FIRST DRAFT

VOICE VIDEO POLICY SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 0.1

19 June 2017

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

This Voice Video Policy Security Technical Implementation Guide (STIG) contains the architectural and policy requirements providing security guidance to voice and video systems operating over DoD IP networks. These systems consist of session managers, border controllers, gateways, and ancillary devices working together to provide voice over IP (VoIP), video-enhanced VoIP (VVoIP), unified capabilities (UC), and video conferencing (VC) services.

The Voice Video Policy STIG applies to the organizations and locations providing voice and video services within DoD. The specific scope includes, but is not limited to:

- Mission-critical communications
- Assured services (AS) considerations
- Defense Information Systems Network (DISN) voice precedence
- Mandatory boundary protections and network infrastructure augmentation
- Reliability, redundancy, and uptime system requirements
- Fire and emergency services (FES) requirements

The organizations and locations implementing this voice video policy guidance will also rely on several technical documents for the devices contained within the voice video systems being addressed. This document will coordinate with the Network Device Management (NDM) Security Requirements Guide (SRG), Voice Video Session Management SRG, Voice Video Endpoint SRG, Application Layer Gateway (ALG) SRG, and Network Infrastructure STIGs.

This Voice Video Policy STIG provides appropriate evaluation and remediation functions for organizations and locations deploying voice and video systems. The policy controls not included in this STIG may be addressed outside the scope of this document. Some policies outside of this document are set by DoD to be overarching, applying to all organizations and information systems. In some cases, DoD has determined that policy should be set at the Enterprise level. The guidance provided in this STIG addresses controls to be set by all organizations and locations in support of voice video systems.

1.2 Authority

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

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

1.3 Vulnerability Severity Category Code Definitions

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

Table 1-1: Vulnerability Severity Category Code Definitions

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

1.4 STIG Distribution

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

1.5 Document Revisions

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

1.6 Other Considerations

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

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

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

1.7 Product Approval Disclaimer

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

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

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

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

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The applicable baseline policy CCI requirements derived from the NIST SP 800-53 guidance and security best practice requirements are included in this STIG. To assess voice video components and systems, the following resources apply.

2.1.1 Voice Video Policy

The Voice Video Policy STIG addresses voice and video systems implemented by organizations and locations within DoD. This provides the policy and architectural guidance for VoIP systems (also referred to as UC systems or implementations) used to support the mission and business functions of the DoD. It also contains the policy and architectural guidance for VC systems used within DoD.

2.1.2 Network Device Management (NDM)

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

2.1.3 Voice Video Session Management

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

2.1.4 Voice Video Border Elements

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

2.1.5 Voice Video Endpoints

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

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Overview

Systems incorporating voice and video services have evolved from circuit-switched analog systems to efficient digital packet-switched networks as bandwidth and reliability improved. Addressing security concerns for current voice video systems operating on the DoD Information Network (DoDIN) requires an understanding of the architecture and how the various components communicate and relate to each other. The most common protocols used for communications of voice and video are SIP, H.323, and proprietary protocols such as SCCP and UNIStim.

3.2 Unified Capabilities (UC)

UC are the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. The DoD Unified Capabilities Requirements (UCR) specifies the technical requirements for certification of approved products to be used in DoD networks to provide end-to-end UC and is available for download from https://www.disa.mil/network-services/UCCO/Policies-and-Procedures.

3.2.1 Approved Products List (APL)

The DoDIN APL is established and mandated by DISA and DoD guidance. Its purpose is to maintain a single consolidated list of products that have completed interoperability and cybersecurity certification. DoD components must meet their system needs by only purchasing APL listed products, providing one of the listed products meets their needs. If no listed product meets the organization’s needs, they may sponsor a product for testing that does meet their needs.

3.3 Assured Services (AS)

The need for high availability and robustness, ensuring decision-making users have the capability to communicate, mandated the development of AS. The voice video system implementing AS uses several layers of support including network infrastructure, boundary protection, and protocols.

3.3.1 Assured Services Network Infrastructure

The network infrastructure supporting AS must provide a robust and redundant architecture to ensure operational communications meet stringent standards. All the network elements within the AS LAN must be supported by uninterrupted power supplies (UPS) of sufficient capability to ensure continuous service. Interconnections among access, distribution, and core switches must have multiple pathway links to prevent any single point of failure. The network boundary and transport must support DISA AS requirements and configurations.

3.3.2 Assured Services Session Initiation Protocol (AS-SIP)

AS-SIP builds on the IETF standard Session Initiation Protocol (SIP) to provide necessary end-to-end assured service over DoD networks. Implementing AS-SIP provides the capability for DISN voice precedence, ensuring military and civilian decision makers have uninterrupted, essential communications, especially during times of crisis. The specification requires using SRTP, TLS, and Differentiated Services Code Point (DSCP) and specifies how the protocol is implemented on both unclassified and classified networks.

3.4 DISN Voice Precedence

The organizations and locations supporting mission-critical communications must provide DISN voice precedence, permitting higher-precedence users to preempt lower-precedence sessions. For precedence, each user is designated with one of four categories: Flash/Flash Override (F/FO), Immediate/Priority (I/P), Routine (R), and non-mission critical/non-AS.

3.4.1 Flash/Flash Override (F/FO)

This is a special class of user with the highest access to DISN voice video service for origination and reception of essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crisis, pre-attack, and theater nonnuclear war communications for intelligence, alert, and strategic readiness. Requests for F/FO must be validated by the appropriate Combatant Command/ Services/Agencies (CC/S/A) and approved by the Joint Staff.

3.4.2 Immediate/Priority (I/P)

This class of user has the requirement to originate and receive mission-critical communications but does not meet the criteria for F/FO access. These users can exercise authority and direction as a Joint Staff or Combatant Command/Service/Agency (CC/S/A) designated commander over assigned and attached forces to accomplish missions. The use of I/P precedence by DoD personnel assigned to non-U.S. organizations must be approved by the appropriate CC/S/A.

3.4.3 Routine (R)

Users granted (R) precedence are those (regardless of the position in the chain of command) who issue or receive guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime.

3.4.4 Non-Mission Critical/Non-AS

This is a class of users with no missions or communications requirements to ever originate or receive mission-critical communications. During times of crisis or contingency, these users may be denied access to some features and capabilities to ensure the needs of higher-precedence users are met first. These users are not required to have AS.

Table 3-1: DISN Voice Precedence User Categories

	F/FO	I/P	R	Non-AS
Availability	99.999%	99.997%	99.9%	99.8%
UPS Battery Time	8-Hour UPS	2-Hour UPS	N/A	N/A
Redundancy	Required	Required	Optional	Optional
AS Network	Required	Required	Required	Optional

3.5 Fire and Emergency Services

The FCC requires interconnected VoIP telephone services using the Public Switched Telephone Network (PSTN) meet Enhanced 911 (E911) obligations. Fire and Emergency Services (FES) rely on E911 systems to automatically provide to emergency service personnel a 911 caller's callback number through Automatic Number Identification (ANI) and, in most cases, location information through extended Automatic Location Identification (ALI) information or access to an extended ALI database. Providing 911 service is mandatory and cannot be opted out.

To reduce possible risks to public safety, functionality supporting FES and E911 must be implemented for voice systems. Customers must have a clear understanding of the limitations, if any, of their 911 service. Labels warning customers must be used if 911 service is limited or not available, and customers must place the labels on or near equipment used with VoIP service. Calls must be routed to the Public Safety Answering Point (PSAP) in areas where emergency service providers are not capable of receiving or processing the location information or callback numbers not automatically transmitted with 911 calls.

3.6 Common Log Format

Logging of session events for SIP is best performed according to RFC 6873, which identifies the Common Log Format (CLF) for SIP. The CLF is analogous to the Call Detail Records (CDRs) used in packet-switch networks and provides a non-proprietary framework for logging essential session information. This CLF mimics the successful event logging format found in well-known web servers such as Apache, which provides familiarity for administrators. It allows session correlation across diverse processing elements. In operational SIP networks, a request will typically be processed by more than one SIP server, and the CLF allows the administrator to trace the progression of the requests as they traverse through the different servers, establishing a concise diagnostic trail of a SIP session.

4. REFERENCES

The following list of documents are applicable to supporting the many missions and business functions for Voice Video systems in DoD. This is not an exhaustive list but provides a first read of guidelines.

1. CJCSI 6211.02D, "Defense Information Systems Network (DISN) Responsibilities", 24 January 2012 (current as of 04 August 2015)
2. DoDI 8100.04, "DoD Unified Capabilities (UC)", 09 December 2010
3. DoD "Unified Capabilities Requirements 2013 (UCR 2013)", January 2013
4. CNSSI 5000, "Guidelines for Voice over Internet Protocol (VoIP)", August 2016
5. CNSSI 5001, "Type-Acceptance Program for Voice over Internet Protocol (VoIP) Telephones", December 2007
6. CNSSI 5007, "Telephone Security Equipment Submission and Evaluation Procedures", April 2013
7. IC Tech Spec-For ICD/ICS 705, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities", version 1.3, 10 September 2015
8. JAFAN 6/0 Manual, "Special Access Program Security Manual – Revision 1", 29 May 2008
9. JAFAN 6/9 Manual, "Physical Security Standards for Special Access Program Facilities", 23 March 2004

Note: The CJCSI 6215.01C contained the policy for DoD voice networks with real-time services. The CJCSI 6215.01C was cancelled by the CJCSI 6211.02D included above. The CJCSI 6215.01C definitions for Command and Control (C2) telecommunications and DSN multilevel precedence and preemption (MLPP) were not carried forward into the CJCSI 6211.01D. As defined in the CJCSI 6211.01D, DISN Voice Precedence replaces some of the functions previously defined as C2 and MLPP.