 The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. **Reference:** UCR 2008 5.3.5.3.7	Required: SS, NA, EBC, R, LS, EI	1. Configure an ICMP message with information contained in the payload of the message. 2. As the ICMP message is sent from the host intercept the message from another system on the test network and attempt to perform a change to the information contained in the payload of the ICMP message. 3. Verify that the system tested attempts to validate the ICMP before acting on the information contained in the payload.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4443			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
50	**Section:** Routing Functions **ID:** 15 If the system supports routing functions, the system shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 2740. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Conduct an analysis of the system configuration and verify the router configuration. 2. Verify that routing functions are configured to support the OSPF for IPv6 methodologies.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2740			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
51	**Section:** Routing Functions **ID:** 15.1 If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Verify that routing functions are configured to support the OSPF for IPv6 methodologies. 2. Analyze network traffic to determine if IPSec is used to secure the routing functions.	CAT II	
	IA Control: ECSC-1	**Origin:** UCR 2008, Section 5.4, Information Assurance			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
52	**Section:** Routing Functions **ID:** 15.2 If the system supports routing functions, the system shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-128 as described in RFC 4302. **Reference:** UCR 2008 5.3.5.3.8	Required: R Conditional: LS	1. Examine the system configuration and verify that routing functions are supported. 2. Ensure that router-to-router communications are secured by using the IP Authentication Header with HMAC-SHA1-128 encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4302			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
53	**Section:** Routing Functions **ID:** 16 If the system acts as a CE router, the system shall support the use of Border Gateway Protocol (BGP) as described in RFC 1772 and 4271 **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. Inspect the system under test to verify its use as a Customer Edge Router. 2. Ensure that another router setup on a test network is able to communicate to the system under test. 3. Generate traffic on the test network where the system under test would need to update its routing tables. 4. Ensure that when the router on a separate test network attempts to communicate with the system under test that it is able to exchange its routing information per RFC 4271.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4271			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
54	**Section:** Routing Functions **ID:** 16.1 If the system acts as a customer edge router, the system shall support the use of BGP-4 multiprotocol extensions for IPv6 Inter-Domain routing (RFC 2545). NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. Configure the test network for IPv6 communication. 2. Ensure that the system under test supports BGP-4 per RFC 2545 and allows for Inter Domain Routing for IPv6. (i.e. In terms of routing information, the most significant difference between IPv6 and IPv4 (for which BGP was originally designed) is the fact that IPv6 introduces scoped unicast addresses and defines particular situations when a particular address scope must be used.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2545			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
55	**Section:** Routing Functions **ID:** 17 If the system acts as a CE router, the system shall support multiprotocol extensions for BGP-4 RFC 2858 and RFC 4760 (FY2010). NOTE: The requirement to support BGP-4 is in UCR 2008, Section 5.3.3, Wide Area Network General System Requirements **Reference:** UCR 2008 5.3.5.3.8	Conditional: R, LS	1. Verify that the CE router allows for support of BGP-4. 2. Document the use of the NEXT_HOP attribute and also the use of Network Layer Reachability Information for its support of IPv4 and IPv6.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4760			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
56	**Section:** Routing Functions **ID:** 18 If the system acts as a CE router, the system shall support the Generic Routing Encapsulation (GRE) as described in RFC 2784. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. The system under test should allow for the support of Generic Routing Encapsulation per RFC 2784. 2. Ensure that you have the ability to create a tunnel between the system under test and another router configured. 3. Make sure that the traffic between the two routers is being encapsulated and that the routers are able to properly communicate.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2784			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
57	**Section:** Routing Functions **ID:** 19 If the system acts as a CE router, the system shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473. NOTE: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture. **Reference:** UCR 2008 5.3.5.3.8	Conditional: R	1. The system shall allow the ability for the tunneling between two nodes on the network. 2. Attempt to create a tunnel between two nodes to communicate on the network. 3. Once the tunnel has been established verify that the two nodes do not have any issues with communication. 4. Analyze the network traffic and verify that it is being encapsulated and decapsulated by the nodes on the tunnel.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2473			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
58	**Section:** Routing Functions **ID:** 20 If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. NOTE: The FY 2008 VVoIP design does not utilize multicast, but routers supporting VVoIP also support data applications that may utilize multicast. A softphone will have non-routing functions that require MLDv2. **Reference:** UCR 2008 5.3.5.3.8	Required: R, EI (Softphone) Conditional: LS	1. Conduct an analysis of the systems configuration and verify that it supports Multicast Listener Discovery. 2. Make certain that the system under test has the ability to discover multicast listeners on directly attached links. 3. Verify that the system has the ability to discover multicast addresses which are of interest to neighboring nodes. 4. If MLDv2 is supported MLDv2 provides for source filtering to allow nodes to listening to packets only from specific sources.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3810			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
59	**Section:** Routing Functions **ID:** 21 The system shall support MLD as described in RFC 2710. NOTE: This requirement was added in order to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement. **Reference:** UCR 2008 5.3.5.3.8	Required: SS, NA, EBC, EI, LS	1. Conduct an analysis of the systems configuration and verify that it supports Multicast Listener Discovery. 2. Make certain that the system under test has the ability to discover multicast listeners on directly attached links. 3. Verify that the system has the ability to discover multicast addresses which are of interest to neighboring nodes.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2710			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
60	**Section:** IP Security **ID:** 22 If the system uses IPSec, the system shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (FY2010). In FY2008, RFC 2401 (and its related RFCs) is the Threshold requirement as described in UCR 2008, Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that the system supports the use of IPSec. 2. Ensure that the system has the ability to communicate with another host on the network with IPSec in use. 3. Analyze the network traffic to ensure communication between the hosts is encrypted and that both hosts are communicating properly according to RFC 2401 and RFC 4301.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
61	**Section:** IP Security **ID:** 22.1 If RFC 4301 is supported, the system shall support binding of a security association (SA) with a particular context. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Certify that IPSec is currently in use by the system. 2. Configure the system under test to allow for the ability to bind separate security associations on the test network to a particular context. (e.g. A security gateway that provides VPN service to multiple customers will be able to associate each customer's traffic with the correct VPN.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
62	**Section:** IP Security **ID:** 22.2 If RFC 4301 is supported, the system shall be capable of disabling the BYPASS IPSec processing choice. NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that IPSec is in use by the system. 2. Ensure that the system does not have the ability to enable the BYPASS IPSec option for the Security Policy Database. 3. Attempt to set the process choice of BYPASS IPSec in the Security Policy Database and verify that you are unable to do so.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
63	**Section:** IP Security **ID:** 22.3 If RFC 4301 is supported, the system shall not support the mixing of IPv4 and IPv6 in a security association. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Create a security association between the system under test and a separate host. 2. Attempt to communicate in the Security Association with IPv6 traffic and verify that a connection is made correctly. Also attempt to communicate with IPv4 traffic and verify that a connection is made correctly. 3. Verify that the security association does not provide the ability to use both IPv4 and IPv6 traffic on a single security association.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
64	**Section:** IP Security **ID:** 22.4 If RFC 4301 is supported, the system's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario where this could occur. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Ensure that the Security Association Database has the ability to create a separate entry for each host in a specific security association. 2. Verify the systems ability to create a unique entry for each host in a security association. (i.e. This may be done through a unique identifier for each system on the network) (Section 4.4.2 per RFC 4301 explains the situation where a SAD entry could be associated with multiple SA's: For instance, two hosts behind the same NAT could choose the same SPI value. The situation also may arise if a host is assigned an IP address (e.g., via DHCP) previously used by some other host, and the SAs associated with the old host have not yet been deleted via dead peer detection mechanisms. This may lead to packets being sent over the wrong SA or, if key management ensures the pair is unique, denying the creation of otherwise valid SAs. Thus, implementors should implement links between the SPD cache and the SAD in a way that does not engender such problems.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
65	**Section:** IP Security **ID:** 22.5 If RFC 4301 is supported, the system shall be capable of correlating the Differentiated Services Code Point (DSCP) for a VVoIP stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. For a more detailed description of the requirement, please see Section 4-1 of RFC 4301 - Security Architecture for the Internet Protocol. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Prepare the system under test to process traffic for a number of different security associations that are configured. 2. Verify that the system has the ability to properly correlate the DSCP values on packets and route those packets to the appropriate security association mapped to that DSCP value of the traffic.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
66	**Section:** IP Security **ID:** 22.6 If RFC 4301 is supported, the system shall implement IPSec to operate with both integrity and confidentiality. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify the system has the ability to operate IPSec with integrity and confidentiality. 2. Integrity and Confidentiality in IPSec is completed through the use of the IP Authentication Header and the Encapsulating Security Payload.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
67	**Section:** IP Security **ID:** 22.7 If RFC 4301 is supported, the system shall be capable of enabling and disabling the ability of the system to send an ICMP message informing the sender that an outbound packet was discarded. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Confirm that ICMPv6 is in use on the system under test. 2. Certify that the system has the ability to enable and disable ICMP error messages such as that of an ICMP PMTU error message. 3. Send an ICMP packet outbound that will be discarded; For example sending a packet larger than that of a security associations PMTU in which fragmentation is not enabled. 4. Verify that if the ability to send an ICMP error message is enabled the system sends out an ICMP error message, also verify that if the ability to send an ICMP error message is disabled the system does not send out an ICMP error message.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
68	**Section:** IP Security **ID:** 22.7.1 If an ICMP outbound packet message is allowed, the system shall be capable of rate limiting the transmission of ICMP responses **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4301	1. Confirm that the system is capable of configuring rate limiting. 2. Verify that you have the ability to set the parameter for rate limiting to a desired rate. 3. After you have configured rate limiting to a determined rate Attempt to spoof a system on the network with a source address already in use, then send out packets to another system on the network to elicit it to send ICMP packets to the original system in which you spoofed its source address. 4. Ensure that with rate limiting set that the system in which you spoofed on the network only receives a limited amount of ICMP packets before they are discarded or delayed.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
69	**Section:** IP Security **ID:** 22.8 If RFC 4301 is supported, the system shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4301	1. Ensure that the system has the ability to enable and disable Explicit Congestion Notification bits. 2. Next Generate a large amount of traffic on the network in which without Explicit Congestion Notification enabled the packets directed at a particular host would be discarded due to the high volume of traffic. 3. Now with Explicit Congestion Notification enabled attempt to create that large amount of traffic to communicate with a specific host, verify that the packets are not discarded, but are labeled with the Explicit Congestion Notification bits to allow the continuous communication between the sources.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
70	**Section:** IP Security **ID:** 22.9 If RFC 4301 is supported, the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4301	1. View the Security Policy Database for the IPSec Implementation. 2. Ensure that the final entry in the Security Policy Database is set to discard any traffic that is not already identified as being mapped to the Security Policy Database to specify secure communications.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
71	**Section:** IP Security **ID:** 22.10 If RFC 4301 is supported, and the system receives a packet that does not match any SPD cache entries and the system determines it should be discarded, the system shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Attempt to communicate through a security association with a separate host by means of which you have set to not allow in the Security Policy Database. 2. Verify that the packet is discarded and that the system logs the event and includes the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
72	**Section:** IP Security **ID:** 22.11 If RFC 4301 is supported, the system should include a management control to allow an administrator to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of an INVALID_SELECTORS. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Verify that the system is capable of enabling and disabling the sending of an Internet Key Exchange notification of INVALID_SELECTORS. 2. Establish communication through a security association with a designated host. 3. Send a packet inbound on the SA in which the packets headers are inconsistent with the selectors on the SA. 4. Verify that if the system has the ability to send an IKE notification of INVALID_SELECTORS enabled that the system receives a packet indicating that the message sent was discarded due to failure to pass selector checks. If the system has the ability to send an IKE notification of INVALID_SELECTORS disabled ensure that the system does not receive a packet indicating that the message sent was discarded due to failure to pass selector checks.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
73	**Section:** IP Security **ID:** 22.12 If RFC 4301 is supported, the system shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. The Encapsulating Security Payload is used to provide for Integrity, data origin authentication, and confidentiality in IPv4 and IPv6 environments. 2. Verify that ESP is being used by the system per RFC 4303 to provide secure communication.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4303			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
74	**Section:** IP Security **ID:** 22.12.1 If RFC 4303 is supported, the system shall be capable of enabling anti-replay. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4303	1. Ensure that the system supports Encapsulating Security Payload which provides anti-replay features for Security Associations. 2. Verify that the integrity feature is enabled for ESP as the anti-replay feature can not be enabled with out the integrity feature of ESP, because without the integrity service available the Sequence number field which is used to protect against anti-replay can not be checked for integrity. 3. Analyze network traffic sent from the security association and verify that the anti-replay service is in use.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
75	**Section:** IP Security **ID:** 22.12.2 If RFC 4303 is supported, the system shall check as its first check after a packet has been matched to its SA whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the sec **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4303	1. Create a Security Association between two hosts on the test network. 2. After the SA has been created begin to generate traffic between the two hosts. 3. Verify that with each packet generated between the hosts that the counter for each packet is incremented. 4. If a sequence number between the hosts is duplicated it is an auditable event and the system will audit the event in its event log.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
76	**Section:** IP Security **ID:** 22.13 If RFC 4301 is supported, the system shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI **Origin:** RFC 4308	1. Verify the system is capable of supporting the cryptographic algorithms for Suite VPN-B from RFC 4308. IPsec: Protocol: ESP ESP encryption: AES with 128-bit keys in CBC mode [AES-CBC] ESP integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] IKE and IKEv2: Encryption: AES with 128-bit keys in CBC mode [AES-CBC] Pseudo-random function: AES-XCBC-PRF-128 [AES-XCBC-PRF-128] Integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] Diffie-Hellman group: 2048-bit MODP	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
77	**Section:** IP Security **ID:** 22.13.1 If RFC 4301 is supported, the system shall support the use of AES-CBC with 128-bits keys for encryption. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Ensure the system is capable of supporting AES-CBC with 128-bit key for encryption. 2. Analyze network traffic between the system under test and a predetermined host to certify that it is using 128-bit encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
78	**Section:** IP Security **ID:** 22.13.2 If RFC 4301 is supported, the system shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 (FY2010). **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Confirm the test system is capable of supporting HMAC-SHA1-96 and AES-XCBC-MAC-96 for encryption. 2. Examine traffic between the system tested and another host on the network to confirm that HMAC-SHA1-96 and AES-XBC-MAC-96 is utilized for encryption.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
79	**Section:** IP Security **ID:** 22.14 If RFC 4301 is supported, the system shall support IKE Version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE Version 2 (IKEv2) (FY2010) as defined in RFC 4306. NOTE: Internet Key Exchange version 1 (IKEv1) requirements are found in UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.9	Required: R, EI (Softphone) Conditional: SS, NA, EBC, LS, EI	1. Create a Security Association between the system tested and another host on the test network. 2. Once the security association has been created begin to generate traffic between the hosts on the encrypted tunnel. 3. Verify that the request and response is created for the security association utilizing IKE and that the communication between the two hosts is encrypted properly. 4. The system must be capable of utilizing IKE and IKEv2 for secure communication.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
80	**Section:** IP Security **ID:** 22.14.1 If the system supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size. **Reference:** UCR 2008 5.3.5.3.9	Conditional: SS, NA, EBC, R, LS, EI	1. Confirm that the system is capable of supporting IKEv2. 2. Once you have verified that IKEv2 is utilized ensure that is capable of configuring UDP message size used for IKEv2. (i.e Although IKEv2 messages are intended to be short, they contain structures with no hard upper bound on size (in particular, X.509 certificates), and IKEv2 itself does not have a mechanism for fragmenting large messages. IP defines a mechanism for fragmentation of oversize UDP messages, but implementations vary in the maximum message size supported. Furthermore, use of IP fragmentation opens an implementation to denial of service attacks [KPS03]. Finally, some NAT and/or firewall implementations may block IP fragments. All IKEv2 implementations MUST be able to send, receive, and process IKE messages that are up to 1280 bytes long, and they SHOULD be able to send, receive, and process messages that are up to 3000 bytes long. IKEv2 implementations SHOULD be aware of the maximum UDP message size supported and MAY shorten messages by leaving out some certificates or cryptographic suite proposals if that will keep messages below the maximum. Use of the "Hash and URL" formats rather than including certificates in exchanges where possible can avoid most problems. Implementations and configuration should keep in mind, however, that if the URL lookups are possible only after the IPsec SA is established, recursion issues could prevent this technique from working.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
81	**Section:** IP Security **ID:** 22.14.2 If IKEv2 is supported, the system shall support the use of the ID_IPv6_ADDR and ID_IPV4_ADDR Identification Type. **Reference:** UCR 2008 5.3.5.3.9.22.14.2	Conditional: SS, NA, EBC, R, LS, EI	1. Check the system under test to ensure that it is capable of supporting IKEv2. 2. Verify that the system is able to process both IPv4 and IPv6 addresses. 3. The ID_IPv6_ADDR and ID_IPv4_ADDR fields will be defined in the payload of the IKEv2 messages.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
82	**Section:** IP Security **ID:** 22.14.3 If the system supports IKEv2, the system shall be capable of ignoring subsequent SA setup response messages after the receipt of a valid response. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Validate that the system tested has the ability to support IKEv2. 2. Certify that the system tested can create a security association between itself and another host. 3. Verify that the system receives a valid request and response to initially establish the security association. 4. Ensure that once the system has established the SA that any subsequent response messages pertaining to the request of the establishment of the SA is ignored rather than dropping the original security association and attempting to build a new one between the hosts.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
83	**Section:** IP Security **ID:** 22.14.4 If the system supports IKEv2, the system shall be capable of sending a Delete payload to the other end of the security association. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Verify that the system under test supports IKEv2 2. Create a security association between the test system and a separate host. 3. Confirm the ability of the system tested to send a delete payload to the other end of the security association to terminate the SA.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
84	**Section:** IP Security **ID:** 22.14.5 If the system supports IKEv2, the system shall reject initial IKE messages unless they contain a Notify payload of type COOKIE. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Conditional: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Ensure that the system tested is capable of using IKEv2 2. Attempt to send an initial IKE message to the system with a spoofed IP address and verify that the request is rejected. (e.g. An expected attack against IKE is state and CPU exhaustion, where the target is flooded with session initiation requests from forged IP addresses. This attack can be made less effective if a responder uses minimal CPU and commits no state to an SA until it knows the initiator can receive packets at the sending address. To accomplish this, a responder SHOULD -- when it detects a large number of half-open IKE_SAs -- reject initial IKE messages unless they contain a Notify payload of type COOKIE. It SHOULD instead send an unprotected IKE message as a response and include COOKIE Notify payload with the cookie data to be returned. Initiators who receive such responses MUST retry the IKE_SA_INIT with a Notify payload of type COOKIE containing the responder supplied cookie data as the first payload and all other payloads unchanged.)	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
85	**Section:** IP Security **ID:** 22.14.6 If the system supports IKEv2, the system shall close a SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA EBC,R, LS,EI	1. Configure the system tested and the remote host with a basic IPv6 configuration. 2. Configure IKEv2 on both the system tested and remote host. 3. Create a Security Association between the two hosts with a preset lifetime for the SA. 4. Ensure that when the Security Association is created there is no traffic generated between the two hosts for this scenario. 5. Validate that when the lifetime expires that the system tested attempts to create a new Security Association rather than attempting to rekey the current session.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
86	**Section:** IP Security **ID:** 22.14.7 If the system supports IKEv2, the system shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Configure IKEv2 on the system tested. 2. Confirm that the system tested does not use EAP to authenticate. 3. Attempt to initiate IKE authentication using EAP with the system tested by having an initiator attempt to connect to the system tested with the request with AUTH payload absent from the inquiry. 4. Verify that the system tested does not respond back with the EAP payload accepting the request.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
87	**Section:** IP Security **ID:** 22.14.8 If the system supports IKEv2, the system shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Attempt to send messages to the system tested with a separate host on UDP ports 500 and 4500. 2. The system shall not respond to a response message sent on UDP ports 500 and 4500 and must also audit the event. 3. The system may respond to a request message on these ports, if a response is sent it must be sent to the IP address and port from whence it came with the same IKE SPIs and the Message ID copied. The response MUST NOT be cryptographically protected and must contain a Notify payload indicating INVALID_IKE_SPI. 4. A node SHOULD treat such a message (and also a network message like ICMP destination unreachable) as a hint that there might be problems with SAs to that IP address and SHOULD initiate a liveness test for any such IKE_SA.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4306			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
88	**Section:** IP Security **ID:** 22.14.9 If the system supports IKEv2, the system shall not support temporary IP addresses or respond to such requests. **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4306	1. Create a security association with the system tested with the need of having the IP address of the system dynamically assigned to the system. 2. Confirm that the system does not support the ability to create this security association with the temporary IP address. 3. Also confirm that the system tested does not allow the system on the other end of the SA to allow for having a dynamic IP address.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
89	**Section:** IP Security **ID:** 22.14.10 If the system supports IKEv2, the system shall support the IKEv2 cryptographic algorithms defined in RFC 4307. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4307	1. Verify that the system supports IKEv2. 2. The system shall support the following algorithms defined in Section 3 of RFC 4307. **Encryption Algorithms** ENCR_3DES ENCR_NULL ENCR_AES_CBC ENCR_AES_CTR **Random Generating Algorithms** PRF_HMAC_MD5 PRF_HMAC_SHA1 PRF_AES128_CBC **Integrity Algorithms** AUTH_HMAC_MD5_96 AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
90	**Section:** IP Security **ID:** 22.14.11 If the system supports IKEv2, the system shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (FY2010) **Reference:** UCR 2008 5.3.5.3.9 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4869	1. Confirm that the system has the ability to support IKEv2. 2. Verify the system is capable of supporting the cryptographic algorithms for Suite VPN-B from RFC 4308. IPsec: Protocol: ESP ESP encryption: AES with 128-bit keys in CBC mode [AES-CBC] ESP integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] IKE and IKEv2: Encryption: AES with 128-bit keys in CBC mode [AES-CBC] Pseudo-random function: AES-XCBC-PRF-128 [AES-XCBC-PRF-128] Integrity: AES-XCBC-MAC-96 [AES-XCBC-MAC] Diffie-Hellman group: 2048-bit MODP 3. Also verify the system is capable of supporting the additional cryptographic algorithms for Suite VPN-B from Section 3 of RFC 4869.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
91	**Section:** IP Security **ID:** 22.15 If RFC 4301 is supported, the system shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Confirm the system tested provides support for ISAKMP. 2. Attempt to create a security association between the system tested and a separate host and verify the use of ISAKMP to negotiate that SA. 3. Verify the creation of the security association with ISAKMP and also ensure the encryption schemes defined in RFC 2407 are utilized.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2407			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
92	**Section:** IP Security **ID:** 22.16 If RFC 4301 is supported, the system shall support the ISAKMP as defined in RFC 2408. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Confirm the system tested provides support for ISAKMP. 2. ISAKMP is used to define procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). ISAKMP also defines payloads for exchanging key generation and authentication data. 3. Verify the systems use of ISAKMP while attempting to create a security association between the system tested and a separate host.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2408			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
93	**Section:** IP Security **ID:** 22.17 If the system supports the IPsec Authentication Header Mode, the system shall support the IP Authentication Header (AH) as defined in RFC 4302. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Attempt to create a security association between the system tested and a separate host. 2. The system will need to support the authentication header which is used in secure communication between systems to provide connectionless integrity and data origin authentication, the authentication header also provides protection against replays. 3. Confirm its use by the system and analyze network traffic to see its use for outbound packets and the use of sequence numbering o the packets.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4302			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
94	**Section:** IP Security **ID:** 22.18 If RFC 4301 is supported, the system shall support manual keying of IPSec. **Reference:** UCR 2008 5.3.5.3.9	Required: SS, NA, EBC, R, LS, EI	1. Verify that the system under test has manual management techniques to employ statically configured, symmetric keys. 2. Verify the ability of the system to operate effectively after the manual keying.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4301			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
95	**Section:** IP Security **ID:** 22.19 If RFC 4301 is supported, the system shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (FY2010). **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4835 & RFC 4305	1. Verify that the system under test shall support the Encapsulating Security Payload and Authentication Header cryptographic algorithms which protect data sent being sent over a security association. 2. The cryptographic algorithms defined in RFC 4305 and RFC 4835 are as follows: **(ESP)** Requirement Algorithm ---------- ---------- **MUST** NULL **MUST** AES-CBC with 128-bit keys **MUST** TripleDES-CBC **SHOULD** AES-CTR **SHOULD NOT** DES-CBC **MUST** HMAC-SHA1-96 **SHOULD+** AES-XCBC-MAC-96 **MAY** NULL **MAY** HMAC-MD5-96 **(AH)** Requirement Algorithm ---------- ---------- **MUST** HMAC-SHA1-96 **SHOULD+** AES-XCBC-MAC-96 **MAY** HMAC-MD5-96	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
96	**Section:** IP Security **ID:** 22.21 If RFC 4301 is supported, the system shall support the IKEv1 security algorithms as defined in RFC 4109. **Reference:** UCR 2008 5.3.5.3.9 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4109	1. Check the system tested to confirm that it can support IKEv1. 2. The cryptographic algorithms defined in RFC 4109 are as follows: Requirement Algorithm ---------- ---------- **MAY** DES for Encryption **MUST** Triple DES for Encryption **SHOULD** AES-128 for Encryption **MAY** MD5 for Hashing and HMAC **MUST** SHA1 for Hashing and HMAC **MAY** Tiger for Hashing **SHOULD** AES-XCBC-MAC-96 for PRF **MUST** Preshared Secrets **SHOULD** RSA with signatures **MAY** DSA with Signatures **MAY** RSA for Encryption **MAY** D-H Group 1 (768) **MUST** D-H Group 2 (1024) **SHOULD** D-H Group 14 (2048) **MAY** D-H elliptical curves	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
97	**Section:** Network Management **ID:** 23 The system shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293. NOTE: The requirements to support SNMPv3 are found in UCR 2008, Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and UCR 2008, Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.10 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 4293	1. Verify the systems use of IPv6 and SNMP. 2. The system tested will need to conform to RFC 4293 for all of its MIBs for support of IPv6. 3. The changes defined in RFC 4293 for IPv6 are as follows: (There are several general classes of change that are required. -The first and most major change is that most of the previous objects have different object IDs and additional indexes to support the possibility of different address types. The general counters for IP and ICMP are examples of this. They have been moved to the ipSystemStatsTable and icmpMsgStatsTable, respectively. The second change is the extension of all address objects to allow for both IPv4 and IPv6 addresses and the addition of an address type object to specify what address type is in use. The third change is the addition of several new objects to the replacement for a previously existing table such as IpNetToPhysical. The fourth change is the addition of completely new tables such as ipIfStatsTable and ipDefaultRouterTable. The first is based on the previous statistics groups, while the second is completely new to this MIB.)	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
98	**Section:** Network Management **ID:** 23.1 If the system performs routing functions, the system shall support the SNMP management framework as described in RFC 3411. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: LS **Origin:** RFC 3411	1. Verify that the system under test will support SNMP management framework. 2. Ensure several (potentially many) nodes, each with an SNMP entity containing command responder and notification originator applications, which have access to management instrumentation (traditionally called agents). 3. Verify at least one SNMP entity containing command generator and/or notification receiver applications (traditionally called a manager) 5. Verify management protocol, used to convey management information between the SNMP entities.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
99	**Section:** Network Management **ID:** 23.2 If the system performs routing functions, the system shall support SNMP message processing and dispatching as described in RFC 3412. **Reference:** UCR 2008 5.3.5.3.10 **IA Control**: ECSC-1	Required: LS **Origin:** RFC 3412	1. Verify that the system currently supports SNMP. 2. The system that supports SNMP must follow RFC 3412 for message processing and dispatching of SNMP. 3. The dispatcher in SNMP sends and receives the messages in SNMP and also dispatches SNMP PDU's to SNMP applications. 4. The message processor is responsible for processing SNMP version-specific messages and coordinating the interaction with the security subsystem to ensure proper security is applied to the SNMP message being handled.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
100	**Section:** Network Management **ID:** 23.3 If the system performs routing functions, the system shall support the SNMP applications as described in RFC 3413. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: LS **Origin:** RFC 3413	1. Confirm that the system has the ability to supports SNMP applications defined in RFC 3413. 2. RFC 3413 currently defines the following five types of SNMP application in which the system tested will need to support. - Applications which initiate SNMP Read-Class, and/or Write-Class requests, called 'command generators.' - Applications which respond to SNMP Read-Class, and/or Write-Class requests, called 'command responders.' - Applications which generate SNMP Notification-Class PDUs, called 'notification originators.' - Applications which receive SNMP Notification-Class PDUs, called 'notification receivers.' - Applications which forward SNMP messages, called 'proxy forwarders.' 3. Verify that the system tested shows the ability to support each of these SNMP applications.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
101	**Section:** Network Management **ID:** 24 The system shall support the ICMPv6 MIBs as defined in RFC 4293. **Reference:** UCR 2008 5.3.5.3.10 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS **Origin:** RFC 4293	1. Confirm that the system tested if currently utilizing ICMPv6 MIBs. 2. The system is to support ICMPv6 MIBs defined in RFC 4022. 3. The system under test will need to support the addition of the ipSystemStatsTable and ipIfStatsTable tables which specify IP address type in order to separate information based on IP versions. 3. The system will also have the need to support tables, such as ipDefaultRouterTable, which may be useful on both IPv4 and IPv6 nodes and also ipv6RouterAdvertTable.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
102	**Section:** Network Management **ID:** 25 The system shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS **Origin:** RFC 4022	1. Confirm that the system tested is currently utilizing TCP MIB. 2. The system is to support TCP MIBs defined in RFC 4022. 3. TCP MIBs defined in RFC 4022 includes a group of scalars and two tables which are the following: The tcp group of scalars includes two sets of objects: -Parameters of a TCP protocol engine. These include parameters such as the retransmission algorithm in use (e.g., vanj [VANJ]) and the retransmission timeout values. -Statistics of a TCP protocol engine. These include counters for the number of active/passive opens, input/output segments, and errors. Discontinuities in the stats are identified identified via the sysUpTime object, defined in [RFC 3418]. -The tcpConnectionTable provides access to status information for all TCP connections handled by a TCP protocol engine. In addition, the table reports identification of the operating system level processes that handle the TCP connections. -The tcpListenerTable provides access to information about all TCP listening endpoints known by a TCP protocol engine. And as with the connection table, the tcpListenerTable also reports the identification of the operating system level processes that handle this listening TCP endpoint.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
103	**Section:** Network Management **ID:** 26 The system shall support the UDP MIBs as defined in RFC 4113. **Reference:** UCR 2008 5.3.5.3.10	Required: SS, NA, EBC, R, LS	1. Confirm that the system tested if currently utilizing UDP MIBs. 2. The system is to support UDP MIBs defined in RFC 4113. 3. UDP MIBs defined in RFC 4113 includes a group of scalars and one table which are the following: The current UDP-MIB consists of one table and a group of scalars: -The udp group of scalars reports parameters and statistics of a UDP protocol engine. Two scalars, udpHCInDatagrams and udpHCOutDatagrams, have been added to this group since the publication of RFC 2013 in order to provide high-capacity counters for fast networks. Discontinuities in the values of the counters in this group are indicated by discontinuities in the value of the sysUpTime object, which is defined in RFC 3418 -The udpEndpointTable provides access to status information for all UDP endpoints handled by a UDP protocol engine. The table provides for strictly listening endpoints, as with the historical udpTable, and also for "connected" UDP endpoints, which only accepts packets from a given remote system. It also reports identification of the operating system level processes that handle UDP connections. Addresses and ports of UDP endpoints in this table are represented using the InetAddressType, InetAddress, and InetPortNumber textual conventions defined in RFC 4001.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4113			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
104	**Section:** Network Management **ID:** 27 If the system performs routing functions, the system shall support IP tunnel MIBs as described in RFC 4087. **Reference:** UCR 2008 5.3.5.3.10	Required: LS	1. Ensure that the system tested can support IP tunnel MIBs. 2. The system is to support IP tunnel MIBs which are defined in RFC 4113. 3. IP tunnel MIBs defined in RFC 4087 includes two current tables. The current tables are: -The Tunnel Interface Table, containing information on the tunnels known to a router; and -The Tunnel Inet Config Table, which can be used for dynamic creation of tunnels, and also provides a mapping from endpoint addresses to the current interface index value.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4087			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
105	**Section:** Network Management **ID:** 28 If the system performs routing functions, the system shall support the IP Forwarding MIB as defined in RFC 4292. **Reference:** UCR 2008 5.3.5.3.10 **IA Control**: ECSC-1	Required: LS **Origin:** RFC 4292	1. Confirm that the system under test may process IP Forwarding MIBs. 2. The system is to support IP Forwarding MIBs which are defined in RFC 4292. 3. IP Forwarding MIBs defined in RFC 4292 includes one current table and two global objects: -The object inetCidrRouteNumber indicates the number of current routes. This is primarily to avoid having to read the table in order to determine this number. -The object inetCidrRouteDiscards counts the number of valid routes that were discarded from inetCidrRouteTable for any reason. This object replaces the ipRoutingDiscards and ipv6DiscardedRoutes objects. -The inetCidrRouteTable provides the ability to display IP version-independent multipath CIDR routes.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
106	**Section:** Network Management **ID:** 29 If the system supports mobile users, the system shall support the Mobile IP Management MIBs as described in RFC 4295. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: R, LS **Origin:** RFC 4295	1. Check the system being tested to verify that it may use Mobile IP Management MIBs. 2. The system is to support Mobile IP Management MIBs which are defined in RFC 4295. 3. Mobile IP Management MIBs defined in RFC 4295 includes: -It is assumed that the Mobile IPv6 Management Information Base (MOBILEIPV6-MIB) will always be implemented in conjunction with the IPv6-capable version of the IP-MIB. The MOBILEIPV6-MIB uses the textual conventions defined in the INET-ADDRESS-MIB. The Mobile-IPv6 MIB is composed of the following groups of definitions: - mip6Core: a generic group containing objects that are common to all the Mobile IPv6 entities. - mip6Ha: this group models the home agent service. It is composed of objects specific to the services and associated advertisement parameters offered by the home agent on each of its links. It also contains objects pertaining to the maintenance of the home agent list on each of the	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
106 (continued)			links on which the service is offered. - mip6Mn: this group models the mobile node service. It is composed of objects specific to the Dynamic Home Agent discovery function and related parameters. It also contains objects that record the movement of the mobile node. - mip6Cn: models the correspondent node and is primarily scoped to its participation in the Return Routability procedure for achieving Route Optimization triggered by the mobile node. - mip6Notifications: defines the set of notifications that will be used to asynchronously monitor the Mobile IPv6 entities. The tables contained in the above groups are as follows: -mip6BindingCacheTable: models the binding cache on the home agent and correspondent node. It contains details of the Binding Update requests that have been received and accepted. -mip6BindingHistoryTable: tracks the history of the binding cache. -mip6NodeTrafficTable: the mobile node-wise traffic counters. -mip6MnHomeAddressTable: contains all the home addresses pertaining to the mobile node and the corresponding registration status. -mip6MnBLTable: models the Binding Update List on the mobile node. It contains information about the registration requests sent by the mobile node and the corresponding results. -mip6CnCounterTable: contains the mobile node-wise registration statistics. -mip6HaConfTable: contains the configurable advertisement parameters for all the interfaces on which the home agent service is advertised. -mip6HaCounterTable: contains registration statistics for all mobile nodes registered with the home agent.		

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
106 (continued)			-mip6HaListTable: contains the list of all routers that are acting as home agents on each of the interfaces on which the home agent service is offered by this router. -mip6HaGlAddrTable: contains the global addresses of the home agents.		
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
107	**Section:** Network Management **ID:** 31 If the system supports SNMP and IPsec, the system shall support the IPsec security policy database as described in RFC 4807. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: LS **Origin:** RFC 4807	1. Confirm support for the Management Information Base (MIB) module for configuring the security policy database of a device implementing the IPsec protocol. 2. The system shall conform to the requirements listed in RFC 4807 for support of the IPSec security policy: (i.e. The Distributed Management Task Force (DMTF) has created an object oriented model of IPsec policy information known as the IPsec Policy Model White Paper [IPPMWP]. The "IPsec Configuration Policy Model" (IPCP) [RFC 3585] is based, in large part, on the DMTF's IPsec policy model and on RFC 2401. The IPCP document describes a model for configuring IPsec. This MIB module is a task-specific derivation (i.e., an SMIv2 instantiation) of the IPCP's IPsec configuration model for use with Simple Network Management Protocol version 3 (SNMPv3). The high-level areas where this MIB module diverges from the IPCP model are: -Policies, Groups, Conditions, and some levels of Actions are generically named. In other words, IPsec-specific prefixes like "SA" (Security Association), or "IPsec", are not used. This naming convention is used because packet classification and the matching of conditions to actions is more general than IPsec. The tables in this document can possibly be reused by other packet-transforming actions, which need to conditionally act on packets matching filters. -Filters are implemented in a more generic and scalable manner, rather than enforcing the condition/filtering pairing of the IPCP and its restrictions upon the user. This MIB module offers a compound filter object providing greater flexibility for complex filters than the IPCP.)	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
108	**Section:** Network Management **ID:** 32 If the system uses Uniform Resource Identifiers (URIs), the system shall use the URI syntax described in RFC 3986. **Reference:** UCR 2008 5.3.5.3.10 **IA Control**: ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 3986	1. Verify that the system uses Uniform Resource Identifiers for the identifying resources on the network which is essentially a resource locator. 2. The syntax for URI defined in RFC 3896 is as follows: The generic URI syntax consists of a hierarchical sequence of components referred to as the scheme, authority, path, query, and fragment. URI = scheme ":" hier-part ["?" query] ["#" fragment] hier-part = "//" authority path-abempty / path-absolute / path-rootless / path-empty	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
109	**Section:** Network Management **ID:** 33 If the system uses the Domain Name System (DNS), the system shall conform to RFC 3596 for DNS queries. NOTE: DNS is primarily used for NM applications. **Reference:** UCR 2008 5.3.5.3.10 **IA Control:** ECSC-1	Required: SS, NA, EBC, R, LS, EI **Origin:** RFC 3596	1. Confirm that the system is using Domain Name System for IPv6. 2. DNS is unable to support IPv6 addresses unless it conforms to the requirements in RFC 3596. (i.e. Current support for the storage of Internet addresses in the Domain Name System (DNS) cannot easily be extended to support IPv6 addresses since applications assume that address queries return 32-bit IPv4 addresses only. To support the storage of IPv6 addresses in the DNS, RFC 3596 defines the following extensions: -A resource record type is defined to map a domain name to an IPv6 address. -A domain is defined to support lookups based on address. -Existing queries that perform additional section processing to locate IPv4 addresses are redefined to perform additional section processing on both IPv4 and IPv6 addresses.)	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
110	**Section:** IP Version Negotiation **ID:** 37 The system shall forward packets using the same IP version as the version in the received packet. NOTE: If the packet was received as an IPv6 packet, the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur. REMINDER: This requirement may be waived from FY2008 to FY2012 in order to support IPv4 or IPv6 only EIs. **Reference:** UCR 2008 5.3.5.3.12	Required: SS, EBC	1. Send packets to the system under test with both an IPv4 and IPv6 system on the test network. 2. Verify that when the packets are received by the system tested from either the IPv4 or IPv6 system that the packet forwarded uses the same IP version as the packet that was received.	CAT II	
	IA Control: ECSC-1	**Origin:** Network STIG v7r1			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
111	**Section:** IP Version Negotiation **ID:** 38 The system shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual stacked appliances for AS-SIP signaled sessions. **Reference:** UCR 2008 5.3.5.3.12	Required: SS, NA, EI	1. Confirm that the system under test has the capability of providing Alternative Network Address Types for the Session Description Protocol. 2. Attempt to create a request for ANAT with the system tested and a dual stacked appliance. 3. Confirm that the system is offered the use of both an IPv6 and an IPv4 address. 4. The system tested shall choose the one set of addresses to create a single logical media stream for communication with the dual stacked appliance.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4091			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
112	**Section:** IP Version Negotiation **ID:** 38.2 The system shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092. **Reference:** UCR 2008 5.3.5.3.12	Required: SS, NA, EI	1. Attempt to solicit a request for the use of an Alternative Network Address Type (ANAT) to a separate system. 2. Verify that the SDP-ANAT option-tag is placed in the header-field when sending the ANAT request. 3. The SDP-ANAT option tag is used to verify that the recipient of the offer to use ANAT in fact supports its use, in which case it does not support its use the SDP-ANAT header can be used to ensure that an offer using ANAT is not processed by answerers without support for ANAT. The option-tag can also be used to explicitly discover the capabilities of a UA (i.e., whether it supports ANAT).	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4091 and RFC 4092			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
113	**Section:** IP Version Negotiation **ID:** 38.3 Dual stacked systems shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP. **Reference:** UCR 2008 5.3.5.3.12	Required: EI	1. Verify session establishment and the exchanging of the SDP between the system tested and a separate host. 2. Confirm that IPv4 and IPv6 addresses and located within the SIP INVITE.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4091			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
114	**Section:** AS-SIP IPv6 Unique Requirements **ID:** 45 The system shall be able to provide topology hiding (e.g., NAT) for IPv6 packets in the manner described in UCR 2008 Section 5.4, Information Assurance. **Reference:** UCR 2008 5.3.5.3.13	Required: EBC	1. Confirm the system tested has the ability to provide topology hiding for IPv6 addresses. 2. Topology Hiding can be accomplished in a number of different ways in Section 5.4.5.4.7 Edge Boundary Control Appliances in UCR 2008 it talks about the use of private addressing in IPv6 for the function of topology hiding. 3. Verify from outside the test network that you do not have the ability to map out the IP addresses used within the test network.	CAT II	
	IA Control: ECSC-1	**Origin:** UCR 2008 Section 5.4			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
115	**Section:** AS-SIP IPv6 Unique Requirements **ID:** 46 The system shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1). **Reference:** UCR 2008 5.3.5.3.13	Required: EI (Softphone)	Validate that the system tested has the ability to process the algorithms defined in RFC 3484 to complete default address selection to communicate with IPv6 hosts. (i.e. The IPv6 addressing architecture allows multiple unicast addresses to be assigned to interfaces. These addresses may have different reachability scopes (link-local, site-local, or global). These addresses may also be "preferred" or "deprecated". Privacy considerations have introduced the concepts of "public addresses" and "temporary addresses". The mobility architecture introduces "home addresses" and "care-of addresses". In addition, multi-homing situations will result in more addresses per node. For example, a node may have multiple interfaces, some of them tunnels or virtual interfaces, or a site may have multiple ISP attachments with a global prefix per ISP. The end result is that IPv6 implementations will very often be faced with multiple possible source and destination addresses when initiating communication.)	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3484			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
116	**Section:** Miscellaneous Requirements **ID:** 47 If the system supports Remote Authentication Dial In User Service (RADIUS) authentication, the system shall support RADIUS in the manner defined in RFC 3162. **Reference:** UCR 2008 5.3.5.3.13	Required: EBC, R, LS	1. Conduct an analysis of the system. 2. Verify accuracy of diagrams delineating each component, operating system, firmware version, application version, and test boundaries. Make a connection through RADIUS to both an IPv6 and IPv4 system.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3162			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
117	**Section:** Miscellaneous Requirements **ID:** 48 If the system supports Mobile IP version 6 (MIPv6), the system shall provide mobility support as defined in RFC 3775. **Reference:** UCR 2008 5.3.5.3.14 **IA Control:** ECSC-1	Required: EI (Softphone) **Origin:** RFC 3775	1. Check the system to confirm that has the capability to utilize Mobile IP version 6. 2. Attempt to setup the system on the test network to support Mobile IP version 6. 3. Take note of the home address of the system as this is what will be used to communicate with the host. 4. Connect the host to a separate segment on the test network and attempt to bind the care-of-address from the separate segment to the home agent to route source packets for the test system. 5. Verify that you are able to communicate with the system while it is on its normal link via its home address and you are able to communicate with the system while it is on a separate network segment via its care-of-address.	CAT II	
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
118	**Section:** Miscellaneous Requirements **ID:** 48.1 If the system acts as a home agent, the system shall provide mobility support as defined in RFC 3775. **Reference:** UCR 2008 5.3.5.3.14 **IA Control**: ECSC-1	Required: R **Origin:** RFC 3775	1. Validate that the system has the ability to act as a home agent. 2. Verify that once the system is setup as a home agent that you configure a separate host on the network to work as a mobile node. 3. Confirm that the host registers its home address with the home agent to allow it to bind its car-of-address once taken off of the local network to its home address to allow for the home agent to provide mobility support. 4. Remove the separate host from the local network segment and attach it to another segment, verify that it sends a binding update to the test system. 5. Attempt to communicate with the host on the separate network segment and ensure that the system tested routes the traffic to the mobile host.	CAT II	

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
119	**Section:** Miscellaneous Requirements **ID:** 49 If the system supports Mobile IP version 6 (MIPv6), the system shall provide a secure manner to signal between mobile nodes and home agents in manner described in RFC 3776 and RFC 4877 (FY2010). **Reference:** UCR 2008 5.3.5.3.14	Required: R, EI (Softphone)	1. The system tested shall have the ability to support Mobile IP version 6. 2. The home agent should check if a particular mobile node is authorized to use a home address before creating an IPSec security association. 3. The system shall have the ability to verify through the SPD the binding update of either a mobile node or a home agent. 4. The home agent then may store the assigned home address in the SPD entries created for a mobile node.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4877			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
120	**Section:** Miscellaneous Requirements **ID:** 51 If the system supports network mobility (NEMO), the system shall support the function as defined in RFC 3963. **Reference:** UCR 2008 5.3.5.3.14	Required: R, EI (Softphone)	1. Confirm the existence of the mobile network and also a mobile router for support of that network. 2. Setup the mobile router on the test network in place to register its home address on the local network with a local router. 3. Connect the router to a separate network segment and configure it to support the mobile network configured. 4. Confirm that the mobile router sends a binding update back to the local system on the original network where its home address is registered on and that the mobile router sends the binding update with its new care-of-address. 5. Verify that you are able to communicate with the system while it is on its normal link via its home address and you are able to communicate with the mobile network while it is on a separate network segment via its care-of-address.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3963			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
121	**Section:** Miscellaneous Requirements **ID:** 52 The systems shall support Differentiated Services as Described in RFC 2474 and RFC 5072 (FY 2010) for a voice and video stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and UCR 2008, Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. **Reference:** UCR 2008 5.3.5.3.14	Required: SS, NA, EBC, R, LS, EI	1. Ensure the system has the ability to support the use of differentiated services in accordance with RFC 2474 and RFC 5072. 2. Setup a security association between the test system and a separate host on the network. 3. Make sure that for that security association of the two systems that you have a voice and video system configured for use. 4. Begin to generate traffic to communicate with the voice and video system. 5. Analyze traffic on the network to confirm that the system is properly forwarding packets and is also differentiating between the voice and video packets 6. Also verify that the system is allowing for the ability to configure parameters for the differential treatment for the care of the different services of the network traffic.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 5072			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
122	**Section:** Miscellaneous Requirements **ID:** 53 If the system acts as an IPv6 tunnel broker, the system shall support the function in the manner defined in RFC 3053. **Reference:** UCR 2008 5.3.5.3.14	Required: EI (Softphone)	1. Ensure that the system has the ability to act as an IPv6 tunnel broker. 2. Once it is verified that the system has the ability to act as a tunnel broker you will need to place it on the test network. 3. Once placed on the test network configure a tunnel to allow for access by a preconfigured IPv6 host already on the test network. 4. Verify that the host on the network has the ability to tunnel through the system under test to communicate with a preconfigured IPv4 test network through the use of the tunnel broker.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 3053			
Test Case	**Requirement**	**System(s) Affected**	**Test Procedure(s)**	**Risk**	**Result(s)**
123	**Section:** Miscellaneous Requirements **ID:** 54 If the system supports roaming (as defined within RFC 4282), the system shall support this function as described by RFC 4282. **Reference:** UCR 2008 5.3.5.3.14	Required: R	1. Configure the system under test to have the ability to have a secure VPN communication between itself and a host. 2. Per RFC 4282 there are a number of means for a system to comply with roaming. 3. The user of the system must first have a Network Access Identifier to identify themselves to authenticate with the Network Access Server. 4. Once the user has authenticated to the Network Access Server through the Network Access Identifier then he will have the ability to open a tunnel for secure access to a VPN.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 4282			

Table E-13. IPv6 Requirements (continued)

Test Case	Requirement	System(s) Affected	Test Procedure(s)	Risk	Result(s)
124	**Section:** Miscellaneous Requirements **ID:** 55 If the system supports the Point-to-Point Protocol (PPP), the system shall support PPP as described in RFC 2472. **Reference:** UCR 2008 5.3.5.3.14	Required: R	1. Verify the system under test is capable of supporting the Point-to-Point Protocol. 2. Attempt to create a Point-to-Point connection between the system under test and another host on the test network. 3. Ensure that the system tests the connection and ensures it is available and that PPP reaches the network-layer protocol phase. 4. Once both sides have verified the connection view communication between the hosts until one side explicitly closes the connection.	CAT II	
	IA Control: ECSC-1	**Origin:** RFC 2472			

LEGEND:

AES	Advanced Encryption Standard
AH	Authentication Header
ANAT	Alternative Network Address Types
AS-SIP	Assured Services Session Initiation Protocol
BGP	Border Gateway Protocol
CAT	Category
CBC	Cipoher Block Chaining
CE	Customer Edge
CPU	Central Processing Unit
DCBP	Design Configuration Best Practices
DCCS	Design Configuration Configuration Standards
DCPA	Design Configuration Partitioning Application
DCSP	Design Configuration System
DHCP	Domain Host Control Protocol
DMTF	Distributed Management Task Force
DNS	Domain Name System
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EBC	Edge Border Controller
ECSC	Enclave Computing Environment Security Configuration Compliance
EI	End Instrument
ESP	Encapsulating Security Payload
EUI	Extended Unique Identifier
FY	Fiscal Year
HMAC	Hashed Message Authentication Code
IA	Information Assurance
ICMP	Internet Control Message Protocol
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPCP	IPsec Configuration Policy
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
LAN	Local Area Network
LS	LAN Switch
MAC	Media Access Control
MIB	Management Information Base
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NA	Network Appliance
NAT	Network Address Translation
NIC	Network Interface Card
NM	Network Module
OSPF	Open Shortest Path First
PC	Personal Computer
PMTU	Path Maximum Transmission Unit
PPP	Point-to-Point Protocol
R	Revision
R	Router
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAD	Security Association Database
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SPI	Security Parameter Index
SS	Softswitch
STIG	Security Technical Implementation Guidelines
TCP	Telecommunications Protocol
UA	User Agent
UC	Unified Capabilities
UCR	Unified Capabilities Requirement
UDP	User Datagram Protocol
URI	Uniform Resource Identifiers
V	Version
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VVoIP	Video and Voice over Internet Protocol
VLAN	Virtual Local Area Network

RTS INTERNET PROTOCOL VULNERABILITY (IPV) TESTING. In addition to the previously described IPV Phase II testing, the SIP, H.248/ Media Gateway Control (MEGACO), and Media Gateway Control Protocol (MGCP) will be tested to determine the security posture of each protocol.

The test cases were created from the specific IA requirements delineated in the RTS IA UCRs as well as requirements in the Call Control Agent (CCA), Signaling Gateway (SG), Media Gateway (MG), and Network Management (NM) UCRs.

Although many of the requirements in this test plan do not specifically address IA, after careful review, the IATT believes that many are deemed as closely related to security-type issues if the requirement failed in some way. As an example, if a requirement involves a specific protocol, it could be deduced that the protocol was not engineered correctly and a Denial-of-Service (DoS) could occur. This will be made clear as each vulnerability listed is examined in each test case.

In addition to testing requirements and specifications, informal ad hoc testing may also occur during this test phase.

The IPV testing examines those requirements that pertain to the Transport Layer Security (TLS) Internet Protocol Security (IPSec), and its underlying capabilities as used by the various RTS components.

Table E-14 shows the RTS IPV testing cases.

Table E-14. RTS Internet Protocol Vulnerability Testing

Test Case: 1	**Vulnerability:** Passwords transmitted in clear text may be sniffed by an adversary, thus allowing unauthorized access. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS, SS, LSC, MG, EBC, R, and LS **Reference:** IA UCR 4.1.1 R-12.12 **IA Control:** IAIA-1 and DCNR-1	The system shall only transmit passwords that are encrypted. Note: The Backbone Transport Services STIG requires that router administrative passwords be encrypted using MD5.	1. For any operation on the SUT that involves logging in using a UserID/Password combination, confirm that the password is sent in an encrypted form. This can be done by monitoring the communication link with network analyzer. 2. Verify that the encryption method being used is one that is authorized and FIPS-140-2 compliant.	
Test Case: 2	**Vulnerability:** An adversary can modify information and then masquerade or modify message stream traffic. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS, SS, LSC, MG, EBC, R, and LS **Reference:** IA UCR 4.1.1 R-13.13 **IA Control:** DCNR-1, DCSR-2, and ECTM-2	The default authentication mechanism for SNMPv3 shall be HMAC-SHA-96.	1. Configure the SNMPv3 communication path to include network sniffer. 2. Initialize an SNMPv3 session and verify that the HMAC-SHA-96 algorithm is being used.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 3	**Vulnerability:** If pinholes are not closed in sufficient time, a possible DoS situation can occur. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: EBC **Reference:** IA UCR 4.1.1 R-15.4.1.1 **IA Control:** DCSQ-1	The system 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.	1. Using network analyzer to monitor an AS-SIP signaling and media communication session, determine the ports (pin holes) used for the transport of the session by examining the information contained in the SDP of the INVITE message as well as the network analyzer trace information. 2. Immediately after concluding the session, perform a network scan on the specific ports found for the transport. 3. Confirm that the ports (pinholes) are closed.	
Test Case: 4	**Vulnerability:** If pinholes are not closed in sufficient time, a possible DoS situation can occur. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: EBC **Reference:** IA UCR 4.1.1 R-15.4.1.1.1.1 **IA Control:** DCSQ-1	The default media inactivity value for closing a session and issuing BYE messages shall be 5 minutes.	1. Establish an AS-SIP call. 2. Mute both ends of the call to simulate media inactivity. 3. Confirm that a BYE message is sent to end the session within 5 minutes.	
Test Case: 5	**Vulnerability:** An adversary can sniff signaling traffic and obtain information that could lead to numerous unauthorized actions, including masquerading, session hijacking, and billing fraud. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS, SS, LSC, and EBC [Conditional: EI] **Reference:** IA UCR 4.1.3 R-16.1.1 **IA Control:** DCNR-1 and ECTM-2	The system 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.	1. While monitoring the communications link with a network analyzer, establish an AS-SIP call. 2. Confirm that the call is using TLS for the signaling portion of the call on TCP port 5061.	
Test Case: 6	**Vulnerability:** An adversary can sniff signaling traffic and obtain information that could lead to numerous unauthorized actions, including masquerading, session hijacking, and billing fraud. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS, SS, LSC, and EBC [Conditional: EI] **Reference:** IA UCR 4.1.2 R-16.1.1.1 **IA Control:** DCNR-1 and ECTM-2	The system shall be capable of using HMAC-SHA1-96 with 160-bit keys. Note: The condition for the EI is the support of AS-SIP.	1. While monitoring the communications link with a network analyzer, establish an AS-SIP call. 2. Confirm that during the TLS handshake, the HMAC-SHA1-96 algorithm is being used for integrity. Note: This confirmation will have to occur at every hop of the call.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 7	**Vulnerability:** An adversary can sniff signaling traffic and obtain information that could lead to numerous unauthorized actions, including masquerading, session hijacking, and billing fraud. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS, SS, LSC, EBC, and EI **Reference:** IA UCR 4.1.3 R-16.1.2 **IA Control:** DCNR-1 and ECTM-2	If the system uses H.323, the system 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.	1. While monitoring with a network analyzer, establish an AS-SIP call that uses the H.323 protocol for video applications. 2. Examine the network analyzer's trace and verify that the Baseline Security Profile H.235.1, HMAC-SHA1-96 is being used for integrity purposes.	
Test Case: 8	**Vulnerability:** An adversary can sniff the voice or video traffic, thus obtaining critical information. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: EI, MG, and MFSS **Reference:** IA UCR 4.1.2, 4.1.3 R-16.8.1, R-17.2 , R-17.2.3, and R-17.2.4 **IA Control:** ECCT-1 and DCNR-1	R-16.8.1 [EI, MG, and MFSS] The system shall be capable of using HMAC-SHA1-32 to authenticate the tag with 60-bit key length as the default integrity mechanism for SRTP packets. R-17.2 [EI, EBC, and MG] The system shall be capable of providing confidentiality for media streams using SRTP with the AES_CM_128 encryption algorithm as the default (Threshold) or AES 256-bit algorithm (Objective). R-17.2.3 [MFSS, SS, LSC, MG, EBC, and EI] The system shall be capable of distributing the Master Key and the Salt Key in concatenated form. R-17.2.4 [EI, EBC, and MG] The system shall use a Master Key of 128 bits in order to support 128-bit AES encryption. Note: This implies that the Master Salt Key may be null.	The integrity algorithm being used to secure the RTP packets for an AS-SIP call is located in the SDP of the INVITE message. Because of the use of TLS to secure the signaling stream, SDP information is not able to be determined. If the SUT allows, temporarily inhibit TLS for this test. This could be achieved by forcing the NULL cipher to be the first choice of the SUT for TLS. 1. While monitoring the AS-SIP communication link, establish a call. 2. In the INVITE message, examine the SDP a=crypto: field to determine the algorithm and key length being used for the integrity of the SRTP packets and the encryption algorithm used for confidentiality. Examine the inline: field to confirm the Master and Salt key information. If TLS on the SUT cannot be inhibited, the vendor should display the database or configuration data information that equates to the SDP data. Note: This should be confirmed on every hop of the call.	
Test Case: 9	**Vulnerability:** Using a weak integrity algorithm can lead to insecure communications. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, MG, EBC, R, and LS] **Reference:** IA UCR 4.1.2 R-16.15 **IA Control:** DCNR-1	If the system uses SSHv2, the system shall use HMAC-SHA1-96 for data integrity.	1. While monitoring the SSH communication, link a network analyzer and establish an SSH session with the SUT. 2. Examine the network analyzer's trace and confirm that the SSH handshake shows that HMAC-SHA1-96 is being used for data integrity.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 10	**Vulnerability:** An adversary may be able to eavesdrop on critical communications. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, MG, and EI] **Reference:** IA UCR 4.1.3 R-17.3.1 **IA Control:** DCSR-1 and ECCT-1	If H.323, MGCP, or H.248 (MEGACO) is used, the system shall be capable of using IPsec to provide confidentiality.	1. While monitoring the communication link using network analyzer, establish an H.323, MGCP or H.248 session with the SUT. 2. Examine the network analyzer's trace and confirm that IPsec is being used to preserve confidentiality.	
Test Case: 11	**Vulnerability:** Improper handling of the session keys could lead to compromising of security features. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, and MG] **Reference:** IA UCR 4.1.3 R-17.3.1.1 **IA Control:** ECCT-1	If the system uses H.248 (MEGACO), the system shall be capable of distributing the SRTP Master Key and Salt Key in the SDP "k =" crypto field when using H.248.15.	1. While using a network analyzer to monitor the communication link for H.248 type calls, establish an H.248 call. 2. Examine the network analyzer's trace and confirm the Master/Salt key information located in the "k=" field. Note: May have to inhibit IPsec for this test.	
Test Case: 12	**Vulnerability:** Improper handling of the session keys could lead to compromising of security features. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, and MG] **Reference:** IA UCR 4.1.3 R-17.3.1.2 **IA Control:** ECCT-1	If H.323 is used, the system shall be capable of distributing the SRTP Master Key and Salt Key in H.235 using the H235 Key as described in H.235.0 and H.235.8.	1. While using a network analyzer to monitor the communication link for H.323 type calls, establish an H.323 call. 2. Examine the network analyzer's trace and verify the Master/Salt key information located in the H235Key parameter.	
Test Case: 13	**Vulnerability:** Improper handling of the session keys could lead to compromising of security features. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: Conditional: MFSS, SS, LSC, and MG **Reference:** IA UCR 4.1.3 R-17.3.1.3 **IA Control:** ECCT-1	If IPsec is used, the system shall be capable of using IKE version 1 [Threshold], version 2 [Objective FY10] for IPsec key distribution. Note: IKEv2 requirements are found in Appendix F, IPv6 UCR.	1. Verify the IKE key exchange process is supported by the IPsec on the SUT. 2. While establishing test calls, monitor IPsec communications. 3. Verify the ISAKMP exchanges. Note: As an integrity check of the IKE process, run the IPsec/IKE fuzzing tool.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 14	**Vulnerability:** An adversary may be able to submit erroneous certificates, thereby gaining un-authorized access. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: Conditional: MFSS, SS, LSC, and MG **Reference:** IA UCR 4.1.3 R-17.3.1.3.4.1 **IA Control:** ECCT-1	If IPsec is used, the system shall only support the following erroneous messages associated with a certificate request: • Invalid Key • Invalid ID • Invalid certificate encoding • Invalid certificate • Certificate type unsupported • Invalid CA • Invalid hash • Authentication failed • Invalid signature • Certificate unavailable	Confirm that IPsec sessions will not be successful due to the following certificate conditions: • Invalid Key • Invalid ID • Invalid certificate encoding • Invalid certificate • Certificate type unsupported • Invalid CA • Invalid hash • Authentication failed • Invalid signature • Certificate unavailable All IPsec attempts with the above error conditions should fail.	
Test Case: 15	**Vulnerability:** Unsecured SIP messages could allow an adversary access to the system. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, EI, and EBC] **Reference:** IA UCR 4.1.3 R-17.3.2.8 **IA Control:** DCSR-2 and ECCT-1	The system shall reject all received AS-SIP packets associated with port 5061 that are not secured with TLS. Note: This ensures that the system does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.	1. Using a network analyzer, create a non-TLS AS-SIP INVITE message and send it over the AS-SIP link using TCP port 5061 2. Confirm that the message is discarded. 3. Repeat step 1 using the UDP protocol. 4. Confirm that the message is discarded.	
Test Case: 16	**Vulnerability:** AS-SIP messages that are accepted and processed on any port except 5061 can provide an adversary with unauthorized access to the system. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, EI, and EBC] **Reference:** IA UCR 4.1.3 R-17.3.2.9 **IA Control:** DCSR-2 and ECCT-1	The system shall only accept and process AS-SIP packets that arrive on port 5061. Note: The system should discard AS-SIP packets that arrive on a different port.	1. Using a network analyzer, create a non-TLS SIP INVITE message and send it over the AS-SIP link using TCP port 5060. 2. Confirm that the message is discarded or ignored. 3. Repeat step 1 using the UDP port 5060 protocol. 4. Confirm that the message is discarded or ignored.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 17	**Vulnerability:** Using a cipher of a lesser strength could allow an adversary to compromise the lesser strength cipher, thus allowing the adversary the ability to decrypt potentially sensitive information. If compression is used, this may affect interoperability with other vendor implementations, possibly causing a DoS situation. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: Conditional: MFSS, SS, LSC, MG, and EBC **Reference:** IA UCR 4.1.3 R-17.3.1.3 **IA Control:** DCSR-2, ECCT-1, and DCNR-1	17.6 [Conditional: MFSS, SS, LSC, MG, and EBC] If the system uses TLS, it shall do so in a secure manner as defined by the following subtended requirements. 17.6.1 [Conditional: MFSS, SS, LSC, MG, and EBC] If the system uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA (Threshold) or TLS_RSA_WITH_AES_256_CBC_SHA (Objective) as its default cipher. 17.6.2 [Conditional: MFSS, SS, LSC, MG, and EBC] If the system uses TLS, it shall be capable of using a default of no compression. Note: This requirement is not associated with Network Management related sessions.	1. Using a network analyzer to monitor the communication, establish an AS-SIP call. 2. Examine the network analyzer's trace and confirm that the TLS handshake has chosen the TLS_RSA_WITH_AES_128_CBC_ SHA algorithm. 3. Also during the same network analyzer's examination, confirm that no compression is being used.	
Test Case: 18	**Vulnerability:** Use of rarely used or non-standard encryption algorithms could allow an adversary to decrypt sensitive communications. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [Conditional: MFSS, SS, LSC, and MG] **Reference:** IA UCR 4.1.3 R-17.11 **IA Control:** ECCT-1	If the system uses IPsec, the system shall be capable of using 3DES-CBC (class value 5) as the default IKE encryption algorithm (Threshold) AES-CBC (Objective).	1. While monitoring the communications path, establish a call that uses IPsec. 2. During the handshaking process, confirm that the 3DES-CBC encryption algorithm is chosen.	
Test Case: 19	**Vulnerability:** The lack of a secure key exchange can allow an adversary access to information that could subsequently allow an adversary to exploit the system, possibly performing DoS or Replay attacks. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [MFSS, SS, LSC, MG, and EI] **Reference:** IA UCR 4.1.3 R-17.3.1.3 **IA Control:** ECCT-1	If IPsec is used, the system shall be capable of using IKE version 1 [Threshold], version 2 [Objective FY10] for IPsec key distribution. Note: IKEv2 requirements are found in Appendix F, IPv6 UCR.	1. While monitoring the communications path, establish a call that uses IPsec. 2. During the IPsec/IKE handshake process, verify that ISAKMP is being used via port 500.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 20	**Vulnerability:** The more coded text an adversary can accumulate, the faster the adversary can crack the key. Re-keying after a certain number of bytes have been sent is desirable. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: [MFSS, SS, LSC, MG, EBC, R, and LS] **Reference:** IA UCR 4.1.3 R-17.13 **IA Control:** ECCT-1	The system shall re-key each encrypted session once the session has transmitted a maximum of 2** (L/4) blocks of data. L represents 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.	1. While monitoring the AS-SIP signaling link using a network analyzer, establish communications that require TLS. 2. Ensure the TLS session is one in which large amounts of data is exchanged (e.g. video messaging). 3. Confirm that a re-key occurs after an exchange of 2** (L/4) blocks of data. 4. Establish an IPsec session and confirm that a re-key occurs after 2** (L/4) blocks of data are exchanged.	
Test Case: 21	**Vulnerability:** An adversary could attempt to establish H.248 calls if authentication is not verified, resulting in un-authorized resource usage. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (LSC1, LSC2, MG, and SG) **Reference:** CCA UCR 3.6.3 R-186 and IA UCR 17.3.1 **IA Control:** IAIA-1 and ECCT-1	[Required for MFSS, Conditional for LSC1 and LSC2] The CCA MGC shall relay received H.248 and IPsec (or proprietary-protocol-equivalent) authentication credentials and encryption key information from sending end systems (MGs and SGs) to the IA Function, to support the IA Function's MG and SG authentication capabilities, and its MG and SG signaling stream encryption capabilities.	1. While monitoring the CCA interface using a network analyzer, H.248 calls should be originated that contain valid authentication and encryption information. 2. Repeat step 1; however, using a fuzzer, create an H.248 signaling with invalid authentication and encryption information included in the signaling messages. 3. Confirm that the IA function rejects the invalid calls.	
Test Case: 22	**Vulnerability:** An adversary could attempt to access the H.248 subsystem with invalid encryption information. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA) **Reference:** CCA UCR 3.6.3 R-187 **IA Control:** ECCT-1 and DCNR-1	The CCA shall relay SRTP encryption key information received from sending end systems (EI, MG, and EBC) to the IA Function, to support the IA Function's EI, MG, and EBC media stream encryption capabilities.	1. While monitoring the CCA interface using a network analyzer, H.248 calls should be originated that contain valid encryption information. 2. Repeat step 1; however, using a fuzzer, create an H.248 signaling with invalid encryption information included in the signaling messages. 3. Confirm that the IA function rejects the invalid calls.	
Test Case: 23	**Vulnerability:** Theft of services can occur if un-authenticated calls are permitted to complete. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA, EI, and EBC) **Reference:** CCA UCR 3.6.3 R-188 **IA Control:** IAIA-1 and DCNR-1	The CCA shall relay authentication credentials received in a SIP or AS-SIP REGISTER message from an EI or EBC to the IA Function, so that the IA Function can validate those credentials and allow that EI or EBC to register with the Appliance.	1. Configure the EI with invalid authentication data. 2. While monitoring the CCA using a network analyzer, the EI attempts to Register. 3. Confirm that the Registration was rejected. 4. Repeat 1-3 using the EBC.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 24	**Vulnerability:** An adversary may be able to perform a MITM attack, thereby having access to all communications between the MG and the CCA. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and MG) **Reference:** CCA UCR 3.6.3 R-189 **IA Control:** IAIA-1 and DCNR-1	[Conditional – FY2008] The CCA MGC shall relay authentication credentials received with an H.248 message in an IPsec packet from an MG to the IA Function, so that the IA Function can validate those credentials and allow that MG to register with the Appliance.	1. Configure the MG with invalid authentication data. 2. While monitoring the CCA using a network analyzer, ensure the MG sends H.248 messages with invalid authentication information. 3. Confirm that the call is rejected.	
Test Case: 25	**Vulnerability:** An adversary may be able to perform a MITM attack, thereby having access to all communications between the SG and the CCA. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and SG) **Reference:** CCA UCR 3.6.3 R-190 **IA Control:** IAIA-1 and DCNR-1	[Required for MFSS, Conditional for LSC1 and LSC2] The CCA MGC shall relay authentication credentials received with an encapsulated CCS7 message in an IPsec packet from an SG to the IA Function, so that the IA function can validate those credentials and allow that SG to register with the Appliance.	1. Configure the SG with invalid authentication data. 2. While monitoring the CCA using a network analyzer, ensure the SG sends an IPsec. 3. Encapsulate the SS7 message with invalid authentication information. 4. Confirm that the call is rejected.	
Test Case: 26	**Vulnerability:** Use of weak encryption algorithms in an EI could lead to an adversary decrypting sensitive communications. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and EI) **Reference:** CCA UCR 3.6.3 R-191 **IA Control:** ECCT-1	The CCA shall relay TLS encryption key information received from an EI to the IA Function, so that the IA Function can verify that this encryption key information can be used on the resulting signaling stream for the resulting VoIP or Video session from that EI.	1. Configure the EI to use an encryption algorithm that is invalid (not 160 bits in length). Key information is contained in the INVITE SDP information. 2. Calls from this EI should be rejected. Note: TLS may need to be inhibited for this test.	
Test Case: 27	**Vulnerability:** Use of weak encryption algorithms in an EBC could lead to an adversary decrypting of sensitive communications. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and EBC) **Reference:** CCA UCR 3.6.3 R-192 **IA Control:** ECCT-1	The CCA shall relay TLS encryption key information received from an EBC to the IA Function, so that the IA Function can verify that this encryption key information can be used on the resulting signaling stream for the resulting VoIP or Video session from that EBC.	1. Configure the EBC to use an encryption algorithm that is invalid (not 160 bits in length). 2. Calls using this EBC should be rejected.	
Test Case: 28	**Vulnerability:** An adversary could attempt to use invalid encryption key information to obtain un-authorized access. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and EI) **Reference:** CCA UCR 3.6.3 R-193 **IA Control:** ECCT-1	The CCA shall relay SRTP encryption key information received in a SIP or AS-SIP INVITE message from an EI to the IA Function, so that the IA Function can verify that this encryption key information can be used on the resulting media stream for the resulting VoIP or Video session from that EI.	1. Create an AS-SIP INVITE message with invalid encryption key data in the SDP. 2. When this INVITE is sent to the CCA, the call is rejected.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 29	**Vulnerability:** An adversary could attempt to use invalid encryption key information to obtain un-authorized access. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and EBC) **Reference:** CCA UCR 3.6.3 R-194 **IA Control:** ECCT-1	The CCA shall relay SRTP encryption key information received in an AS-SIP INVITE message from an EBC to the IA Function, so that the IA Function can verify that this encryption key information can be used on the resulting media stream for the resulting VoIP or Video session from that EBC.	1. Create an AS-SIP INVITE message with invalid encryption key data in the SDP. 2. When this INVITE is sent, via the EBC, to the CCA, the INVITE is rejected. Note: In order to execute this procedure, TLS may have to be turned off.	
Test Case: 30	**Vulnerability:** An adversary could attempt to use invalid encryption key information to obtain un-authorized access. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA) **Reference:** CCA UCR 3.6.3 R-195 **IA Control:** ECCT-1	[Conditional – FY2008] The CCA shall relay SRTP encryption key information received in an H.248 message in an IPsec packet from a MG to the IA Function, so that the IA Function can verify that this encryption key information can be used on the resulting media stream for the resulting VoIP session from that MG.	1. Establish H.248 call with invalid encryption key data in the SDP. 2. When this INVITE is sent to the CCA, the INVITE is rejected. Note: In order to execute this procedure, IPsec may have to be turned off. Alternatively, a protocol emulator/simulator could be used to fabricate H.248 calls.	
Test Case: 31	**Vulnerability:** The MGC could react to invalid or malformed Notify and Service Change messages in a non-graceful manner, possibly causing a DoS, or other service disruptions. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MGC and MG **Reference:** CCA UCR 3.3.1 R-171 **IA Control:** DCNR-1 and DCSQ-1	[Conditional – FY2008] The MGC shall be capable of receiving, interpreting and acting upon the following two commands as part of TransactionRequests received from MGs, as specified by H.248: • Notify • ServiceChange	1. Using a fuzzer, create malformed Notify and ServiceChange H.248 messages. 2. The messages should contain invalid information. 3. Verify that the MGC rejects the malformed messages in a graceful manner and is then able to process valid H.248 calls.	
Test Case: 32	**Vulnerability:** An adversary could maliciously forward invalid H.248 packets to the MGC or MG, possibly causing a DoS condition or other disruptive actions. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MGC and MG **Reference:** CCA UCR 3.3.1 R-174 **IA Control:** DCNR-1	[Conditional – FY2008] When the MGC uses ITU-T H.248 for MG control, the MGC shall secure the H.248 messages that it exchanges with the MG using IPsec at the IP Network Layer, consistent with the H.248 IA requirements in the DoD IA UCR.	1. Using a network analyzer to monitor the communication, confirm that the H.248 protocol is secured by IPsec. 2. Originate CAS calls that require the H.248 protocol. 3. The calls should complete. The network analyzer should indicate that IPsec is being used to secure the calls. The AES_128_CBC should be the default encryption algorithm. 4. Using a fuzzer, create and send invalid H.248 messages to the MGC and MG. 5. Expect the H.248 messages to be dropped or ignored due to not being secured with IPsec.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 33	**Vulnerability:** An adversary could attempt an "uncontrolled barge-in" attack. This attack can be performed by directing media packets to the IP address and UDP port used by a connection, causing theft of service or DoS. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MGC and MG **Reference:** ITU-T H.248.1 Section 10.3 AdHoc **IA Control:** DCNR-1	Note: An alternative to checking the source address is to encrypt and authenticate the packets, using a secret key that is conveyed during the call set-up procedure. This will not slow down the call setup and provides strong protection against address spoofing.	1. Using a network analyzer to monitor the communication, confirm that IPsec secures the H.248 protocol. If IPsec is in use, this test is not applicable. Otherwise, continue to step 2. 2. Using network analyzer, create and send H.248 Media packets using a spoofed source IP address. 3. If the spoofed packets are allowed, this is a finding.	
Test Case: 34	**Vulnerability:** An adversary could attempt to inject malformed or invalid H.248 packets toward the H.248 appliance, possibly causing a DoS. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MGC and MG **Reference:** ITU-T H.248.1 Section 10.3 AdHoc **IA Control:** DCNR-1	The following H.248 commands should be tested for basic message parsing integrity (fuzzing). **Add:** The "Add" command adds a Termination to a particular Context. On the first Termination in a Context, "Add" is used to create a Context. **Modify:** The "Modify" command modifies the properties, events, and signals of a Termination. **Subtract:** The "Subtract" command disconnects a Termination from its Context and returns statistics on the Termination's participation in the Context. **Move:** The "Move" command automatically moves a Termination to another Context. **AuditValue:** The "AuditValue" command returns the current state of properties, events, signals, and statistics of Terminations. **AuditCapabilities:** The "AuditCapabilities" command returns all the possible values for Termination properties, events, and signals allowed by the Media Gateway. **Notify:** The "Notify" command allows the MG to inform the MGC of the occurrence of events in the MG. **ServiceChange:** The "ServiceChange" Command allows the MG to notify the MGC that a Termination or group of Terminations is about to be taken out of service, or have just been returned to service. A number of *ServiceChangeReasons* are provided with further details.	1. Using a network analyzer to monitor the communication, confirm that IPsec secures the H.248 protocol. If IPsec is in use, this test is not applicable. Otherwise, continue to step 2. 2. Using fuzzer, create and send H.248 messages that are malformed or contain an invalid date. 3. The H.248 appliance should handle these messages in a graceful manner.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 35	**Vulnerability:** Communications that are not secure could allow an adversary to sniff traffic and acquire information that could be used on subsequent attacks. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA and SG) **Reference:** CCA UCR 3.4.1 O-6, DR-4 **IA Control:** ECCT-1 and DCNR-1	**[O-6]** [Objective – FY2008] It is desirable for the CCA to use IETF-standard SS7-over-IP protocols for SG control. In this case, the CCA shall transport the CCS7 messages that it exchanges with the SG using one of the following IETF-standard Transport Layer Protocols: • TCP • UDP • SCTP **[DR-4]** [Objective – FY2008] When objective O-6 is supported and the CCA uses IETF standard SS7-over-IP protocols for SG control, the CCA shall secure the SS7-over-IP information that it exchanges with the SG using IPsec at the IP Network Layer, consistent with the IA requirements in the DoD IA UCR.	1. Using a network analyzer to monitor the communication, confirm that the SS7-over-IP protocol is secured by IPsec. 2. Originate calls that require the SS7-over-IP protocol. 3. The calls should complete. The network analyzer should indicate that IPsec is being used to secure the calls. 4. Also, confirm that IPsec or TLS is being used on every hop of the call, from EI to EI.	
Test Case: 36	**Vulnerability:** An adversary can sniff unsecured signaling. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MG and MGC **Reference:** MG UCR 3.3.2 R-31 **IA Control:** ECCT-1 and DCNR-1	When an open MGC-MG interface is used, the MG shall support IPsec. The IPsec is for use to secure IP Packets containing H.248 signaling and encapsulated ISDN PRI signaling messages. The MG support for IPsec shall conform to the ARTS Appliance IPsec requirements in the DISA IA UCR. Note that the MG is not required to support IPsec for use in IP Packets containing SRTP media streams for VoIP, FoIP, and MoIP calls.	1. Using a network analyzer to monitor the communication, confirm that the incoming ISDN PRI protocol is secured by IPsec between the MGC and MG. 2. Originate calls that require the ISDN PRI protocol. 3. The calls should complete. The network analyzer should indicate that IPsec is being used to secure the calls.	
Test Case: 37	**Vulnerability:** Unsecured media streams can be sniffed by an adversary. **Category**: Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MG and MGC **Reference:** MG UCR 3.3.4 R-36 **IA Control:** ECCT-1 and DCNR-1	When an open MGC-MG interface is used, the MG shall support exchange of VoIP media streams with Appliance EIs, other Appliance MGs, and the Appliance EBC (and through the Appliance EBC, with other EIs and MGs on other ARTS Appliances) using the following IETF-defined Media Transfer Protocols: • SRTP is conformant with IETF RFC 3711, SRTP, March 2004. • SRTCP is also conformant with IETF RFC 3711.	1. Using a network analyzer to monitor the communication, confirm that the media stream is secured by SRTP. 2. Originate voice, and video calls. The calls should complete. The network analyzer should indicate that SRTP (UDP) is being used to secure the calls. The HMAC-SHA1-32 should be used for integrity and AES_CM_128 for confidentiality.	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

Test Case: 38	**Vulnerability:** Unsecured signaling messages could allow an adversary to sniff the traffic and obtain useful information for a subsequent attack. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MG and MGC **Reference:** MG UCR 3.3.5 R-40 **IA Control:** ECCT-1 and DCNR-1	When an open MGC-MG interface is used, and the VoIP Signaling Streams contain H.248 Gateway Control Protocol messages at the Application Layer, the MG shall use • IPsec at the Network Layer, and • UDP, TCP, or SCTP at the Transport Layer. The MG shall secure the H.248 message exchange with the MGC using IPsec at the Network Layer in this case. The MG is not required to use an H.248 Adaptation Layer between the Transport Layer and the H.248 Application Layer in this case. In addition, the MG is not required to use TLS to secure UDP, TCP, or SCTP packets at the Transport Layer in this case, because IPsec is used to secure the underlying IP packets at the Network Layer.	1. Monitor the interface between the MGC and the MG using a network analyzer. 2. Establish CAS or PRI calls that would terminate at the MG. 3. Examine the network analyzer's trace and confirm that the signaling is secured with IPsec.	
Test Case: 39	**Vulnerability:** The inability of the MG/MGC to properly inter-work CAS signaling could lead to a Denial of Service situation. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MG and MGC **Reference:** MG UCR 3.3.7.1 R-46 **IA Control:** DCSQ-1	When an MG inter-works a TDM call from a CAS Trunk with a VoIP Session within the ARTS Appliance, the MG shall • Convert between the TDM Media Stream on the CAS Trunk and the VoIP SRTP/Transport Layer/IP Media Stream within the ARTS Appliance • Convert between the CAS signaling sequences on the CAS trunk and the VoIP signaling sequences within the ARTS Appliance.	1. Monitor the interface out of the MG using a network analyzer. 2. Establish a CAS call to the MG. 3. Examine the INVITE message in the network analyzer's trace. (Note: TLS will have to be inhibited for this test.) 4. The SDP data in the INVITE should correspond with the incoming CAS signaling.	
Test Case: 40	**Vulnerability:** Billing information could be intercepted during transmission, allowing an adversary access to sensitive information. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA **Reference:** NM UCR 7.2.5 R-147 **IA Control:** DCSR-2 and ECCT-1	[Required – FY2008] The BA should be able to electronically output the records over a secured connection. (Note: This is needed to allow transfer of CDRs from one DSN/RTS location to another in a secure manner (e.g., to prevent intruder detection, theft, and/or manipulation of DSN/RTS CDRs)).	Verify that output of billing records is done so in a secure manner (e.g., using SSH).	

Table E-14. RTS Internet Protocol Vulnerability Testing (continued)

LEGEND:

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ARTS	Assured Real Time Services
AS-SIP	Assured Services-Session Initiation Protocol
BA	Budget Activity
CA	Certificate Authority
CAS	Channel Associated Signaling
CBC	Cipher Block Chaining
CCA	Call Control Agent
CCS7	Common Channel Signaling Seven
CDR	Compact Disk Recordable
CM	Counter Mode
DCNR	Design Configuration Non-Repudiation
DCSQ	Design Configuration Software Quality
DCSR	Design Configuration
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoS	Denial of Service
DSN	Defense Switched Network
E1	European Standard 1
EBC	Edge Border Controller
ECCT	Enclave Computing Confidentially at in Transit
ECTM	Enclave Computing Environment, Transmission Integrity Controls
FIPS	Federal Information Processing Standards
FoIP	Fax over Internet Protocol
FY	Fiscal Year
H.235	Security and encryption for H-series multimedia terminals
H.248	Gateway Control Protocol
H.323	ITU Recommendation Audiovisual and multimedia systems
HMAC	Hash Message Authentication Code
IA	Information Assurance
IAIA	Identification Authentication Individual Identification and Authentication
IETF	Internet Engineering Task Force
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol security
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization
LS	LAN Switch
LSC	Local Call Control
MD5	Message Digest algorithm 5
MEGACO	Media Gateway Control
MFSS	Multifunction Soft Switch
MG	Media Gateway
MGC	Media Gateway Controller
MoIP	Media over Internet Protocol
NM	Network Management
PRI	Primary Rate Interface
R	Requirement
R	Router
RFC	Request For Comment
RTS	Real Time Services
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SG	Signaling Gateway
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SNMPv3	Simple Network Management Protocol version 3
SRTCP	Secure Realtime Control Protocol
SRTP	Secure Real-time Transport Protocol
SS	Soft Switch
SS7	Signaling System 7
SSH	Secure Shell
SSHv2	Secure Shell version 2
STIG	Security Technical Implementation Guidelines
SUT	System Under Test
TCP	Transmission Control Protocol
TDM	Time Division Multiplexer/Multiplexing
TLS	Transport Layer Security
UCR	Unified Capabilities Requirements
UDP	User Datagram Protocol
V	Version
VoIP	Voice over Internet Protocol

RTS TDM PROTOCOL SECURITY ANALYSIS

Time Division Multiplexing (TDM) Protocol Security Analysis (TPSA) consists of examining those requirements or specifications that have to do with Signaling System 7 (SS7), Integrated Services Digital Network (ISDN) Signaling, and Channel Associated Signaling (CAS).

The test cases were created from the RTS IA UCR and requirements in the CCA, SG, MG, and NM UCRs.

Additionally, requirements, specifications, and standards used during the development of this test plan include International Telecommunications Union – Telecommunications Standardization Sector (ITU-T) Q.921, Q.922, Q.931, and I.431 and Telcordia 2000 Version of National ISDN Primary Rate Interface (PRI) CPE Generic Guidelines System Requirement (SR)-4994, and the American National Standards Institute (ANSI) T1-111 through T1-114 for SS7.

Many of the requirements in this test plan do not specifically address IA. However, after careful review, the IATT believes that many RTS requirements are closely related to security issues if the requirement failed in some way during testing. As an example, if a requirement concerns a specific protocol message, the tester can deduce that a DoS could occur if the protocol is not engineered correctly. This will be made clearer as the tester examines the vulnerability listed for each test case.

In addition to the testing of requirements and specifications, informal ad hoc testing may also occur during this test phase. Table E-15 shows SS7 Protocol Security Analysis. Table E-16 shows ISDN Protocol Security Analysis, and Table E-17 shows CAS Protocol Security Analysis.

Table E-15. SS7 Protocol Security Analysis

<table>
<tr><td>Test Case: 1</td><td colspan="3">Vulnerability: An adversary could send SS7 messages towards the RTS SS7 network, possibly disrupting SS7 traffic.
Category: Medium</td></tr>
<tr><td>Test Information</td><td>Requirement</td><td>Test Procedure</td><td>Results</td></tr>
<tr><td>Systems Affected:
MFSS (CCA)

Reference:
CCA UCR 3.2.4.12.4 R-91
ANSI T1.111

IA Control: DCSQ-1</td><td>The SIP/SS7 IWF shall process received CCS7 RSC, GRS, or CGB messages as such:
<table><tr><th>Received from SS7</th><th>Sent to AS-SIP</th></tr><tr><td>RSC
GRS
CGB</td><td>500 Server Internal Error or BYE</td></tr></table></td><td>1. Using a TPSA testing tool, create Reset Circuit, Group Reset, and Carrier Group Blocking messages.
2. Establish an AS-SIP call.
3. While monitoring the AS-SIP call with the network analyzer, verify that sending the RSC, GRS, and CGB messages result in either the 500 Server Internal Error or the BYE message. The established AS-SIP call should not be affected.</td><td></td></tr>
<tr><td>Test Case: 2</td><td colspan="3">Vulnerability: Invalidly coded SS7 IAM messages incoming from the SS7 network could cause a Denial of Service.
Category: High</td></tr>
<tr><td>Test Information</td><td>Requirement</td><td>Test Procedure</td><td>Results</td></tr>
<tr><td>Systems Affected:
SG

Reference:
SG UCR 3.1.2.3.1 R-13
ANSI T1.111

IA Control: DCSQ-1</td><td>[R-13] The SG shall adhere to the rules and specifications for formatting of SS7 messages and coding of the fields and subfields as specified in Chapter T1.111.4 of ANSI T1.111 [1].</td><td>1. Using a TPSA test tool, create and send the following ISUP messages to the SG:
• IAM with invalid DPC
• IAM with invalid SIO NI octet
• IAM with invalid Network Indicator
• IAM with invalid OPC (decimal value)
• IAM with invalid DPC (decimal value)
• IAM with invalid SI
• IAM with invalid Network Indicator (decimal value)
2. Confirm that the SG responds to the invalid IAM's with a RELease message and no other adverse effects.</td><td></td></tr>
<tr><td>Test Case: 3</td><td colspan="3">Vulnerability: An adversary could send SS7 messages toward the RTS SS7 network to cause Denial of Service or other SS7 network interruptions.
Category: High</td></tr>
<tr><td>Test Information</td><td>Requirement</td><td>Test Procedure</td><td>Results</td></tr>
<tr><td>Systems Affected:
SG

Reference:
SG UCR 3.1.2.6.1 R-51
ANSI T1.111

IA Control: DCSQ-1 and VIVM-1</td><td>The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e. screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].</td><td>1. Attempt to send a Link Inhibit message from a TPSA test tool to the SG, from a foreign network.
2. The TPSA test tool should be configured as an end office (SSP) in a foreign network. The Link Inhibit message contains an OPC from a foreign network. The DPC is the SG. This would be an outsider attempt at an attack.</td><td></td></tr>
</table>

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 4	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network in to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to send a Link Inhibit message from TPSA test tool to the SG, from the local network . 2. The TPSA test tool should be configured as an SSP with a valid OPC, however the LIN message contains an invalid OPC (spoofed OPC = STP OPC). The DPC is the SG. This is an insider attack attempt.	
Test Case: 5	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1]. **(a)**	1. Attempt to isolate the SG by strategically sending LIN messages to SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC; however, the LIN message should contain an invalid OPC (spoofed OPC = STP).	
Test Case: 6	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause Denial of Service or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to isolate the SG by sending ECO messages to the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The ECO message contains an OPC (spoofed OPC = STP). The DPC is the SG point code.	
Test Case: 7	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to isolate the SG by sending COO messages to the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The COO message contains a spoofed OPC (spoofed OPC = STP). The DPC is the SG point code.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 8	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to isolate the SG by sending UPU messages to the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The UPU message contains a spoofed OPC (spoofed OPC = STP). The DPC is the SG point code.	
Test Case: 9	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to isolate the SG by sending TFP messages to the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The TFP message contains a spoofed OPC (spoofed OPC = STP A). The DPC is spoofed as STP B. The Affected Point Code parameter should indicate the SG Point Code.	
Test Case: 10	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to isolate the SSP by sending TFR messages to the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The TFR message contains a spoofed OPC (spoofed OPC = STP A). The DPC is spoofed as STP B. The Affected Point Code parameter should indicate the SG Point Code.	
Test Case: 11	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. A TFC message is sent by an STP in response to a received MSU when the priority of the concerned message is less than the current congestion status of the signaling link selected to transmit the MSU. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The TFC message contains a spoofed OPC (spoofed OPC = STP A). The DPC is spoofed as STP B. The congested Point Code parameter should indicate the SG Point Code. The congestion level should be a negative value.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 12	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Attempt to cause a DoS to the SG by strategically sending TFP's and LIN's that correspond to the two signaling links of the SG. 2. The TPSA test tool should be configured as an SSP with a valid OPC. The TFP message contains a spoofed OPC (spoofed OPC = STP A). The DPC is spoofed as STP B. The Affected Point Code parameter should indicate the SG Point Code. 3. The LIN message contains an invalid OPC (spoofed OPC = SG).	
Test Case: 13	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	Build and send an IAM message containing a spoofed OPC (spoofed OPC = a point code that the SUT knows). The DPC is the SG.	
Test Case: 14	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Build and send an IAM message containing a valid OPC. The DPC is a non-existent point code in the SG/CCA routing tables. 2. A RELease should be returned with a cause value of "No route to Destination" or the message ignored.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 15	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	Construct and send an IAM with missing mandatory parameters.	
Test Case: 16	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	Using a TPSA test tool, construct and send an IAM with duplicate parameters.	
Test Case: 17	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	The 4 bit SI and 2 bit NI are included in the SIO and are used within an SP's distribution function to determine the "User" to which the incoming message should be delivered. The SI will determine the "User," e.g., SCCP or ISUP, and the NI will determine which network is concerned, e.g., international or national. 1. Build and send an IAM message containing all valid call information; however, the Service Indicator is set to something other then ISUP. 2. A RELease should be returned with a cause value indicating the type of failure.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 18	**Vulnerability:** An adversary can inject invalid SS7 messages toward the RTS SS7 network, possibly causing a DoS or other service interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG shall generate an event notification to the RTS Management System when an outgoing SS7 message fails MTP routing procedures because its routing label DPC does not match a configured destination/route set in the SG's configuration management database, or its Status Indication Out-of Alignment contains an invalid NIC, indicating an MTP network not recognized by the SG. The event notification shall include the following information: 1. The alarm priority for a major alarm. 2. The error condition: • Invalid DPC. • Invalid network indicator. 3. The invalid message's routing label OPC, in terms of the decimal values of its NI, NC, and NCM subfields. 4. The invalid message's routing label DPC, in terms of the decimal values of its NI, NC, and NCM subfields. 5. The decimal value of the invalid message's SI. 6. The decimal value of the invalid message's network indicator. Such errors may occur due to translation errors within signaling applications at the CCA, which issue transfer requests to the SG via the CCA-SG interface, including parameters used to populate the outgoing SS7 message's DPC and NIC. If such errors occur, they can be expected to occur for large numbers of outbound SS7 messages. Therefore, the SG will need to provide a mechanism to throttle the generation of the event notification messages when these events occur.	1. Using a TPSA test tool, create and send the following ISUP messages to the SG: • IAM with invalid DPC • IAM with invalid SIO NI octet • IAM with invalid Network Indicator • IAM with invalid OPC (decimal value) • IAM with invalid DPC (decimal value) • IAM with invalid SI • IAM with invalid Network Indicator (decimal value) 2. Confirm that the SG responds to the invalid IAM's with a RELease message and no other adverse effects.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 19	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	1. Send an IAM with SIO sub-service indicating international and the OPC is spoofed. 2. Verify that the SG handles the attempted DoS gracefully.	
Test Case: 20	**Vulnerability:** An adversary could send SS7 messages toward the RTS SS7 network to cause DoS or other SS7 network interruptions. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.6.1 R-51 ANSI T1.111 **IA Control:** DCSQ-1 and VIVM-1	The SG and CCA shall support procedures to identify unauthorized SS7 messages (i.e., screening procedures) specified in Chapter T1.111.5 Section 8 of ANSI T1.111 [1].	Construct and send an IAM with a total length greater than 256 bytes.	
Test Case: 21	**Vulnerability:** An adversary can inject SS7 messages toward an SG that are not meant for the SG, thereby causing service interruptions or DoS. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.3.4 R-17 **IA Control:** DCSR-2	The SG shall examine each message received to verify that the DPC is valid.	1. Using TPSA test tool, create and send messages to the SG that contain an invalid DPC. 2. Confirm there are no adverse affects from the SG and the messages are discarded.	
Test Case: 22	**Vulnerability:** The SG may not be aware of a User Part outage, thus causing unnecessary traffic to be sent to the affected user part. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.4.8 R-41 **IA Control:** DCSR-2	SG shall be capable of receiving and accepting valid UPU messages.	1. Using TPSA test tool, create UPU messages with the following characteristics: • An invalid OPC • An invalid DPC • A valid "Affected Point Code" • An invalid "Affected Point Code" 2. Verify that sending these UPU messages toward the SG will have no adverse affect on the SUT operationally.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 23	**Vulnerability:** If the SG looses connectivity to the CCA, it will not report the outage, thus causing a DoS to go unnoticed for an extended period. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** SG UCR 3.1.2.4.10 R-44 **IA Control:** DCSQ-1	The SG shall send the SIPO message on all SS7 links when loss of connectivity to the CCA is detected. The method for detecting this loss and performing this action is implementation dependent.	The TPSA test tool should be configured to monitor one of the SG's A-Links. Cause the SG to lose connectivity to the CCA. Confirm that the SG sends SIPO on both A-links.	
Test Case: 24	**Vulnerability:** The SG reacts unpredictably to malformed incoming SS7 messages. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** ANSI T1.111 **IA Control:** DCSQ-1	The following MTP parameters shall be checked during the screening process: • SIO • OPC • DPC • Affected Destination (in MTP management messages). • Heading Code (H0 and H1 codes for MTP management messages)	1. Using a TPSA test tool, create the following messages: • IAM with invalid SIO • IAM with invalid OPC • IAM with invalid DPC • TFR with invalid H0 • TFR with invalid H1 2. The SG should reject or ignore the invalid incoming messages.	
Test Case: 25	**Vulnerability:** The SG reacts unpredictably to malformed incoming SS7 messages, possibly causing a DoS.		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG, CCA **Reference:** ANSI T1.111 **IA Control:** DCSQ-1	The SG and the CCA shall support screening procedures to verify the validity of ISUP messages. This shall include: • Verifying that the Message Type field has a valid value. • Verifying whether the originating signaling point is allowed to send the specific message to the destination node.	1. Using TPSA test tool, create a message with an invalid message type. 2. When the message is sent to the SG, the SG should ignore or return a RELease message. 3. Create a message that contains an invalid OPC. 4. The SG should reject, ignore or send a RELease in response.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 26	**Vulnerability:** By flooding the SUT with IAM messages, an adversary may be able to perform a DoS. **Category**: Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG and CCA **Reference:** SG UCR 3.3.4 R-67 **IA Control:** DCSQ-1	The SG shall be able to detect when the resources associated with signaling message handling are in danger of becoming overloaded. The method used to detect overload, while supplier-dependent, shall be such that congestion controls can be performed by the SG. The following two congestion cases apply: • If congestion occurs for traffic directed towards the SS7 network (from the CCA), the SG shall execute congestion control procedures on the transport connection to the CCA. • If the congestion occurs for traffic directed toward the CCA (from the SS7 network), the SG shall execute the MTP Level 2 flow control procedures on the signaling links to the SS7 network nodes causing the congestion.	1. Verify that the SG/CCA can withstand DoS attacks that are being attempted by flooding the SS7 signal link with IAM messages. 2. Using TPSA test tool, attempt to perform a DoS by flooding the SG with IAM messages. 3. If enough traffic is being sent to the SG, the SG should execute congestion control.	
Test Case: 27	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA and MG **Reference:** NM UCR 4.4.2 R-41.2 **IA Control:** DCSQ-1	The CCA shall increment an "incorrect message" Performance Monitoring counter when the CCA receives a message that cannot be understood or does not permit a valid response to be formed and sent to a specific MG.	1. Using a TPSA test tool, force SS7 type signaling toward the CCA. The messages should be created such that the CCA cannot process the signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "incorrect message" count is incremented.	
Test Case: 28	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA) **Reference:** NM UCR 4.4.2 R-41.3 **IA Control:** DCSQ-1	The CCA shall increment an "invalid message" Performance Monitoring counter when the CCA receives a transaction request or message which is invalid or cannot be successfully acted upon, but for which a valid response can be directed to the transmitting MG.	1. Using the a TPSA test tool, force SS7 type signaling toward the CCA. The messages should be created such that the CCA can process the invalid signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "invalid message" count is incremented.	
Test Case: 29	**Vulnerability:** If an SS7 outage occurs because of STP isolation, the outage can go unnoticed because of the lack of event notification, in essence causing an extended major DoS. **Category:** High		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: SG **Reference:** NM UCR 5.3.2 R-72.1 **IA Control:** DCSQ-1	The SG shall generate an event notification to the RTS Management System immediately when it becomes isolated from both member STPs of its serving STP pair, as a result of simultaneous link set outages on both A-link sets. The event notification shall be generated as a critical alarm.	Confirm that removing the A-link connections from the SG will result in a real-time notification alarm to the RTS Management System.	

Table E-15. SS7 Protocol Security Analysis (continued)

Test Case: 30	**Vulnerability**: Improperly coded ISUP messages cause a Denial of Service or other system disruption. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: LSC, MFSS, and MG **Reference:** AdHoc functional protocol testing. **IA Control:** DCSQ-1	Functional protocol testing, also known as "black-box testing" or "fuzzing," sends many diverse input messages to a vendor's implementation, exercising error handling routines and generating conditions never anticipated by the protocol designers or software developers. Fuzzers systematically send test messages, randomly or sequentially, within the framework defined by a given protocol specification. The implementation undergoing testing is observed for buffer overflows, unhandled exceptions and unexpected behavior.	1. Using a TPSA test tool, force SS7 ISUP type signaling toward the SUT. Scripts that test the most critical fields of the IAM message should be used. 2. Expect the SUT to react gracefully to the invalid signaling.	

LEGEND:

ANSI	American National Standards Institute	NCM	Network Cluster Member
AS-SIP	Assured Services-Session Initiation Protocol	NI	Network Indicator
CCA	Clear Channel Assessment	NIC	Network Interface Card
CCS7	Common Channel signaling System 7	NM	Network Management
CGB	Consumer and Governmental Affairs Bureau	OPC	Originating Point Code
COO	Cell Of Origin	RSC	Re-Set Circuit
DCSQ	Demand Control Support Questionnaire	RTS	Real Time Services
DCSR	Design Configuration Specific Robustness	SCCP	Simple Client Control Protocol
DoS	Denial of Service	SG	Signaling Gateway
DPC	Destination Point Code	SI	Service Indicator
ECO	Emergency Changeover Order	SIO	Service Information Octet
GRS	Group Re-Set	SIP	Session Initiation Protocol
H0	Heading Code 0	SIPO	Serial In Parallel Out
H1	Heading Code 1	SS7	Signaling System 7
IA	Information Assurance	SSP	Service Switching Point
IAM	Initial Address Message	STP	Signal Transfer Point
ISDN	Integrated Services Digital Network	SUT	System Under Test
ISUP	ISDN User Part	TFC	Transfer Controlled
IWF	Internetworking Function	TFP	Tops Filing Protocol
LIN	Location Identification Number	TFR	Time-Frequency Representation
LSC	Local Call Controller	UCR	Unified Capabilities Requirements
MFSS	Multifunction Softswitch	UPU	User Part Unavailable
MG	Media Gateway	VIVM	Vendor Independent Messaging Interface
MSU	Message Signal Unit		
MTP	Message Transfer Protocol		
NC	Network Cluster		

Table E-16. ISDN Protocol Security Analysis

Test Case: 1	Vulnerability: NA - For reference only.		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA, MGC, and MG **Reference:** CCA UCR 3.3.2 R-189	The MGC shall use the following protocol stack to support encapsulation of ISDN PRI signaling messages sent from the MGC to the MG, and de-encapsulation of ISDN PRI signaling messages sent from the MG to the MGC: • National ISDN PRI signaling messages, as described in Telcordia SR-4994. • IUA frames, where IUA shall be supported as defined in IETF RFC 4233, ISDN Q.921-User Adaptation Layer, January 2006. • Use one of the following IETF-standard Transport Layer Protocols: TCP, UDP or SCTP. Note that GR-3051-CORE uses SCTP to transport ISDN PRI messages within IUA frames. IPsec packets, secured using mutual MGC and MG encryption, at the IP Network Layer. This encryption shall be performed consistent with the MGC and MG encryption of H.248 messages described in the IA UCR.	NA	
Test Case: 2	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA and MG **Reference:** NM UCR 4.4.2 R-41.2 **IA Control:** DCSQ-1	The CCA shall increment an "incorrect message" Performance Monitoring counter when the CCA receives a message that cannot be understood or does not permit a valid response to be formed and sent to a specific MG.	1. Using TPSA test tool, force PRI type signaling toward the CCA. The messages should be created such that the CCA cannot process the signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "incorrect message" count is incremented.	
Test Case: 3	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA) **Reference:** NM UCR 4.4.2 R-41.3 **IA Control:** DCSQ-1	The CCA shall increment an "invalid message" Performance Monitoring counter when the CCA receives a transaction request or message which is invalid or cannot be successfully acted upon, but for which a valid response can be directed to the transmitting MG.	1. Using a TPSA test tool, force PRI type signaling toward the CCA. The messages should be created such that the CCA can process the invalid signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "invalid message" count is incremented.	

Table E-16. ISDN Protocol Security Analysis (continued)

Test Case: 4	**Vulnerability:** Improperly coded ISDN Q.931 messages cause a DoS or other system disruption. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: LSC, MFSS, and MG **Reference:** AdHoc functional protocol testing. **IA Control:** DCSQ-1	Functional protocol testing, also known as "black-box testing" or "fuzzing," sends many diverse input messages to a vendor's implementation, exercising error handling routines and generating conditions never anticipated by the protocol designers or software developers. Fuzzers systematically send test messages, randomly or sequentially, within the framework defined by a given protocol specification. The implementation undergoing testing is observed for buffer overflows, unhandled exceptions and unexpected behavior.	1. Using a TPSA test tool, force PRI type signaling toward the SUT. Scripts that test the most critical fields of the Q.931 protocol messages should be used. 2. Expect the SUT to react gracefully to the invalid signaling.	

LEGEND:

CCA	Clear Channel Assessment	NA	Not Applicable
DCSQ	Design Configuration Software Quality	NM	Network Management
DoS	Denial of Service	PRI	Primary Rate Interface
GR	Generic Requirement	Q.921	ISDN Q-921-User Adaptation Layer
H.248	Gateway Control Protocol	Q.931	User Signaling Bearer Service
IA	Information Assurance	RFC	Request For Comment
IETF	Internet Engineering Task Force	SCTP	Stream Control Transmission Protocol
IP	Internet Protocol	SR	Signaling Rate
IPsec	IP Security	SUT	System Under Test
ISDN	Integrated Services Digital Network	TCP	Transmission Control Protocol
IUA	ISDN User Adaptation	TDM	Time Division Multiplexing/Multiplexer
LSC	Local Session Controller	TPSA	TDM Protocol Security Analysis
MFSS	Multifunction Softswitch	UCR	Unified Capabilities Requirements
MG	Media Gateway	UDP	User Datagram Protocol
MGC	Media Gateway Controller		

Table E-17. CAS Protocol Security Analysis

Test Case: 1	**Vulnerability:** Inconsistent CAS signaling to the CCA IWF can result in DoS or other operational errors. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA (MG and IWF) **Reference:** CCA UCR 3.3.2 R-31 ARTS UCR **IA Control:** DCSQ-1	The CCA IWF shall support reception of CAS signaling sequences (Supervisory, Control, and Alerting) from the MG, and transmission of CAS signaling sequences to the MG. The mechanisms that the IWF uses to transfer CAS signaling sequences between the IWF and the MG (i.e., use of vendor-proprietary protocols with security protection, or use of ITU-T H.248 Gateway Control Protocol over Transport Layer Protocols over IPsec) are described in the MG chapter of the ARTS UCR.	Configure a CAS signaling trunk on a TPSA test tool. Cause the TPSA test tool CAS trunk to send inconsistent signaling data to the CCA/IWF. Confirm that the CCA/IWF treats the signaling irregularity in a graceful manner.	
Test Case: 2	**Vulnerability:** Inconsistent CAS signaling toward the MGC could result in DoS or other system disruptions. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MGC and MG **Reference:** CCA UCR 3.2.3 R-165 **IA Control:** DCSQ-1	The MGC shall support the following set of CAS trunk signals: • Seizure signal. A signal, sent from the originating switching system [or MGC/MG] to the terminating switching system [or MGC/MG], that defines the transition from the trunk idle state to the trunk seizure state. • Addressing control signal. A signal that marks the transition from the seizure state to the addressing state. Two addressing control methods of operation exist: ○ Wink Start. After receiving a seizure signal, the terminating switching system [or MGC/MG] sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information. ○ Immediate-Dial. No addressing control signal is used. The originating switching system [or MGC/MG] waits for a specified time after sending a seizure signal before sending the first address digit. • Answer signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state) • Transfer of address digits using DTMF signaling (for DTMF trunk groups). • Transfer of address digits using MF signaling (for MF trunk groups). • Disconnect signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.	**A TPSA test tool will be used to simulate a T1 CAS E&M Wink Start trunk that terminates on the MGC/MG.** 1. Configure a TPSA test tool T1 as a CAS E&M Wink Start trunk. 2. From the TPSA test tool, send multiple seizure signals towards the MG. 3. Verify the MGC processes the multiple seizures gracefully. 4. From the TPSA test tool, send a single seizure signal to the MGC. 5. Expect to receive an off-hook (wink) signal from the MGC. 6. From the TPSA test tool, send an invalid address signal toward the MGC. 7. Expect the MGC to process the inconsistent address signal in a graceful manner.	

Table E-17. CAS Protocol Security Analysis (continued)

Test Case: 3	**Vulnerability:** Inconsistent CAS signaling toward the MGC could result in a DoS or other system disruptions. **Category:** Medium		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MG and MGC **Reference:** MG UCR 3.4.3 R-110 **IA Control:** DCSQ-1	The MGC shall support the following set of CAS trunk signals, consistent with their use in Telcordia GR-3055-CORE (for the MG) and GR-3051-CORE (for the MGC): • Seizure signal. A signal, sent from the originating switching system [or MGC/MG] to the terminating switching system [or MGC/MG], that defines the transition from the trunk idle state to the trunk seizure state. • Addressing control signal. A signal that marks the transition from the seizure state to the addressing state). Two addressing control methods of operation exist: o Wink Start: After receiving a seizure signal, the terminating switching system [or MGC/MG] sends an off-hook signal with a defined duration (wink) to indicate that it is prepared to receive address information. o Immediate-Dial: No addressing control signal is used. The originating switching system [or MGC/MG] waits for a specified time after sending a seizure signal before sending the first address digit. • Answer signal. A signal that defines the transition from the call-processing state to the communications state, and persists for the duration of the communications state. • Transfer of address digits using DTMF signaling (for DTMF trunk groups). • Transfer of address digits using MF signaling (for MF trunk groups). • Disconnect signal. A signal that defines the transition from the call-processing state or the communications state to the idle state.	**A TPSA test tool will be used to simulate a T1 CAS E&M Wink Start trunk that terminates on the MGC/MG.** 1. Configure a TPSA test tool T1 as a CAS E&M Wink Start trunk. 2. From the TPSA test tool, send multiple seizure signals towards the MGC. 3. Verify the MGC processes the multiple seizures gracefully. 4. From the TPSA test tool, send a single seizure signal to the MGC. 5. Expect to receive an off-hook (wink) signal from the MGC. 6. From the TPSA test tool, send an invalid address signal toward the MGC. 7. Expect the MGC to process the inconsistent address signal in a graceful manner.	

Table E-17. CAS Protocol Security Analysis (continued)

Test Case: 4	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: CCA and MG **Reference:** NM UCR 4.4.2 R-41.2 **IA Control:** DCSQ-1	The CCA shall increment an "incorrect message" Performance Monitoring counter when the CCA receives a message that cannot be understood or does not permit a valid response to be formed and sent to a specific MG.	1. Using a TPSA test tool, force CAS-type signaling toward the CCA. The messages should be created that the CCA cannot process the signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "incorrect message" count is incremented.	
Test Case: 5	**Vulnerability:** Incorrect messaging can go undetected if not logged, thereby allowing an adversary to continue malicious activity. **Category:** Low		
Test Information	**Requirement**	**Test Procedure**	**Results**
Systems Affected: MFSS (CCA) **Reference:** NM UCR 4.4.2 R-41.3 **IA Control:** DCSQ-1	The CCA shall increment an "invalid message" Performance Monitoring counter when the CCA receives a transaction request or message that is invalid or cannot be successfully acted upon, but for which a valid response can be directed to the transmitting MG.	1. Using TPSA test tool, force CAS type signaling toward the CCA. The messages should be created such that the CCA can process the invalid signaling. 2. Expect the CCA to drop the incoming signaling with no adverse affects. 3. The "invalid message" count is incremented.	

LEGEND:

ARTS	Assured Reat Time Services	IWF	InterWorking Feature
CAS	Channel Associated Signaling	MF	Multifrequency
CCA	Call Control Agent	MFSS	Mutlifunction Soft Switch
DCSQ	Design Configuration Software Quality	MG	Media Gateway
DoS	Denial of Service	MGC	Media Gateway Control
DTMF	Dual Tone Multi-Frequency	NM	Network Management
E&M	Ear & Mouth (telephone signaling)	T1	T-Carrier 1
GR	Generic Requirement	TPSA	TDM Protocol Security Analysis
IA	Information Assurance	UCR	Unified Capabilities Requirements
IPsec	Internet Protocol Security		
ITU-T	International Telecommunications Union - Telecommunications		

E-7 INTERNET PROTOCOL VULNERABILITY (IPV) TESTING/PROTOCOL ANALYSIS (PA)

E-7.1 Background. The Global Information Grid GNTF's mission is to enhance the product's IA posture and readiness, as well as their Defense-in-Depth strategy. The JITC conducts vulnerability assessments and penetration testing of vendors' products before they undergo interoperability certification. Program managers or DoD agencies must obtain IA accreditation for their new telecommunication equipment for which DSN connectivity is planned or for existing DSN telecommunication equipment that has planned upgrades, systems that are UC, and the RTS systems. The IPV testing is conducted in accordance with the recommendations contained in the NIST Special Publication 800-42: "Guideline on Network Security Testing." The system will be evaluated for its ability to maintain confidentiality, integrity, and availability derived from FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

E-7.2 Purpose. The purpose of the IPV test plan is to provide a consistent set of guidelines for testers and developers to evaluate the operation of any switch system to their applicable STIG (Phase I IA Test), IA Requirements (Phase I IA Test), and IPV (Phase II IA Test) requirements. To address IT (hardware/software), the JITC IATT performs a systematic examination of vendor products to determine compliance with IA vulnerability management documents, including alerts, bulletins, technical guidance, and STIGs.

E-7.3 Functionality Test Procedures. The first step in conducting a vulnerability test is to perform a functionality check. Testing the SUT's functionality ensures that the product operates as intended in a fielded environment. Perform the functionality test at the beginning of Phase II testing to ensure that all services and applications are functioning and communicating correctly. Functionality testing varies from system to system and targets the basic operational functions. It is not meant to be a substitute for an interoperability test.

Some products, such as CPE, rely on external systems to exercise their capabilities. For example, a secure modem solution is inactive until an external switch initiates a call. In this case, the external switch is outside the scope of the IA test. However, the tester and vendor must ensure the external switch is operational to perform IPV testing on the secure modem solution. Functionality tests are performed before Phase II testing begins, and then again at the conclusion of Phase II testing. Monitor IP traffic during the functionality test and save the results for further evaluation, if necessary. The objective is to ensure that the SUT is functionally operational before Phase II IPV testing commences.

The IPV testing should be performed from the external or outside perspective and from the internal or inside perspective. An inside perspective is analogous to what a "trusted insider" or an employee has, or the same as an attacker would have once perimeter defenses (firewalls) are breached. An outside perspective is analogous to the

same perspective someone would have on the Internet, looking in at the system. The attacker would have the perspective of an "untrusted outsider" and would be looking in at the product. The following DoDI 8500.2 IA Controls apply to all the IPV testing procedures: DCPP-1, ECVI-1, ECTM-2, VIVM-1, and ECMT-1.

E-7.4 Internet Protocol Interface Identification. Verify operational and identify all IP interfaces.

E-7.5 Lines. If the SUT supports lines, the following manual calls are attempted: Analog to Analog, IP to IP, Analog to IP, and IP to Analog. Verify that all test calls can be completed successfully.

E-7.6 Trunks. If the SUT supports trunks, the following manual calls are attempted: Analog over trunk and IP over trunk. Verify that all test calls can be completed successfully.

E-7.7 Internet Protocol Handsets. All IP handsets are identified and the protocols used identified (e.g., Session Initiation Protocol (SIP) and Simple Client Control Protocol (SCCP)).

E-8 SUT TEST PROCEDURES

E-8.1 Test Perspectives. The IPV and PA testing are performed from an external and internal perspective. An external perspective is what someone on the Internet, DISA Network, or Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) would see from outside the network (i.e., an attacker looking in at the network's outer perimeter defenses, such as a firewall and/or router with an ACL). An internal perspective is what someone would see from inside the system (i.e., a trusted employee, a client user, or an attacker who has breached the firewalls). This method of testing can be found in section 3 of the NIST Special Publication 800-42, Guideline on Network Security Testing. The following DoDI 8500.2 IA Controls apply to all of the IPV testing procedures: DCPP-1, ECVI-1, ECTM-2, VIVM-1, and ECMT-1.

E-8.2 Host Discovery. Detecting all possible hosts in use by the SUT and their corresponding IP address information is the first step in the technical evaluation. Although the product vendor provides the IP address information, the test team ensures that there are no other undocumented IP-routable addresses. In addition to physical host network adapters, an IP address can be discovered from a variety of sources. Such sources include virtual Ethernet adapters, virtual machine addresses, and host-based network addresses, which could all create possible vulnerabilities in the SUT. The following are general techniques that are used to discover available hosts, an IP address, or any other IP-routable end-points.

E-8.3 Ping Sweep. A general Packet Internet Groper (Ping) sweep determines what hosts are available via the Internet Control Message Protocol (ICMP) message.

This is generally an ICMP echo request (type 8) to elicit an ICMP echo reply (type 0) from a host.

Table E-18 shows the Ping sweep test procedures, which use the following testing components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-18. Ping Sweep Test Procedures

Procedure	Results
Configure IP vulnerability testing laptop. Ethernet connection: An Ethernet port on the SUT, with its associated IP address, should be available for test purposes. The port location should be such that access to the largest number of IP addresses within the solution is possible. Use of an Ethernet hub is the preferred method of connection.	The IP test laptop and the IP interfaces under test are cabled to the Ethernet hub.
Assign IP address: An IP address and Subnet mask will be assigned to the laptop NIC that is within the range being used by the SUT.	The IP test laptop is configured with an IP address that is included within the Subnet range of the SUT. The use of the "Ping" command verifies that the test laptop can communicate with the SUT.
Host Discovery: A general ICMP (Ping) sweep of the entire subnet will be conducted to discover any devices within the SUT that respond to an ICMP. The following is an example of a ping sweep of a standard class C IP address range using NMAP: #NMAP –sP –n 192.168.1.1-254	The results returned by the ICMP Ping sweep will include all available hosts within the subnet.
Eliminate "out of bounds" components: Items such as gateways, network elements, or end-points that are outside the IA test boundary will be removed from the discovery findings and a list of discovered hosts will be established.	An evaluation of the returned results will eliminate all components that are considered "out of the test boundary" for the SUT.

LEGEND:

IA	Information Assurance	NMAP	Networked Messaging Application Protocol
ICMP	Internet Control Message Protocol	Ping	Packet Internet Groper
IP	Internet Protocol	SUT	System Under Test
NIC	Network Interface Card		

E-8.4 Transmission Control Protocol (TCP) Sweep. A TCP sweep provides insight into available hosts when the ICMP is disabled. A TCP sweep attempts to make TCP connections to a host range on a specified port list. In the process of the TCP sweep, a "three-way handshake" happens. The originator sends an initial packet called a "synchronize" to establish communication and "synchronize" sequence numbers in counting bytes of data that will be exchanged. The destination then sends a "SYN/ACK," which again "synchronizes" his byte count with the originator and acknowledges the initial packet. The originator then returns an "ACK," which acknowledges the packet the destination just sent to him. The connection is now "OPEN," and ongoing communication between the originator and the destination are permitted until one of them issues a FINish (FIN) packet or a Reset (RST) packet, or the connection times out. The "three-way handshake" establishes the communication.

By providing a list of possible ports that might be available within a system or product, the TCP connections are able to determine which hosts are up and available.

Common ports used in TCP sweeps include, but are not limited to, 21, 22, 23, 25, 54, 80, 137, 139, 443, and 445. Table E-19 shows the TCP sweep test procedures, which use the following components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-19. TCP Sweep Test Procedures

Procedure	Results
Host Discovery: A TCP sweep of the IP address space will be conducted to discover devices that are not responding to ICMP or might be using host-based firewalls or IDSs. The following is an example of a TCP ping sweep (System Ping) of a standard class C IP address range using NMAP: # NMAP –PS 21,22,23,25,53,80,137,139,443,445, and 2049 192.168.1.1-254	The results returned by the TCP sweep will include all available hosts within the subnet that did not respond to the ping sweep.
Eliminate "out of bounds" components: The list of hosts that responds to this sweep will be compared to the list of hosts defined in the ICMP sweep and any newly discovered host will be added to the list of known hosts.	An evaluation of the returned results will eliminate all components that are considered "out of bounds" for this test.
Additional Hosts: At this point, if the test team is satisfied that all the hosts are discovered, they could move to traffic analysis or they could use ACK scans, ARP scans, or alternate ICMP scans using different ICMP types.	Any additional hosts discovered should be confirmed to be part of the SUT.

LEGEND:

ACK	Acknowledge	NMAP	Networked Messaging Application Protocol
ARP	Address Resolution Protocol	SUT	System Under Test
ICMP	Internet Control Message Protocol	TCP	Transmission Control Protocol
IDS	Intrusion Detection System		
IP	Internet Protocol		

E-8.5 Traffic Analysis. Traffic analysis allows the test team to determine all the hosts that the SUT uses in an operational environment. Accessing the network traffic in transit provides an in-depth look at how information flows within the application and can also be helpful in revealing hosts that are part of the communications process. This process may require placing a network hub within the environment, network traffic flow, or possibly in the configuration of a mirror port on an existing network element. Table E-20 shows the traffic analysis test procedures, which use the following testing components: a laptop with a port scanning application installed, a laptop assigned with an IP address compliant with the test environment, and an Ethernet hub.

Table E-20. Traffic Analysis Test Procedures

Procedure	Results
Initialize Traffic Sniffer: A network analyzer such as *WireShark* (Ethereal) or *tcpdump* would be enabled to view all the network traffic and ensure that data was not traveling to devices that were not detected by the scanning and sweeping methods.	Confirm that all network traffic being generated and passed is between components of the System Under Test only.
Additional Hosts: If any new hosts are discovered during the traffic analysis phase of testing, they will be added to the list of auditable end-points, generally in a text file for the Phase II evaluation.	Any additional hosts discovered should be confirmed to be part of the System Under Test.

E-8.6 Port Enumeration. Port enumeration provides a list of services or applications running on the host and gives the tester a good indication of what operating system might be present on the end-point. When all the hosts in use by the SUT are determined, testers begin the initial evaluation of individual hosts. Each host is individually inspected for all available information, such as running services, operating system versions, and other applications. Information provided by investigating each device in depth helps determine how susceptible an individual component of the SUT might be to a potential attack.

Enumeration, provided by port scanning of each host, provides a detailed list of which ports are open, closed, or filtered on a specified host. Port scans are conducted in a multitude of varieties using many different protocols, packet flags, and techniques. These various scans can yield different results in different situations, depending on the configurations and protections of each host. Additional Open Source Security Testing Methodology Manual (OSSTMM) strategies are in Appendices B and E.

Table E-21 shows the port enumeration test procedures, which use the following testing components: a laptop with a port scanning application installed, an assigned IP address compliant with the test environment, and an Ethernet hub.

Table E-21. Port Enumeration Test Procedures

Procedure	Results
Available Hosts	During previous host discovery, the list of auditable components was defined and recorded.
Perform TCP/UDP Scan: A full TCP/UDP port scan will be completed on the known hosts to determine what services are available for further analysis. The following is an example of general TCP port scan of a list of know hosts: #NMAP –sS –n –P0 –p1- -iL test.ips.txt –oM 4amap.syn.txt –oA NMAP.syn.output.txt All ports, both TCP and UDP (65,535), should be scanned. (Note: There is a GUI available for the NMAP tool.)	The output of this scan will provide a list of open, closed, and filtered TCP ports for each host.
Perform UDP Scan: A full UDP scan will be completed to determine if there are any UDP services listening on the host. The following is an example of an UDP port scan regarding a list of known hosts: #NMAP –sU –p1- –host-timeout 300s –iL test.ips.txt –oM 4amap.udp.txt –oA NMAP.udp.output.txt	The output from this scan will provide a list of available UDP ports from the host list.
Operating System Enumeration: Another portion of detail that can be obtained during the port scan is the operating system. Generally during the Phase I process, the operating system is stated, but the ability to obtain the operating system type and version remotely can provide an attacker with added information. The following is an example of an operating system enumeration using xprobe: #xprobe –v –B –D 1 –D 2 192.168.1.100 NMAP can also be used to perform this function.	The results of this scan should reveal the operating system and version.
Additional Enumeration: At this point the tester may be satisfied with the data on available ports collected or may attempt to use other port scanning techniques suck as ACK scans, FIN scans, Null scans, or any other variety of techniques that might elicit a response from the host.	Not applicable

LEGEND:

ACK	Acknowledge	NMAP	Networked Messaging Application Protocol
FIN	Finished	TCP	Transfer Control Protocol
GUI	Graphical User Interface	UDP	User Datagram Protocol

E-8.7 Service Enumeration. Service enumeration determines what services are listening on an IP port of the SUT. Services and their versions can provide the tester with a list of known exploits or weakness that might be effective against a given target. Service enumeration takes many forms. Banner grabbing, which is another form of service enumeration, uses a specified application to match a service response to a known repository of responses. Those responses are then used to determine the service and its version. Banner grabbing might be as easy as using Telnet to connect to a port or opening a web browser to view a web-based application. Table E-22 shows the service enumeration test procedures using the list of open TCP ports as components.

Table E-22. Service Enumeration Test Procedures

Procedure	Results
1. Evaluate Open Ports: 2. Evaluate the open ports to determine what services are listening on each of the available ports. There are a number of applications that provide this function. The following is an example of a general service enumeration of a known list of hosts and ports: #amap –A –v –i 4amap.syn.txt another option would be: #NMAP –sV –p portlist.txt –iL test.ips.txt It is recommended that all TCP/UDP ports be scanned.	All ports that have services bound will be enumerated. Common services include those that can be found bound to TCP ports 1-1024. Custom services may be found on ports above 1024.
LEGEND: NMAP Networked Messaging Application Protocol UDP User Datagram Protocol TCP Transfer Control Protocol	

E-8.8 Service Analysis. Service analysis provides the test team with specific service details that could be used in attacking the system. When a service is known, a variety of checks may be completed against it. The list of possible checks is as large as the number of services that could run on a host. Examples include permission settings, authentication requirements, or information disclosure. Each of these checks is specific to the service. Table E-23 shows the service analysis test procedures using the list of available services as components.

Table E-23. Service Analysis Test Procedures

Procedure	Results
Service Analysis: 1. Upon determining the services available to be tested, the tester can perform services analysis. 2. Service analysis is wide ranging and the tools and techniques used are based on the services present. 3. The following is an example analysis of the SSH service running on a remote host. The telnet command provides a banner that identifies the service version, which can be compared to current versions and vulnerabilities. The second command attempts to authenticate with SSH v1, which is inherently weaker than Version 2: >telnet 192.168.1.100 22 SSH-1.99-OpenSSH_3.9p1 #ssh –1 192.168.100 The number of checks for service analysis is nearly limitless.	The IP vulnerability tester will analyze the results of the discovered services and determine if there are vulnerabilities associated with the service.
LEGEND: IP Internet Protocol SSH Secure Shell	

E-8.9 Vulnerability Assessment. A vulnerability assessment provides an automated process to determine if a system or application is vulnerable to attack. Vulnerability assessment tools provide the test team an automated process for taking the system and service enumeration information and matching it to known attacks. An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch, or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer

system or allowing privilege escalation or a DoS attack. Performing a vulnerability assessment manually, on a large scale, is time consuming; automated applications provide this information more efficiently. Although modern vulnerability scanners are extremely accurate, a vulnerability scanner's results are always analyzed by the test team to eliminate false positives and to ensure that findings are not overlooked.

E-8.10 Vulnerability Scan. A vulnerability scan checks remote targets for possible vulnerabilities. This automated process generally detects vulnerabilities on the host operating system and on many of the common applications that run on the host's operating systems. Some examples of common applications that are checked by a vulnerability scan are web services, mail applications, file transfer applications, and remote access applications, such as telnet or Secure Shell. Vulnerability scans take the response-and-discovery information they receive during a scan and match this information to a list of known attacks and exploits to determine what possible attacks could be executed against each host. Vulnerability scanners detect information from a remote target in various ways. Some scanners require local log-in credentials; others rely on services such as remote registry. Some rely solely on banner grabbing and port scans. Table E-24 shows the vulnerability assessment test procedures, which use open ports as input.

Table E-24. Vulnerability Assessment Test Procedures

Procedure	Results
1. The testing platform is connected to a port that is shared by the product under evaluation, much like the host discovery portion of the test. 2. Using the data collected from the host discovery and device investigation portion of the testing, the system configures a vulnerability scan with a vulnerability assessment application. 3. The configuration of the tool is set to one of several options depending on the test team's earlier discoveries. 4. The vulnerability scanner is configured to enable all checks, even the checks that could be considered harmful or cause denial of service. The tester then provides the known hosts and selects the known open ports on the target host and executes the assessment. 5. This procedure could be used with more than one vulnerability scanner and may require that user credentials be provided for the hosts depending on results desired from the test team.	The test team should evaluate the output of the scans to determine if the audit produced any false positives. The output of multiple vulnerability assessments is compared for like results and any variances. Any true positives should be further analyzed and documented. This information will be used during the exploitation and penetration testing phase.

E-8.11 User Application Assessment. The user application assessment provides detailed information about the host and its applications. The interface provides access to the system or access to data on the system. User interfaces, although convenient for users, can provide an attacker with a wealth of information about the remote host. Many techniques and tools are available for attempts to attack an application. An example of a possible attack on a user interface is a web attack that uses sequential or non-random session keys for users, allowing an attacker to reuse session keys or possibly cookies to access a site as an authorized user. Other times, interfaces do not protect the data they are sending and, while in transit, that information can be seen in the clear using a network sniffer device.

E-8.12 Application Assessment. The vulnerability assessment of an individual application is much like a general vulnerability assessment. However, in this case, the

scan is against a specific type of application, such as a web server or database application. Application vulnerability scanners use specific attacks associated with the types of applications they are designed to attack. Some very common application assessment tools include web services and database applications. Applications can be even more specialized for a specific type of web service or database, such as Microsoft Internet Information Service or an Oracle database. These tools look for specific vulnerabilities within their given applications. Unlike a network or system vulnerability scanner, application assessment tools know about a single application and nothing about other applications, except as they explicitly relate to the application within the scope of the tool. Additional testing procedures are available in Appendices B and E of this document. Table E-25 shows the application assessment test procedures using the following components:

- Web server IP
- Web application authentication information
- Web application vulnerability scanner

Table E-25. Application Assessment Test Procedures

Procedure	Results
1. The first step in application assessment would be to define the web applications that are present on the hosts. The service enumeration portion of the test provides this information. For each service listed, an application assessment tool is selected to perform a security evaluation. 2. The following command is executed using the web assessment tool Nikto to evaluate a singe host's web services on a given host: #perl nikto.pl –C all –port 80 –host 192.168.1.100 3. The following attempts to evaluate an Server Message Block administrator login with a list of passwords in a text file: #medusa –h 192.168.1.100 –u administrator –P passwords.txt –e ns –M smbnt As mentioned above, these are just examples of possible scenarios that the test team might attempt.	The test team should evaluate the output of the scans to determine if the audit produced any false positives.

E-8.13 DoS. Attempting a DoS attack determines the SUT's susceptibility to actions such as malformed packets or port message flooding. The testing team might take a particular end-point offline to capture one of its attributes, such as an IP address or a Media Access Control address. By knocking a node offline, the test team may be able to impersonate a device or receive traffic that was not intended for them. Another approach to a DoS attack is generating customized packets or streams of packets to be sent to a remote host. Some packets, such as fragmented, unsequential, or unacknowledged, may cause the network stack or some other functionality of the system to halt, thus creating a DoS attack against the system.

The specific procedure used for DoS testing varies and is generally dependent on both the SUT and the toolset used to exploit it. The following test procedures are meant to serve only as representative examples of DoS attacks and are not intended to

describe a comprehensive procedure for all types of DoS attacks. Table E-26 shows the DoS test procedures using the components listed below:

- A list of ports, protocols, and services identified as active on the SUT
- Known exploits (in the form of tools or scripts) against specific enumerated protocols and services

Table E-26. DoS Test Procedures

Procedure	Results
1. Search out and download exploits for various known vulnerabilities that affect major system resources, protocols, applications, and services. A variety of sources exist that contain scripts, tools, and procedures for exploiting known vulnerabilities that cause DoS in a variety of applications and operating systems. Examples of sources include insecure.org's "Exploit World" (http://www.insecure.org/sploits.html) and SecurityFocus (http://www.securityfocus.com/tools and http://www.securityfocus.com/pen-test). 2. Obtain a list of all active IP addresses and active ports and services on the SUT. 3. Using available exploit tools and scripts, set up a DoS attack against one or more of the SUT's active applications or services. An example of a DoS attack includes the following: SYN Flood Attack: Consists of sending one or more of the SUT's components a series of TCP SYN requests from a spoofed IP address, the goal being to overwhelm the target system with unanswered requests, thus causing the system to crash. Phreeon's BlitzNet script (available from http://www.megasecurity.org/DoS/blitznet.html) enables testers to conduct a SYN Flood Attack against a remote server from one or more computers without logging onto any of them. 4. Launch the DoS program against the remote host to be tested.	Depending upon whether or not the SUT has been correctly configured, the system resources of the component under attack will either become overwhelmed (leading to a system lock-up or crash) or will drop the fragmented packets and continue to operate with little or no impact on system resources. The Core Impact tool is recommended for automating this test.

LEGEND:

DoS	Denial of Service	SYN	Synchronize
IP	Internet Protocol	TCP	Transmission Control Protocol
SUT	System Under Test		

E-8.14 Exploitation. Exploitation will attempt to use any means at the test team's disposal to compromise the host. Exploitation is used not only to categorically verify that the vulnerability exists (and is not a false-positive), but also to gain visibility and access to hosts or data not initially accessible. Compromising the host can be as simple as accessing an account that uses a default or null password, or as complicated as creating a custom exploit script to exploit vulnerabilities in a software application. The list of techniques available to take control of a host is endless, with new and unique attacks being created daily.

The general procedure is determined, in part, by the results of enumeration and information gathering that was performed previously. The test team examines the list of known vulnerabilities and potential security holes on the various target hosts and determines which are most likely to be fruitful. Next, they exploit those vulnerabilities to gain illegal access to the target system.

E-8.15 Exploit Code. An exploit script is necessary to verify that vulnerabilities exist or to compromise the remote host. Using an exploit script can have negative effects on remote hosts, and it is generally not used freely outside a lab or a testing environment. An exploit script can be gathered from public channels on the Internet or created in-house by the testing team.

E-8.16 Injection. There are many different types of injection techniques and tools. One of the most common injection techniques is attempting Structured Query Language (SQL) injection through web interfaces that are supported by SQL back ends. During previous network and application analysis, the test team would discover and analyze vulnerabilities in application and network injection and, based on this data, would attempt to compromise the remote host. Table E-27 shows the exploitation and injection test procedures using the components listed below:

- List of possible vulnerable services found in previous tests
- Access to exploit code and/or procedures

Table E-27. Exploitation and Injection Test Procedures

Procedure	Results
1. Obtain a list of all active IP addresses and active ports and services on the SUT. Version numbers of the services found should be recorded. 2. Research and download exploits for the various known vulnerabilities that may affect the services that were previously found to be vulnerable. A variety of sources exist that contain scripts, tools, and procedures for exploiting known vulnerabilities that may cause security violations in a variety of applications and operating systems. Examples of sources include insecure.org's "Exploit World" (<http://www.insecure.org/sploits.html> and SecurityFocus (<http://www.securityfocus.com/tools> and <http://www.securityfocus.com/pen-test>). 3. Using available exploit tools and scripts, attempt to exploit the vulnerability on the affected component of the SUT. Depending on the type of vulnerability, exploitation may consist of running a generally available script, creating a new script, or manipulating a web based application in a fashion not intended during normal functioning of the SUT. There are many services that IP ports could be bound to. This test plan does not attempt to detail plans and procedures for each one. However, services like SQL, SSH, LDAP, and SNMP are just a few of the more popular services used on the equipment within the Defense Switched Network. 4. Launch the exploit against the service to be tested.	Depending on the type of vulnerability, the following actions may occur: 1. The tester may gain control of the system. 2. The system may become unresponsive. 3. The tester may obtain information from the SUT that would not normally be revealed.

LEGEND:

IP	Internet Protocol	SQL	Structured Query Language
LDAP	Lightweight Directory Access Protocol	SSH	Secure Shell
SNMP	Simple Network Management Protocol	SUT	System Under Test

E-8.17 Password Cracking. Password testing determines if a password's strength is sufficient, given the type of hashing or encryption used to protect the system. Testing or cracking encrypted or hashed passwords can be time consuming, depending on the source of the passwords. The test team uses several methods to test passwords. Many common user passwords can be determined by dictionary attacks

using common password validation tools such as *l0phtcrack* or *John the Ripper*. In situations where dictionary attacks are not sufficient, brute force and hybrid (brute force and dictionary) attacks may discover the password. Another technique is to compare the password hash to a known list of password hashes for a match. This list is commonly referred to as a rainbow table. Table E-28 shows the password cracking test procedures, which use the password file and hash components.

Table E-28. Password Cracking Test Procedures

Procedure	Results
1. Obtain the password file or password hashes from the host in question. This might require the password file on a windows box, the shadow file on a Linux machine, or a configuration file from a network element. 2. The procedure for obtaining these files may vary. The file may be provided by the vendor or copied after the host is compromised. 3. Evaluate the password file using an appropriate password cracking tool. The following command is an example of using *John the Ripper* to attempt a standard dictionary attack on a Linux shadow file: ./john –show –wordfile:dictionary.txt host.shadow For Session Initiation Protocol password cracking, tools such as svcrack or SIPtastic can be used.	The results may be a discovered password that is easily cracked. The absence of any results will indicate that a strong password policy is in effect.

E-9 SESSION INITIATION PROTOCOL (SIP) TEST PROCEDURES

The RTS task introduces a new protocol that is meant to replace existing TDM protocols. The SIP is an application-layer control (signaling) protocol used for originating, modifying, and terminating Internet telephone calls, multimedia distribution, and multimedia conferences.

In addition to the test cases mentioned above, new test cases were developed in the major areas of security concerns for SIP. These areas include Registration Hijacking, Server and End Instrument Impersonation, Message Tampering, Call Disruption, Denial of Service, and Eavesdropping. These test cases are by no means an exhaustive set of tests; rather, they focus on the “classic” threats that one could expect in a SIP network.

The protocol-specific SIP tests are developed from the “Real Time Services Information Assurance Generic System Requirements,” Section 7.1.2.

For a ROUTINE precedence RTS session, the system does not require user authentication; therefore, all SIP tests are attempted at the ROUTINE Precedence level unless noted otherwise. Some of the tools that can be used to perform these tests are described at http://www.voipsa.org/Resources/tools.php.

E-9.1 SIP Enumeration. Enumeration is a means to search for information to identify individual systems and network components, by examining the system as a total. Table E-29 shows the SIP Enumeration procedures.

Table E-29. SIP Enumeration

Procedure	Results
Test Description: The following procedure will enumerate the SIP devices within the subnet under test. The results should list all SIP devices located on the subnet. As other subnets containing SIP devices may be present in the system under test, this procedure should be followed for those subnets also.	
SIP Discovery: A sweep of the IP address space will be conducted to discover SIP devices. The following is an example of an Nmap scan of a standard class C IP address range: #NMAP–O –P0 192.168.1-254 The SiVus tool can also be used for discovery.	The results returned by Nmap will include all available SIP devices within the subnet. Open ports 5060 and 5061 indicate SIP devices are listening. Results will include SIP enabled phones as well as other SIP enabled appliances and devices.
Save the initial results.	The results of the Nmap or SiVus scans should be evaluated. An evaluation of the returned results will eliminate all components that are considered "out-of bounds" for this test. The SIP enabled devices returned in the Nmap scan should be documented for use in subsequent tests.
LEGEND: IP Internet Protocol Nmap Network Mapping Tool	 SIP Session Initiation Protocol SiVus SIP Vulnerability Scanner

E-9.2 SIP Vulnerability Assessment. A vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. Table E-30 details the SIP vulnerability assessment procedures.

Table E-30. SIP Vulnerability Assessment

Procedure	Results
Test Description: A vulnerability scan of the SIP subnet is performed. The SiVuS scanner provides features that allow the tester to verify the robustness and secure implementation of SIP components such as Proxies, Registrars, or phones (hard or soft).	
SIP enabled devices should be known from the previous Nmap scans.	IP addresses of SIP enabled devices should be documented and used in the following step:
Execute the SIP vulnerability scanner on those devices (subnets) that are SIP enabled. An example would be running SiVus.	Evaluate the results of the vulnerability scan to eliminate false positives. Relay remaining findings to the responsible vendor, and document them in the IA report.
Save the initial results.	
LEGEND: IA Information Assurance IP Internet Protocol	 SIP Session Initiation Protocol SiVus SIP Vulnerability Scanner

E-9.3 SIP Protocol Evaluation. Fuzzing is a kind of DoS attack in which an adversary sends malformed data packets to a SIP system, with the intention of causing it to crash. Table E-31 details SIP Fuzzing.

Table E-31. SIP Fuzzing

Procedure	Results
Test Description: In this test, the focus is set on a specific PDU, namely INVITE message. The rationale behind this selection was: • Two important SIP entity types, user agents (SIP phones) and proxies, have to support the INVITE-method. • SIP user agents and SIP proxies are by design ready to accept incoming invitations without prior session setup. This exposes a natural attack vector that should be scrutinized with top priority. • The INVITE-method contains a wide range of header-fields and may carry SDP data. Thus a considerable portion of the underlying code is exposed to testing via single PDU-type.	
1. The JAVA tool PROTOS will be used for this test. 2. Using the previous discovered SIP UAs and proxy servers, execute PROTOS on these devices. Detailed information on PROTOS can be obtained at: http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/	Summarize results from the test-runs herein. Tables represent the observations from feeding the test-material against the chosen subject software Present results in a tabular form with test cases divided into test-groups based on the exceptional element types used and PDU fields under examination. Each failed test case represents at minimum a denial of service type chance of exploiting the found vulnerability. In most cases, they represent memory corruption, stack corruption, or other fatal error conditions. Some of these may lead exposure to typical buffer overflow exploits, allowing running of arbitrary code or modification of the target system. Examine all failure cases for false positives. Document in the IA test report the remaining failures and relay them to the proper vendor representative.

LEGEND:

PDU	Protocol Data Unit	SIP	Session Initiation Protocol
PROTOS	Protocol Security Test Suite	UA	User Agent
SDP	Session Description Protocol		

E-9.4 Procedures for General Threats. General threats that could manifest on a SIP network include Eavesdropping, Corruption of data, DoS, Unauthorized access, Subscription fraud, Man-in-the-Middle attacks, and Replay attacks. Table E-32 details the procedures to eavesdrop on SIP transport data. Table E-33 details the procedures to corrupt a SIP subscriber's data, Table E-34 details the procedures to masquerade as valid subscriber, Table E-35 details procedures for eavesdropping on SIP signaling data, Table E-36 describes the procedures for corrupting a subscriber's signaling data, Table E-37 describes how to eavesdrop on the RTS network data, Table E-38 details procedures to corrupt RTS data, Table E-39 details how to attempt to obtain an RTS EI telephone number, Table E-40 describes how to create a SIP DoS, Table E-41 details creating a Man-in-the-Middle Attack, and Table E-42 describes attempting a replay attack.

Table E-32. Eavesdrop on a SIP Subscriber's Transport Data

Procedure	Results
Test Description: Information in SIP header fields is not encrypted. The information in the header fields should be evaluated and a determination should be made as to the vulnerability of the information obtained by sniffing the SIP traffic.	
1. Ensure that protocol sniffers such as WireShark, Cain, etc., are configured to listen on a subnet of the SIP subscribers.	Some traffic should be noticed on the monitored interface.
2. Originate multiple SIP calls and verify that the call traces are present in the above mentioned sniffers.	Evaluate the packet capture as to what information can be viewed. Voice traffic RTP should be available in the sniffer capture. A determination should be made as to the exposed information's value to a would-be adversary.
3. Save all scan results.	Document any abnormal traffic and report the results to the responsible vendor.
LEGEND: RTP Real Time Transport Protocol	SIP Session Initiation Protocol

Table E-33. Corrupt a SIP Subscriber's Transport Data

Procedure	Results
Test Description: Attempt to corrupt a valid SIP conversation by injecting RTP packets onto the RTP transport stream.	
1. Place a SIP call and leave call in the talking state.	The SIP call should be in a state where RTP traffic is recognized, using Wireshark to sniff the traffic.
2. Attempt to corrupt the RTP data stream. A tool such as rtpinjector can be used for this test.	Attempts to corrupt the voice stream should not be possible. Verify the SIP call is not interrupted.
LEGEND: RTP Real Time Transport Protocol	SIP Session Initiation Protocol

Table E-34. Masquerade as a Valid SIP Subscriber

Procedure	Results
Test Description: During a call involving SIP user-agent clients, an adversary could attempt to masquerade as a legitimate SIP user, forging the real identity of the client. Authentication provides a mechanism to verify that a user or client is legitimate. This is also known as registration hijacking.	
1. Using available tools such as SiVus, erase_registrations and add_registrations, attempt to masquerade as a legitimate SIP subscriber. 2. Ensure that the "From:" header information is that of an existing SIP client.	Verify that authentication mechanisms prevent masquerading or registration hijacking.
LEGEND: SIP Session Initiation Protocol	SiVus SIP Vulnerability Scanner

Table E-35. Eavesdrop on a SIP Subscriber's Signaling Data

Procedure	Results
Test Description: Information in SIP header fields is not encrypted. The information in the header fields should be evaluated and a determination should be made as to the vulnerability of the information obtained by sniffing the SIP traffic.	
1. Ensure that protocol sniffers such as WireShark, Cain, etc. are configured to listen on a subnet of the SIP subscribers.	Some traffic should be noticed on the monitored interface.
2. Originate multiple SIP calls and verify that the call traces are present in the above mentioned sniffers.	Evaluate the packet capture as to what information can be viewed. Determine the exposed information's value to a would-be adversary.
3. Save all sniffed packet information.	Document any abnormal traffic and report the results to the responsible vendor.
LEGEND: SIP Session Initiation Protocol	

Table E-36. Corrupt a SIP Subscriber's Signaling Data

Procedure	Results
Test Description: Attempt to corrupt a SIP subscriber's signaling data. This can include sending invalid data in the various SIP parameters. WireShark should be capturing packets during this test procedure.	
Using a tool such as Linkbit or SiVus, originate a SIP call that contains corrupt signaling data within the various SIP parameters.	Verify that the SIP calls are rejected because of corrupt packet information.
LEGEND: SIP Session Initiation Protocol	SiVus SIP Vulnerability Scanner

Table E-37. Eavesdrop on RTS Network Management Data

Procedure	Results
Test Description: The ability to sniff network management traffic may provide an adversary with useful information that he could use in subsequent attacks. The ADIMSS is the primary NMS for the DSN. This test will confirm the usage of authorized and secure protocols in the RTS ADIMSS NMS. This test procedure also applies to those RTS appliances that perform local management, including the management of the CCA, SG, MG, MFSS, SBC and EI's.	
Ensure that a protocol sniffer such as WireShark is configured to listen on a subnet of the RTS ADIMSS NMS.or the local management subnet.	Some traffic should be noticed on the monitored interface.
1. The vendor representative should perform management actions using the RTS ADIMSS. 2. Demonstrate locally performed administrative functions.	Confirm that all management functions are using secure protocols. Sniffing this IP traffic should not expose user ID's, passwords, or other information that could be used by an adversary for subsequent attacks
LEGEND: ADIMSS Advanced DSN Integrated Management Support System CCA Call Connection Agent DSN Defense Switched Network EI End-Instruments ID Identification IP Session Initiation Protocol	NMS Network Management System MFSS Multi-Function Soft Switch MG Media Gateway RTS Real Time Services SBC Session Border Controller SG Signaling Gateway

Table E-38. Corrupt RTS Network Management Data

Procedure	Results
Test Description: The corruption of network management type data can occur in two ways: by unauthorized access to an NMS database, or by corruption of NMS type messages in transit.	
1. Ensure that a protocol sniffer such as WireShark is configured to listen on a subnet of the RTS ADIMSS NMS or the local management subnet.	Some traffic should be noticed on the monitored interface.
2. The vendor representative should perform management actions using the RTS ADIMSS. 3. Administrative functions that are performed locally should also be demonstrated. 4. Generate corrupt type NMS messages and inject between monitored devices and NMS database.	Confirm that all management functions are using secure protocols. Sniffing this IP traffic should not expose user IDs, passwords, or other information that could be used by an adversary for subsequent attacks. Evaluate the packet capture as to what information can be viewed. Verify that NMS traffic is rejected because of corrupt packet information. Document any abnormal traffic and report the results to the responsible vendor.
LEGEND: ADIMSS Advanced DSN Integrated Management Support System ID Identification IP Internet Protocol	NMS Network Management System RTS Real Time Services

Table E-39. Attempt to Obtain an RTS End Instrument Telephone Number

Procedure	Results
Test Description: A malicious user who has access to the signaling traffic may be able to obtain the telephone number of the SIP phone and potentially the dialed numbers.	
Ensure that protocol sniffers such as WireShark, Cain, etc. are configured to listen on a subnet of the SIP subscribers.	Some traffic should be noticed on the monitored interface.
Originate multiple SIP calls and verify that the call traces are present in the above-mentioned sniffers.	Evaluate the packet capture as to what information can be viewed. Determine the exposed information's value to a would-be adversary.
Save all sniffed packet information.	Document any abnormal traffic and report the results to the responsible vendor.
LEGEND: SIP Session Initiation Protocol	RTS Real Time Services

Table E-40. SIP Denial of Service

Procedure	Results
Test Description: DoS attacks will be performed on all components of the RTS solution including the end instruments (SIP phones). DoS attacks should be attempted externally to the solution as well as internally.	
1. Verify that the RTS solution is in an operational state by performing various types of SIP calls including SIP to SIP, and SS7 to AS-SIP.	Confirm that all calls complete.
2. Attempt to cause a DoS on the components of the RTS using tools such as ISIC, INVITE and REGISTER Flooder, etc. SIP calls should be made during all attacks.	Confirm the success or failure to cause a DoS. Report successful DoS attacks to the component vendor and documented in the IA report.
LEGEND: AS-SIP Assured Services SIP DoS Denial of Service RTS Real Time Services	SIP Session Initiation Protocol SS7 Signaling System 7

Table E-41. Man-In-The-Middle Attack

Procedure	Results
Test Description: A man-in-the-middle attack (MITM) is an attack in which an adversary is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The test will attempt to configure an RTS-mitm-NMS scenario as well as an RTS-mitm-RTS scenario.	
1. Attempt a Man-In-The-Middle (MITM) attack for the purpose of spoofing and monitoring the actions of an NMS administrator. The MITM attack should try to configure the CCA to the right and an NMS device to the left. Cain or Ettercap are tools that can be used for this purpose.	Confirm that encryption for session streams as well as authentication and traffic segmentation (VLANs) prohibits a MITM attack.
2. Attempt a MITM attack for the purpose of spoofing and monitoring the actions of legitimate RTS users. The MITM attack should try to configure the EI-mitm-SIP Registrar. Cain or Ettercap are tools that can be used for this purpose.	Confirm that encryption for session streams as well as authentication and traffic segmentation (VLANs) prohibits a MITM attack.
LEGEND: MITM Man-in-the-Middle RTS Real Time Services	SIP Session Initiation Protocol VLAN Virtual Local Area Network

Table E-42. Attempt a Replay Attack (RTP and Signaling)

Procedure	Results
Test Description: A replay attack involves an adversary retransmitting a genuine message in order to establish authorized communication with the entity receiving the message. A replay attack is a common threat to the client-server systems that use messages as communication means	
1...Attempt to record an RTP stream of a valid SIP call. The Wireshark, rtptools utilities can be used to accomplish this. The call should remain up after recording a sufficient amount of conversation (1-2 mins).	The results should be a file that contains the entire voice call.
2. Attempt to replay the previous captured RTP stream by sending it to either of the above subscribers.	Interrupt current conversation with a new RTP stream.
3. Attempt to record an authenticated INVITE message; If the recording was successful, then change the Via and Contact headers to point to the attacker phone; the attacker sends the modified INVITE message to attempt to communicate with the callee.	The callee will assume the call is from a valid subscriber.
LEGEND: RTP Real Time Transport Protocol	

E-9.5 Subscriber Registration, De-Registration.

Table E-43 details the procedures to perform an illegal registration, and Table E-44 describes an illegal de-registration procedure.

Table E-43. Illegal Registration

Procedure	Results
Test Description: Registration hijacking occurs when an attacker impersonates a valid UA to a registrar and replaces the registration with its own address. This attack causes all incoming calls to be sent to the attacker. Registration hijacking allows inbound calls to be hijacked and answered by an attacker, which for example, could play a spoofed voice mail prompt. Registration hijacking also allows an attacker to "get in the middle" and record signaling and audio	
The hijack begins with the attacker sending a specially crafted REGISTER request to the target registrar, to unbind all existing registrations. The "Contact" header line contains the wildcard parameter (*) in conjunction with an "Expires" header line with the value 0 (zero). Together, these lines request the Registrar to remove all bindings for the target user address specified in the "To" header line.	If successful, the Registration hijacking will result in loss of calls to a targeted UA. This may be an individual user, group of users, or a high-traffic resource, such as a media gateway, AA, IVR, or voice mail system. By hijacking calls to a media gateway, all outbound calls can be blocked or otherwise manipulated.
If the registrar requires authentication, it replies to the REGISTER requests with a challenge. For username/password authentication, the registrar includes a nonce in the response, which the attacker uses to calculate a MD5 digest of the username/password.	
Once all legitimate contacts have been deleted, the attacker sends a second REGISTER message containing a new Contact header line with the attacker's address. An arbitrary Expires interval is requested in the Expires header line of the second REGISTER message (for example, 1 day).	If successful, the Registration hijacking will result in loss of calls to a targeted UA. This may be an individual user, group of users, or a high-traffic resource, such as a media gateway, AA, IVR, or voice mail system. By hijacking calls to a media gateway, all outbound calls can be blocked or otherwise manipulated.
LEGEND: AA Automated Attendant IVR Interactive voice Response MDS Message Digest Algorithm Five UA User Agent	

Table E-44. Illegal De-Registration

Procedure	Results
Test Description: This test will attempt to illegally de-register a valid SIP UA. This test can also be considered a DoS.	
1. Construct a "REGISTER" message with the EXPIRES header set to "0". The required header Fields such as To, From, etc., should contain valid information	The target of a successful attack will not be able to originate, nor terminate calls. The target will not have dial tone.
2. Send (inject) the message toward the SIP registrar.	

LEGEND:
DoS Denial of Service
SIP Session Initiation Protocol
UA User Agent

E-10. INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) PROCEDURES FOR SYSTEMS SERVICE IDENTIFICATION.

Testers may use the following OSSTMM strategies.

E-10.1 Expected Results:

- Open, closed, or filtered ports.
- IP addresses of live systems.
- Internal system network addressing.
- List of discovered tunneled and encapsulated protocols.
- List of discovered routing protocols supported.
- Active services.
- Service types.
- Service application type and patch level.
- Operating System type.
- Patch level.
- System type.
- List of live systems.
- Internal system network addressing.
- Network map.

E-10.2 Enumerate Systems:

- Collect broadcast responses from the network.
- Probe past the firewall with strategically set packet time to live settings (Firewalking) for all IP addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and acknowledge on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.

- Use Domain Name Server (DNS) connect attempts on all hosts in the network.
- Use File Transfer Protocol and Proxies to bounce scans to the inside of the Demilitarized Zone for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

E-10.3 Enumerating Ports:

- Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered on the default TCP testing ports for all the hosts in the network.
- Use TCP full connect scans to scan all ports up to 65,535 on all hosts in the network.
- Use TCP fragments in reverse order to enumerate ports and services for the subset of ports on the default packet fragment testing ports in Appendix B for all hosts in the network.
- Use User Datagram Protocol (UDP) scans to enumerate ports as being open or closed on the default UDP testing ports if UDP is **not** being filtered already. [Recommended: first test the packet filtering with a small subset of UDP ports.]

E-10.4 Verifying Various Protocol Response:

- Verify and examine the use of traffic and routing protocols.
- Verify and examine the use of non-standard protocols.
- Verify and examine the use of encrypted protocols.
- Verify and examine the use of TCP and ICMP over IP version 6 (IPv6).

E-10.5 Verifying Pack Level Response:

- Identify TCP sequence predictability.
- Identify TCP initial sequence numbers predictability.
- Identify IP identification sequence generation predictability.
- Identify system up-time.

E-10.6 Identifying Services:

- Match each open port to a service and protocol.
- Identify server uptime to latest patch releases.
- Identify the application behind the service and the patch level using banners or fingerprinting.
- Verify the application to the system and the version.
- Locate and identify service remapping or system redirects.
- Identify the components of the listening service.
- Use UDP-based service and trojan requests to all the systems in the network.

E-10.7 Identifying Systems:

- Examine system responses to determine operating system type and patch level.
- Examine application responses to determine operating system type and patch level.
- Verify the TCP sequence number prediction for each live host on the network.
- Match information gathered to system responses for more accurate results.

E-11 INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL PROCEDURES FOR INTERNET APPLICATION TESTING. Testers may use the following OSSTMM strategies:

E-11.1 Expected Results:

- Applications.
- Application components.
- Application vulnerabilities.
- Application system trusts.

E-11.2 Re-Engineering:

- Decompose or deconstruct the binary codes, if accessible.
- Determine the protocol specification of the server/client application.
- Determine program logic from the error/debug messages in the application output and program behavior/performance.

E-11.3 Authentication:

- Find possible brute force access points in the applications.
- Attempt a valid login credential with password grinding.
- Bypass authentication system with spoofed tokens.
- Bypass authentication system with replay authentication information.
- Determine the application logic to maintain the authentication session–number of (consecutive) failure logins allowed, login timeout, etc.
- Determine the limitations of access control in the applications–access permissions, login session duration, and idle duration.

E-11.4 Session Management:

- Determine the session management information–number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session Identification (ID) in Universal Resource Locator (URL) encoding string, session ID in hidden HyperText Markup Language (HTML) field variables, etc.

- Guess the session ID sequence and format.
- Determine the session ID is maintained with IP address information. Verify if the same session information can be retried and reused in another machine.
- Determine the session management limitations–bandwidth usages, file download/upload limitations, transaction limitations, etc.
- Gather excessive information with direct URL, direct instruction, action sequence jumping, and/or page skipping.
- Gather sensitive information with Man-In-the-Middle attacks.
- Inject excess/bogus information with session-hijacking techniques.
- Replay gathered information to fool the applications.

E-11.5 Input Manipulation:

- Find the limitations of the defined variables and protocol payload—data length, data type, construct format, etc.
- Use exceptionally long character-strings to find buffer overflow vulnerabilities in the applications.
- Concatenate commands in the input strings of the applications.
- Inject Structured Query Language in the input strings of database-tired web applications.
- Examine “cross-site scripting” in the web applications of the system.
- Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.
- Use specific URL-encoded strings and/or unicode-encoded strings to bypass input validation mechanisms of the applications.
- Execute remote commands through “server side include.”
- Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
- Manipulate the hidden field variable in the HTML forms to fool or modify the logic in the server-side web applications.
- Manipulate the “referrer,” “host,” etc., HyperText Transfer Protocol variables to fool or modify the logic in the server-side web applications.
- Use illogical input to test the application error-handling routines and to find useful debug/error messages from the applications.

E-11.6 Output Manipulation:

- Retrieve valuable information stored in the cookies.
- Retrieve valuable information from the client application cache.
- Retrieve valuable information stored in the serialized objects.
- Retrieve valuable information stored in the temporary files and objects.

E-11.7 Information Leakage:

- Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
- Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

E-12 OUT-BRIEF. At the conclusion of all phases of testing and once the vendor has provided mitigations to all open findings, the draft report is discussed with the vendor, IATT, sponsor, UCCO, and FSO. All findings are reviewed, questions about specific findings are discussed, and any outstanding issues are assigned as action items to the respective party. During the outbrief, the vendor, IATT, sponsor, UCCO, and FSO review the supplied network configuration, the hardware, and software to ensure that it is correct before accreditation consideration.

E-13 FINAL REPORT. Following the outbrief meeting and the completion of all action items, a final report is prepared and submitted for approval by the government. The IA task leader distributes copies to all parties, including the FSO for the CA. The CA will send a letter to the DISN Security Accreditation Working Group recommending that the SUT be placed on the APL. Scan and test results are provided with the recommendation letter as baseline examples for sites to use when assessing their solutions and creating their DIACAP artifacts.

APPENDIX F

REFERENCES

DEPARTMENT OF DEFENSE (DoD) DOCUMENTS

DoD Directive 8500.1 “Information Assurance (IA),” 24 October 2002

DoD Instruction (DoDI) 8500.2 “Information Assurance (IA) Implementation,” 6 February 2003

DoDI 8100.3, “Department of Defense Voice Networks,” 16 January 2004

DoDI 8551.1, “Port, Protocol and Services Management (PPSM),” 13 August 2004

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02B, “DISN Connection Policy, Responsibilities, and Processes,” 31 July 2003

CJCSI 6212.01E, “Interoperability and Supportability of Information Technology and National Security Systems,” 15 December 2008

CJCSI 6215.01B, “Policy for Department of Defense Voice Services,” 23 September 2001

CJCSI 6510.01D, “Information Assurance (IA) and Computer Network Defense (CND),” 15 June 2004

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Guidance, 28 November 2007

Assistant Secretary of Defense for Command, Control, Communications, Computers, and Intelligence/DoD Chief Information Officer Memorandum, Subject: “DoD Ports, Protocol, and Services Security Technical Guidance,” 5 November 2002

ETSI TS 165-1, “Telecommunications and Internet Protocol Harmonization over Networks (TIPHON),” Release 4; “Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis,” Version 4.1.1, 1 December 2003.

ETSI TS 102 165-2, “Telecommunications and Internet Protocol Harmonization over Networks (TIPHON),” Release 4; “Protocol Framework Definition; Methods and Protocols for Security; Part 2: Countermeasures,” Version 4.1.1, 1 December 2003.

Executive Order 12333, “United States Intelligence Activities,” 4 December 1981

Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, 25 May 2001

Gold Disk Users Guide: Basic Operations, Version 2.0, DISA Field Security Operations, July 2007

Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," May 2003

DEFENSE INFORMATION SYSTEMS AGENCY (DISA)/JOINT INTEROPERABILITY TEST COMMAND (JITC)

DISA, "Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR), Incorporated Change 1," 1 March 2005

DISA, Security Technical Implementation Guidelines (STIG)

JITC, "Defense Switched Network Generic Switch Test Plan (GSTP)," 23 April 2004

DISA, "Real Time Services (RTS) Unified Capabilities Requirements (UCR)," 2008

OTHER DOCUMENTS

American National Standard Institute (ANSI) T1.111 through T1.116, "Telecommunications Signaling System No. 7 (SS7)," 1992

Department of Defense Real-Time Services (RTS) UCR and Generic System Specifications (GSS) Appendices Overview, Revision 0.2, 16 August 2006.

National Institute of Standards and Technology (NIST), "Security Requirements for Cryptographic Modules," January 1994.

NIST, "Creating a Patch and Vulnerability Management Program version 2" Special Publication (SP) 800-40, November 2005

NIST, "Guideline on Network Security Testing" SP 800-42, October 2003

NIST, "Recommended Security Controls for Federal Information Systems" SP 800-53 February 2005, updated 17 June 2005

Telcordia, "GR-815-CORE," Issue 2, March 2002

APPENDIX G

POINTS OF CONTACT`

Napier, Michael JITC Action Officer	JITC ATTN: JTE/Napier 2001 Brainard Road/Bldg 57305 Fort Huachuca, AZ 85613 E-mail: Michael.Napier@disa.mil	(520) 538-6787 DSN 879-6787 Fax (520) 538-4347
Quick-Keckler, Donna RTS IA Test Manager	JITC ATTN: NGIT/Quick-Keckler 2001 Brainard Road Fort Huachuca, AZ 85613 E-mail: Donna.Quick-Keckler.ctr@disa.mil	(520) 538-4537 DSN 879-4537 Fax (520) 538-5258
Searle, Brent RTS IA Team Lead	JITC ATTN: NGIT/CSC/Searle 2001 Brainard Road Fort Huachuca, AZ 85613 E-mail: Brent.Searle.ctr@disa.mil	(520) 538-2591 DSN 879-2591 Fax (520) 538-5258

(The page intentionally left blank.)