



# VIDEO TELE-CONFERENCE CHECKLIST

Version 1, Release 1.2

24 April 2009

**Developed by DISA for the DoD**

Database Reference Number: \_\_\_\_\_ CAT I: \_\_\_\_\_

Database entered by: \_\_\_\_\_ Date: \_\_\_\_\_ CAT II: \_\_\_\_\_

Technical Q/A by: \_\_\_\_\_ Date: \_\_\_\_\_ CAT III: \_\_\_\_\_

Total: \_\_\_\_\_

## **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 FSO of any non-Federal entity, event, product, service, or enterprise.

**UNCLASSIFIED UNTIL FILLED IN**  
**CIRCLE ONE**  
**FOR OFFICIAL USE ONLY (mark each page)**  
**CONFIDENTIAL and SECRET (mark each page and each finding)**

Classification is based on classification of system reviewed:

- Unclassified System = FOUO Checklist
- Confidential System = CONFIDENTIAL Checklist
- Secret System = SECRET Checklist
- Top Secret System = SECRET Checklist

**Review Information**

<b>Reviewer</b>				<b>Phone</b>		
<b>Previous SRR</b>	<b>Y N</b>	<b>Date of previous SRR</b>		<b>SO1 Available</b>	<b>Y N</b>	
<b>Number of current open Findings</b>						

**Site Information**

<b>Site Name</b>						
<b>Address</b>						
<b>Phone</b>						

**Contacts**

Position	Name	Phone Number	E-Mail Address	Responsibility
<b>IAM</b>				
<b>IAO</b>				

This page is intentionally left blank.

## **Document Change Log**

V1 R1.2 - 24 April 2009 – RTS-VTC 3420.00: DoD Logon “Electronic Notice (Warning) and Consent Banner” - Updated the discussion, check, and fix verbiage to reflect and update references to JTF-GNO CTO 08-008A and DoD CIO Memo, “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement”, dated 9 May 2008. Included the exact banner verbiage as required.

This page is intentionally left blank.

## TABLE OF CONTENTS

	Page
1. PROCEDURES FOR REGISTRATION OF VTC ASSETS IN THE VMS .....	9
1.1 Introduction .....	9
1.1.1 Pre - Requisites .....	9
1.2 VTC Asset Naming Convention .....	9
1.3 RTS Asset Identification .....	10
1.3.1 Local Management System(s) .....	10
1.3.2 Remote Management System(s) .....	10
1.3.3 BCPS LAN/CAN/BAN Infrastructure .....	11
1.3.4 RTS Adjunct/Auxiliary Systems/Devices .....	11
1.4 RTS Asset Creation in the VMS .....	11
1.4.1 The Organization, Site, and/or Location .....	11
1.5 Non-Computing Asset Creation .....	11
1.5.1 Computing Asset Creation .....	13
1.6 Creating Assets – Step-by-Step .....	14
1.6.1 Creating the NON-Computing Asset(s) .....	14
1.6.2 Creating the Computing Assets .....	15
1.6.3 Procedures for Updating the Vulnerability Status of the Asset .....	27
1.6.4 Verify that all necessary assets were reviewed .....	29
1.6.5 Add Comments to a Visit (Reviewer only) .....	30
1.7 Reports – Step-by-Step .....	30
1.7.1 Compliance Monitoring .....	30
1.7.2 Additional Reports .....	31
2 VULNERABILITIES AND IA REQUIREMENTS .....	33
RTS-VTC 1000.00 [IP][ISDN]; DoD Access Control and Auditing Policy Compliance .....	33
RTS-VTC 1020.00 [IP][ISDN]; Power-Off the VTU When Inactive .....	36
RTS-VTC 1025.00 [IP][ISDN]; Disable the VTU When Powered & Inactive .....	38
RTS-VTC 1027.00 [IP][ISDN]; Sleep Mode .....	40
RTS-VTC 1030.00 [IP][ISDN]; Incoming Call Notification .....	42
RTS-VTC 1040.00 [IP][ISDN]; Auto-Answer Availability .....	44
RTS-VTC 1060.00 [IP][ISDN]; Auto-Answer Use Mitigations .....	46
RTS-VTC 1080.01 [IP][ISDN][PC]; SOP Microphone Operation .....	48
RTS-VTC 1120.01 [IP][ISDN][PC]; SOP Camera Operation .....	50
RTS-VTC 1140.00 [IP][ISDN]; Incoming Calls While In a Conference .....	52
RTS-VTC 1160.00 [IP]; Disable VTU Remote Monitoring .....	54
RTS-VTC 1162.00 [IP]; VTU Remote Monitoring Password .....	55
RTS-VTC 1164.00 [IP][ISDN]; Remote Monitoring Notification .....	56
RTS-VTC 1168.00 [IP][ISDN]; Remote Monitoring Operator Clearance .....	57
RTS-VTC 1180.00 [IP][ISDN]; Far End Camera Control .....	58
RTS-VTC 1220.00 [IP][ISDN]; Encryption of Media .....	59
RTS-VTC 1230.00 [IP][ISDN]; Use FIPS 140-2 Validated Encryption .....	63
RTS-VTC 1250.00 [IP][ISDN]; Encryption Indicator .....	64
RTS-VTC 1260.00 [IP][ISDN]; User Validation Of Encryption .....	65

RTS-VTC 2020.00 [IP][ISDN]; Change Default Passwords.....	66
RTS-VTC 2022.00 [IP][ISDN]; Password Display during Logon .....	67
RTS-VTC 2024.00 [IP][ISDN]; Password/PIN Strength or Complexity .....	68
RTS-VTC 2026.00 [IP][ISDN]; Passwords for Different VTU Functions.....	70
RTS-VTC 2028.00 [IP][ISDN]; VTC Endpoint User Access Control .....	72
RTS-VTC 2040.00 [IP][ISDN]; Manual Password Management .....	74
RTS-VTC 2320.00 [IP][ISDN]; One Time Use “Local Meeting Password” .....	76
RTS-VTC 2325.00 [IP][ISDN]; Configuration/Administration Session Timeout .....	78
RTS-VTC 2340.00 [IP]; Use of Streaming in General .....	80
RTS-VTC 2350.00 [IP]; Streaming Indicator.....	83
RTS-VTC 2360.00 [IP]; SOP for CODEC Streaming.....	84
RTS-VTC 2365.00 [IP]; User Training for CODEC Streaming.....	86
RTS-VTC 2380.00 [IP]; Blocking Configuration for VTU/CODEC Streaming.....	88
RTS-VTC 2420.00 [IP]; VTU/CODEC Streaming Configuration .....	90
RTS-VTC 2440.01 [IP][ISDN][PC]; SOP Presentation Sharing.....	92
RTS-VTC 2460.00 [IP][ISDN]; PC Data and Presentation Sharing User Training .....	94
RTS-VTC 2480.00 [IP]; PC Data and Presentation Sharing Software .....	95
RTS-VTC 2820.00 [IP][ISDN]; Password for API Configuration Administrative Command Access 98	
RTS-VTC 2840.00 [IP][ISDN]; API Command Encryption and Authentication .....	100
RTS-VTC 3120.00 [IP]; Use Secure Management Protocols.....	102
RTS-VTC 3130.00 [IP]; Disable Unnecessary Protocols .....	104
RTS-VTC 3140.00 [IP]; SNMP Requirements.....	105
RTS-VTC 3160.00 [IP]; Management/Configuration IP addresses .....	106
RTS-VTC 3320.00 [IP][ISDN]; Use Latest Firmware, Software, and Patches.....	107
RTS-VTC 3420.00 [IP][ISDN]; DoD Logon “Electronic Notice (Warning) and Consent Banner” .....	109
RTS-VTC 3460.00 [IP]; Compliance with all applicable STIGs .....	113
RTS-VTC 3620.00 [IP][ISDN]; VTC Endpoint Office Installation Policy.....	115
RTS-VTC 3640.00 [IP][ISDN]; DAA Approval for VTC Implementation .....	117
RTS-VTC 3660.00 [IP][ISDN]; VTC Endpoint User/Administrator Training .....	119
RTS-VTC 3720.00 [IP][ISDN]; VTC Endpoint User’s Agreement and Training Acknowledgment .....	121
RTS-VTC 3740.00 [IP][ISDN]; VTC Endpoint User’s Guide .....	123
RTS-VTC 4120.00 [IP]; LAN Service Segregation .....	125
RTS-VTC 4220.00 [IP]; Wireless STIG Compliance .....	128
RTS-VTC 4320.00 [IP]; Simultaneous Wired and Wireless LAN Connection.....	129
RTS-VTC 4360.00 [IP]; Disable Wireless Support.....	130
RTS-VTC 4420.00 [IP][ISDN]; Wireless Conference Room Implementation .....	131
RTS-VTC 4520.00 [IP]; PPS Registration .....	133
RTS-VTC 5020.00 [IP][ISDN]; Access Control for Multipoint Conferences .....	134
RTS-VTC 5120.00 [IP][ISDN]; Scheduling System Access Control .....	136

## 1. PROCEDURES FOR REGISTRATION OF VTC ASSETS IN THE VMS

### 1.1 Introduction

This document will describe the proper procedure to follow to register and update the IA status of Video Tele-Conference (VTC) systems and devices in VMSv6. This includes all types of VTC systems, whether they are TDM (ISDN) or IP based, as well as any supporting system or device.

**Note:** VTC assets are also Real Time Services assets. As such this document will also refer to VTC assets as RTS assets.

#### 1.1.1 Pre - Requisites

Any person that needs to interface with the VMSv6 must:

1. Take the on-line CBT, which can be accessed at <https://vmscbt.disa.mil> (no login is required). It is highly recommended that a person taking the CBT review all modules to become familiar with all of the roles that the various VMS users fulfill.
2. Download and become familiar with the appropriate users guide for user role(s) that the trainee will be fulfilling. These may be found at <https://vmscbt.disa.mil/resources.htm>
3. Obtain a VMS account and login to the application. Instructions for this are contained in the CBT.
4. Become familiar with the navigation and features of VMS by reviewing the CBT and users guide while in VMS.

Once these steps have been completed, one can begin to register assets and update their statuses.

### 1.2 VTC Asset Naming Convention

A naming convention for the system and its components must be used when registering the various assets so that the individual assets can be more easily identified as a group or part of a system. This naming convention should be based on the name of the owner/site/location/enclave and the name/type of RTS system being registered.

Some examples of an overall RTS system name might be:

- DISA-SKY7\_VTC\_
- JFCOM-Desktop-VTC

This name represents the Non-Computing Asset for the overall VTC system.

The Computing Assets that make up the RTS system must include the name of the overall system and a unique name for the device. This unique name should include the function of the device and its network addressable name. That is the unique name that is used to identify the box on the network. This is not the IP address or MAC address, which is entered as an attribute of the asset.

Some examples of component device/system names might be:

- DISA-SKY7\_VTC\_Tandberg-6000MXP\_RoomNo#####
- DISA-SKY7\_VTC\_Polycom-VS.X7000\_RoomNo#####
- JFCOM-Desktop-VTC\_Tandberg-1500MXP\_Bldg-RoomNo#####
- JFCOM-VTC\_Tandberg-TMS-Svr
- JFCOM-VTC\_Tandberg-Gateway
- JFCOM-VTC\_Tandberg-MCU\_MPS800

In the event that an asset already exists and uses a different naming convention, place the name derived here the asset 'Description' field.

### 1.3 RTS Asset Identification

An RTS system as a whole is an asset; however, each individual device that makes up the system is also an asset. Each of these assets must be registered in the VMS. VMS has 2 primary types of assets, Computing and Non-Computing.

Each RTS system at a given site/location/enclave needs to be registered as a Non-Computing Asset in the VMS.

The individual assets are registered as Computing Assets. Computing Assets are based on boxes, which have an operating system (OS), as well as applications such as databases, web servers, and control and/or management applications. The OS and the applications are called "Postures" in the VMS. All applicable postures are assigned to the asset.

Typically, a Computing Asset will have at least one IP address and/or one MAC address. Management workstations, LAN switches and routers, firewalls, multiplexers, phones, and similar devices are also Computing Assets that make up the RTS system. Desktops and Laptops are also computing devices that need to be registered.

#### 1.3.1 Local Management System(s)

LAN switches and routers, management workstations/consoles, NMS servers, and front end processors that are used exclusively in the local management the RTS system must be named and registered as part of the RTS system and given a unique name (using the naming convention above) identifying it as part of the RTS system. Local management systems must be treated as an enclave.

#### 1.3.2 Remote Management System(s)

LAN switches and routers, management workstations, NMS servers, and front end processors, etc., that are part of a remote management/monitoring system such as ADIMSS, ARDIMSS, ESRS, etc., must be registered by the owner/SA of the device or the owner/SA of the management/monitoring system that it is part of. It is critical that the 'Location', 'Managed By', and 'Owned by' fields are properly filled out. The device or system must also be associated with the proper program(s), site, and enclave under the 'Sites/Enclaves' tab. Remote management systems are typically separate enclaves from the local management system enclaves.

### 1.3.3 BCPS LAN/CAN/BAN Infrastructure

LAN switches and routers that make up the data and RTS distribution system must be named and registered by the LAN/enclave SA in accordance with the Network Infrastructure asset registration instructions found in the Network Infrastructure Checklist. RTS requirements for the LAN are applied to the asset via the Non-Computing asset assignment of the RTS requirements to it as described below.

### 1.3.4 RTS Adjunct/Auxiliary Systems/Devices

Adjunct/Auxiliary Systems/Devices are defined as systems and devices that augment the basic telephony service. Examples of such systems and devices are: Voice mail systems, call center and/or operator systems, CTI systems, IVR systems, auto-attendant systems, Emergency Services (911) systems, etc. Systems such as these may be registered as part of the RTS system if appropriate (i.e., small systems or single devices), or may be registered as a separate Non-Computing system/enclave asset along with its Computing assets.

## 1.4 RTS Asset Creation in the VMS

The RTS system Non-Computing Assets are registered first, followed by the Computing Assets. This section will provide an overview of the major steps. Subsequent sections will provide step-by-step procedures.

### 1.4.1 The Organization, Site, and/or Location

Before assets can be created, an organization and a site or location must be defined in the VMS. This is a VMS ISSM role and responsibility and is outside the scope of this document. Programs are also defined in the VMS and this is the responsibility of the VMS DAA role.

## 1.5 Non-Computing Asset Creation

First create the Non-Computing Asset for the RTS system using the naming convention described in “RTS Asset Naming Convention” above. On the ‘Asset Posture’ tab, expand the ‘Voice/Video/RTS Policy’ item and check the policies that apply. The available policies are:

- DRSN Policy
- DSN Policy
- VoIP/VoSIP Policy
- Video Tele-Conference Policy

‘DRSN Policy’ applies to an asset that is part of, or connected to, the DRSN. This can also apply to other “secure” or classified voice/video/RTS systems.

‘DSN Policy’ applies to an asset that is part of, or connected to, the DSN or other UN-classified voice/video/RTS systems. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.

‘VoIP/VoSIP Policy’ applies to an asset being registered that provides IP based voice or video communications (i.e., VoIP). This includes IP centric systems as well as IP enabled TDM based systems.

Either DSN Policy **OR** DRSN Policy must be checked. VoIP/VoSIP Policy must **ALSO** be checked if the system provides IP based voice or video communications.

A local RTS system management LAN, that is not part of the site LAN, should be added to, or registered as part of, the RTS Non-Computing Asset. Additionally, a LAN that only supports an adjunct/auxiliary system to the RTS system, such as a call center or IVR system may be added to or registered as part of the RTS Non-Computing Asset.

This is done by adding the 'Network Infrastructure Policy' and/or the 'General Business LAN Enclave' postures.

Additionally, an adjunct/auxiliary system to the RTS system (and its supporting LAN) such as a call center or IVR system etc, that is not part of the site LAN, may be registered a separate complete system to include its supporting LAN. Such a system is registered as a Non-Computing Asset using the naming convention for the overall RTS system and adding the adjunct/auxiliary system name. For Example:

- LacklandAFB\_MSL100\_CallCtr-Sys
- LacklandAFB\_MSL100\_IVR-Sys
- LacklandAFB\_MSL100\_911-Sys

This is done by adding the 'Network Infrastructure Policy' and/or the 'General Business LAN Enclave' as well as the 'Voice/Video/RTS Policy' postures to the Non-Computing Asset.

The second Non-Computing Asset that needs registration consideration is the site LAN/CAN/BAN that provides distribution for both RTS services and data traffic. This network must be registered along with its components whether it supports RTS systems or not. The SA for the RTS system must work with the SA for the LAN/CAN/BAN to insure that the Voice/Video/RTS Policy asset postures are selected as described above for the RTS System itself. These two SAs could be the same person, however, if not, the SA for the LAN/CAN/BAN should grant "update" permissions on LAN assets to the SA for the RTS system. Asset naming would follow that chosen by the SA for the LAN/CAN/BAN.

Alternately, the SA for the RTS system could create his/her own LAN/CAN/BAN Non-Computing Asset and assign the 'Voice/Video/RTS Policy' asset postures to it. Asset naming would follow the naming convention described in "RTS Asset Naming Convention" above. In this case, the individual LAN/CAN/BAN Computing Assets would not be registered since the SA for the LAN/CAN/BAN would register these.

Detailed step-by-step process instructions are provided under "Creating the Non-Computing Asset(s)" below.

### 1.5.1 Computing Asset Creation

All system devices must be defined and registered once the appropriate NON-Computing Assets are created, and the BCPS LAN/CAN/BAN has had the Voice/Video/RTS Policies added to it. The SA for the BCPS LAN/CAN/BAN must register each LAN switch, router, and management system. This does not have to be done by the RTS system SA unless he/she is also the SA for the BCPS LAN/CAN/BAN, or if the RTS system SA has created a separate Non-Computing Asset for the RTS BCPS LAN/CAN/BAN.

The following are examples of RTS Computing Assets:

**Note:** Some of these may have sub-components that are also considered as individual Computing Assets.

- TDM Switch (Possible sub-components)
- Local Call Controller (Possible sub-components)
- Call Manager Subscriber
- Call Manager Publisher
- Media gateway
- RTS firewall or Boundary control device
- LAN Switch / Router
- Phone instrument – endpoint
- Management workstation
- NMS data collection device or server
- Server (of almost any type)
- VTC MCU (Possible sub-components)
- VTC endpoint
- Gatekeeper
- All GSCR device type designations:
- Many others

All computing assets are registered with an OS. They may also have applications such as databases and/or web servers that also must be added to the posture of the asset.

Registering computing assets is an iterative process until all assets are registered.

Detailed step-by-step process instructions are provided under “Creating the Computing Asset(s)” below.

## 1.6 Creating Assets – Step-by-Step

### 1.6.1 Creating the NON-Computing Asset(s)

These instructions apply to creating the Video Tele-Conference system and/or Adjunct/Auxiliary system NON-Computing Asset.

**Note:** (*Reviewer*) It is recommended that a reviewer work with the Video Tele-Conference system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

#### a. Steps

- i. **Expand ‘Asset Findings Maint’**
- ii. **Click ‘Assets/Findings’**
- iii. **Expand ‘By Location’** and then find and expand your site/location. Others may need to expand ‘Managed By’ or ‘Owned By’. What is seen depends upon your permissions or role. Within the location, assets are divided into computing, non-computing and CNDS.
  - o Proceed to step vi.  
(*Reviewer Only*) Expand ‘Visits’ to display its sub-folders.
- iv. (*Reviewer Only*) Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
- v. (*Reviewer Only*) Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
- vi. **Click the ‘yellow folder’** icon located at the right of ‘Non-Computing’. You may expand ‘Non-Computing’ to see assets that have already been created and that you have permissions for.
- vii. **Click the ‘General’ tab**
  - o Enter a ‘Host Name’ using the naming convention described in “VTC Asset Naming Convention” above.
  - o Enter a ‘Description’ of the system.  
**Note:** This should reflect a general description of the VTC System and could include the make and version of the software.
  - o Verify/Select the location of the system in “Location”
  - o Verify/Select the owner of the system in “Owner”: Used to register asset to parent or child location.
  - o Verify/Select the organization or site responsible for management of the system in “Managed By”: Used for remotely managed locations.
  - o Verify ‘Mac level’, ‘Confidentiality’, & ‘Classification’, Change as required.  
**Note:** These default to MAC II, Sensitive, Unclassified. The ‘Confidentiality’ of a RTS system or asset should never be set to ‘Public’ since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.

- o Click **'Save'**.  
**Note:** It is recommended that you click **'Save'** after filling out each tab or more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.
- viii. **Click the 'Asset Posture' tab** to add functions to the asset:
  - o Expand 'Non-Computing'
  - o Expand 'Video Policy'
  - o Check the boxes for appropriate policy/policies as follows:
    - Check 'Video Tele-Conference Policy'
  - o Click **'>>'** to move it to the 'Selected' window. This can be done after each selection or after all selections.
  - o Click **'Save'**
- ix. **Click the 'Systems / Enclaves' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).
  - o Determine the enclave and/or program that the asset is part of.
  - o In the 'Available Systems' box:
    - Find and select 'DISN-DVS.-II' if the system can place or receive calls via DVS.-II.
  - o In the 'Available Enclaves' box:
    - Find and select the local enclave that the RTS system is part of. (i.e., your site/location)
    - Click **'>>'** to move it to the 'Selected Enclaves' window
    - Click **'Save'****Note:** For registered enclaves and/or programs, choose all that apply. If the enclave or program is not present, ensure that the IAM [or (*Reviewer Only*) Team Lead] works with the appropriate site personnel to request the enclave or program be added.
- x. **Click the 'Additional Details' tab** to add building and room number information for the RTS asset; this should reflect the location of the RTS core equipment.
- xi. **Click 'Save'**.
- xii. Return to step vi to create another Non-Computing asset or proceed to creating the Computing Assets in the next section.

**Note:** The above 'Video Tele-Conference Policy' postures and program association may be added to an enclave or network non-computing asset instead of creating a separate Video Tele-Conference Policy non-computing asset.

## 1.6.2 Creating the Computing Assets

These instructions apply to creating the RTS system and/or Adjunct/Auxiliary system Computing Asset(s).

**Note:** (*Reviewer*) It is recommended that a reviewer work with the Voice/Video/RTS system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

*b. Steps*

- i. **Expand ‘Asset Findings Maint’**
- ii. **Click ‘Assets/Findings’**
- iii. **Expand ‘By Location’** and then find and expand your site/location. Others may need to expand ‘Managed By’ or ‘Owned By’. What is seen depends upon your permissions or role. Within the location, assets are divided into computing, non-computing and CNDS. Proceed to step vi.  
(*Reviewer Only*) Expand ‘Visits’ to display its sub-folders.
- iv. (*Reviewer Only*) Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
- v. (*Reviewer Only*) Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
- vi. **Click the ‘yellow folder’** icon located at the right of ‘Computing’. You may expand ‘Computing’ to see assets that have already been created and that you have permissions for.
- vii. **Click the ‘General’ tab**
  - o Enter the ‘Host Name’ following the naming convention described above.
  - o Enter a ‘Description’ of the asset. This should reflect the function and platform of the device. i.e., make and model of the device and software version etc.
  - o Verify/Select the location of the system in “Location”
  - o Verify/Select the owner of the system in “Owner”: Used to register asset to parent or child location.
  - o Verify/Select the organization or site responsible for management of the system in “Managed By”: Used for remotely managed/monitored locations.
  - o Verify ‘Mac level’, ‘Confidentiality’, & ‘Classification’, ‘Status’, ‘Use’, & ‘Workstation’, Change as required.  
**Note:** These default to MAC II, Sensitive, Unclassified, Online, Production, No. The ‘Confidentiality’ of a RTS system or asset should never be set to ‘Public’ since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.
  - o **Click ‘Save’.**  
**Note:** It is recommended that you click ‘Save’ after filling out each tab or even more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.
- viii. **Click the ‘Asset Identification’ tab** to enter as much identifying information as is available:

- o Enter one or all of the following: 'I.P. Address(s)', 'MAC Address(s)', 'System Unique ID'
    - Note:** The 'System Unique ID' field may be used in addition to the IP and/or MAC addresses. The name used in the 'Host Name' field MAY be entered in the 'System Unique ID' field.
    - Note:** When entering IP and/or MAC addresses, complete all fields and click 'add'. The address is listed on the right. Multiple addresses can be entered one by one. Addresses can be deleted by clicking 'remove' next to the address to be deleted.
    - Note:** IPv6 addresses can be entered along with IPv4 addresses. Click 'IPv6' to obtain an IPv6 address box. Click 'IPv4' to revert back to an IPv4 address box. Enter as noted above.
    - Note:** Establish your standards by using the loopback IP address of a network device. If a loopback is not used or is unavailable, use the management interface IP address or MAC address. These entries are not required if the device is not network enabled (i.e., a legacy TDM device that only has a serial management (craft) interface). In this case the device name used in the 'Host Name' field MUST be entered in the 'System Unique ID' field.
  - o Enter the 'Fully-Qualified Domain Name' of the device if it is a member of a network domain.
  - o Click 'Save'.
- ix. Click the 'Asset Posture' tab to add Postures or functions to the asset:
- a) Expand 'Computing' to view the available postures
    - Note:** Expand each of the categories listed throughout the tree and click all applicable boxes for the specific asset being registered. Every asset has an OS. Expand 'Operating System' (and sub-branches) and select the version of OS that is used by the asset. Assets may also have applications. Expand 'Applications' (and sub-branches) and select ALL the application types and versions that are used by the asset. Follow this method for adding all applicable postures or functions to the asset being registered. The following steps will define a more detailed procedure or guide tailored to RTS systems. However, it is impossible to anticipate every possibility with these instructions due to the fact that RTS systems utilize various combinations of all technologies listed. The SA (or reviewer) is responsible for knowing what the asset being registered is, what its OS is, and what other applications or technologies it uses.

**Note:** Technology based rules within the VMS require the selection of additional postures and/or the input of additional information, such as instance identifiers, when selecting some items in the 'Available Postures' list. Refer to the VMS registration instructions found in the Checklist for the related technology. This is most often related to the Database and Web Server postures. A listing of these rules may be found on the VMS Help page. When this information is required, additional information or input boxes are displayed (following a 'Save') in the lower right corner of the 'Available Postures' under the 'Selected' box. Input boxes are accompanied with a 'add' link that must be clicked to enter the information.

**Note:** Clicking '>>>' can be done after each selection or after all selections. You will need to expand the device name that appears in the 'Selected' box to see the various items selected.

**Note: Rules must be satisfied or the Asset Posture selection(s) will not save.** Clicking '>>>' will cause any required additional input box to appear under the 'selected' box. This does NOT display alerts. Clicking 'Save' will cause an alert for any rule that is not satisfied to be displayed under the 'selected' box. Additionally, all rules and input boxes that are displayed must be satisfied before the posture will save successfully. Therefore it is recommended that '>>>' and 'Save' be clicked after selecting any posture tree under the top level. The instructions will reflect this.

- b) **Expand 'Voice/Video/RTS'** to view the available postures or functions.

Check all boxes that apply as follows:

**Note:** If registering a LAN/CAN/BAN network infrastructure device or management system, Expand 'Network' then 'Data Network' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.

- o Check 'VoIP Switch/System/Device' if the asset provides, or is involved in providing IP based RTS communications. This includes Voice as well as VTC that is part of or associated with the Voice system. (i.e., video phones or VTC devices or applications that are controlled by or registered with a RTS/VoIP LCC. This also includes IP enabled TDM switches.

**AND/OR**

- o Check 'TDM Switch/System/Device' if the asset is a TDM based telecommunications switch. This includes IP enabled TDM that provide VoIP service. In this case 'VoIP Switch/System/Device' is also checked.

**Note:** This also applies to TDM signaling a Switch/System/Device such as an SS7 STP, SSP, or SCP. (Refer to the DSN STIG for an explanation of these devices.)

**OR**

- Check 'Voice/Video Adjunct/Aux/Management System/Device' if the asset is involved in managing a RTS system or device or providing some adjunct or auxiliary function to the RTS system other than providing the RTS switching capability.
- OR**
- Check 'Video/VTC System/Device' if the asset is, or is part of, a video or VTC system that is NOT controlled by the RTS/VoIP LCC.
  - **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
  - **Click 'Save'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the 'Selected' box.
    - Click '>>' and **Save** again.
- c) **Expand 'Role'** to view the available Roles for the asset or system being registered. Rules within the VMS require the selection of a Role.
- Check the box next to each role that the asset fulfills. RTS system devices must have one or more of the following selected:
- IF** the asset is part of a classified RTS system or network
- Check the box next to 'Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices.
- OR IF** the asset is used in an UN-classified RTS system
- Check the box next to 'UN-Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices
- AND IF** the asset is part of a RTS management system
- Check the box next to 'RTS Management'. This applies to assets that are part of a system that manages core equipment and/or Adjunct/Auxiliary systems/devices.
  - **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
  - **Click 'Save'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the 'Selected' box.
    - Click '>>' and **Save** again.
- Note:** Additional roles may need to be selected due to rules associated with other postures. One of these is the Windows OS, which requires the selection of 'Domain Controller', 'Member Server', or 'Workstation'. These may be selected now if selecting a Windows OS in the next step.
- d) **Expand 'Operating System'** to view the available OSs. Drill down through the tree to locate the version of OS installed on the asset. Rules within the VMS require the selection of an OS.

- Check the box next to the OS installed on the asset. Some OSs can be found at the top level of the tree. Others and their versions require drilling deeper. The following steps provide a more in depth procedure and explanation.

**IF** the asset is based on a Windows OS

- Expand 'Windows' AND expand the Windows version being used.
  - Check the box next to the version of Windows installed on the asset.  
**Note:** For Windows registration instructions and further explanation, refer to the VMS registration instructions found in the Windows Checklist.  
**Note:** Rules within the VMS require the selection additional postures when selecting the Windows Operating System. This is covered in the next step.  
**Note:** If the version of windows being used is a vendor-customized version, check the box next to the version of Windows on which the vendor based their customization.
  - Expand 'Role' and select 'Domain Controller', 'Member Server', or 'Workstation'. RTS core equipment will typically be registered as a 'Member Server' unless it provides Active Directory Services.

**Note:** Rules within the VMS also add the postures of Application/Browsers/Internet Explorer/IE6 and Application/Desktop Application - General. These appear after the Role rule is satisfied and the selections/Asset is saved. The browser selection may be changed if necessary. See Browser selection below.

**OR IF** the asset is based on a UNIX or Linux OS

- Expand 'UNIX' AND sub-branches to locate the OS and version being used.
  - Check the box next to the version of UNIX/Linux installed on the asset.  
**Note:** For UNIX/Linux registration instructions refer to the VMS registration instructions found in the Unix Checklist.  
At the time of this writing, there are no rules within the VMS require the selection additional postures when selecting the UNIX or Linux Operating System.

**OR IF** the asset is based on a Cisco or Juniper network device OS

- Expand 'Cisco' or 'Juniper' to locate the OS and version being used.
  - Check the box next to the version of OS installed on the asset.  
**Note:** For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.  
**Note:** Rules within the VMS MAY require the selection additional postures when selecting a Cisco or Juniper Operating System.

**OR IF** the asset is based on an embedded network device OS and/or has not been located anywhere else in the OS tree:

- Expand 'Network Device Embedded OS' to locate the OS and version being used.

- Check the box next to the version of OS installed on the asset.  
**Note:** For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.  
**Note:** Rules within the VMS MAY require the selection additional postures when selecting a Network Device Embedded OS. **IF** the appropriate OS has not been located anywhere else in the OS tree, check the box next to 'Other Network OS'
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click '>>' and **Save** again.
- e) **IF** the asset is a server or a piece of RTS system core equipment, proceed to f) and select all the applications used by the device. If the asset is not a server or a piece of RTS system core equipment, skip to step g).
- f) **Expand 'Application'** to view the available applications. Drill down through the tree to locate all applications and versions being used by the asset. This is a required step to define what applications are installed on the asset for which there is configuration guidance or for which IAVM notices exist. This requirement is typically applicable to RTS core equipment and servers. The SA (or reviewer) is responsible for knowing what general-purpose applications the asset being registered uses or is based upon. The SA (or reviewer) is further responsible for selection all general-purpose applications that the asset being registered uses. The following steps will detail applications that are typically found as the basis of or used by RTS assets.
  - **Expand 'Database'** and drill down to find the version of database being used on the asset. If not used or not found; skip this selection.
    - Check the box next to the version of Database being used on the asset.  
**Note:** For Database registration instructions refer to the VMS registration instructions found in the Database Checklist.  
**Note:** Rules within the VMS require the selection additional postures when selecting a Database.
  - **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
  - **Click 'Save'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the 'Selected' box.
    - Click '>>' and **Save** again.
  - **Expand 'Web Server'** and drill down to find the version of Web Server being used on the asset. If not used or not found; skip this selection.

- Check the box next to the version of Web Server being used on the asset.  
**Note:** For Web Server registration instructions refer to the VMS registration instructions found in the Web Server Checklist.  
**Note:** Rules within the VMS require the selection additional postures when selecting a Web Server.
- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the ‘Selected’ box. Click ‘Add’.
- **Click ‘Save’**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the ‘Selected’ box.
  - Click ‘>>’ and **Save’** again.
- **Expand ‘Application Servers’** and drill down to find the version of Application Server being used on the asset. This will typically be a version of Tomcat. If not used or not found; skip this selection.
  - Check the box next to the version of Application Server being used on the asset.  
**Note:** For Application Server registration instructions refer to the VMS registration instructions found in the Web Server and Application Checklists.  
**Note:** Rules within the VMS require the selection additional postures when selecting an Application Server.
- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the ‘Selected’ box. Click ‘Add’.
- **Click ‘Save’**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the ‘Selected’ box.
  - Click ‘>>’ and **Save’** again.
- **Expand ‘Browsers’** and drill down to find the version(s) of Browser(s) being used on the asset. If not used or not found; skip this selection.  
**Note:** If a browser was automatically added to the asset’s posture when selecting a Windows OS and it is the correct browser, skip this selection. If not, select the proper browser, add it, and select the incorrect browser version and click ‘<<’ to remove it.
  - Check the box next to the version of Browser being used on the asset.  
**Note:** For Browser registration instructions refer to the VMS registration instructions found in the Web Checklist and/or Desktop Application Checklist.  
**Note:** Rules within the VMS require the selection additional postures when selecting a Browser.
- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)

- Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click '>>' and **Save** again.
- **Expand 'Antivirus'** and drill down to find the version of Antivirus being used on the asset. If not used or not found, skip this selection. The use of Antivirus software is a requirement for all Windows based systems.
  - Check the box next to the version of Antivirus being used on the asset.  
**Note:** For Antivirus software registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.  
**Note:** Rules within the VMS MAY require the selection additional postures when selecting Antivirus Software.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
- **Expand 'JVM'** and drill down to find the version of Java Virtual Machine Manager being used on the asset. If not used or not found; skip this selection. This is required, however, when registering certain other web server postures.
  - Check the box next to the version of ESM software being used on the asset.  
**Note:** For JVM registration instructions refer to the VMS registration instructions found in the Web Server Checklist.  
**Note:** Rules within the VMS MAY require the selection additional postures when selecting a Java Virtual Machine.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click '>>' and **Save** again.
- **Expand 'MSdotNETFramework'** and drill down to find the version of Framework being used on the asset. If not used or not found; skip this selection.
  - Check the box next to the version of Framework being used on the asset.  
**Note:** For dotNET Framework registration instructions refer to the VMS registration instructions found in the Web Server Checklist.

**Note:** Rules within the VMS MAY require the selection additional postures when selecting a dotNET Framework.

- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the ‘Selected’ box. Click ‘Add’.
- **Click ‘Save’**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the ‘Selected’ box.
  - Click ‘>>’ and **Save**’ again.
- **Expand ‘ESM’** and drill down to find the version of Enterprise System Manager being used on the asset. If not used (not typically used) or not found; skip this selection.
  - Check the box next to the version of ESM software being used on the asset.

**Note:** For ESM registration instructions refer to the VMS registration instructions found in the ESM Checklist.

**Note:** Rules within the VMS MAY require the selection additional postures when selecting ESM software.

- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the ‘Selected’ box. Click ‘Add’.
- **Click ‘Save’**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the ‘Selected’ box.
  - Click ‘>>’ and **Save**’ again.
- **Expand ‘Office Automation’** and drill down to find the version of Office Automation software being used on the asset. If not used (not typically used) or not found; skip this selection.
  - Check the box next to the version of Office Automation software being used on the asset.

**Note:** For Office Automation registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.

**Note:** Rules within the VMS MAY require the selection additional postures when selecting an Office Automation.

- **Click ‘>>’** to move the posture to the ‘Selected’ window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the ‘Selected’ box. Click ‘Add’.
- **Click ‘Save’**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the ‘Selected’ box.
  - Click ‘>>’ and **Save**’ again.

- g) **IF** registering a network switch, router, or other network transmission element, that is part of a LAN supporting an Adjunct or Auxiliary system or the management of the RTS system or an Adjunct or Auxiliary system, AND it is NOT part of the BCPS LAN/CAN/BAN/WAN network infrastructure or management system, proceed to h), otherwise, proceed to i).
- h) Expand 'Network' then 'Data Network' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
  - Check the boxes next to the appropriate postures for the asset.
  - **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
    - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
  - **Click 'Save'**. (Optional/Recommended)
    - Satisfy any Rule alert that appears under the 'Selected' box.
    - Click '>>' and **Save** again.
- i) **Click 'Save'** one last time Proceed to x.
- x. **Click the 'Functions' tab** to select the function of the asset being registered.
  - Select all functions that the asset performs. If an appropriate function is not found; skip this selection.
  - Click '>>' to move it to the 'Selected' window.
  - Click 'Save'
- xi. **Click the 'Systems / Enclaves' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).
  - In the 'Available Systems' box:
    - Find and select 'DISN-DSN' if the system can place or receive DSN calls.
    - OR**
    - Find and select 'DISN-DRSN' if the system can place or receive DRSN calls.
    - OR**
    - Find and select 'DISN-DVS.-II' if the system can place or receive DVS.-II or DVS.-G calls.
    - OR**
    - Skip this step if the RTS system or device is not part of or does not communicate with a Program of Record (i.e., it is a private system)
    - Click '>>' to move it to the 'Selected Systems' window
    - IF the RTS System is managed or monitored by the ADIMSS (DSN), Find and select 'ADIMSS'
    - OR**
    - IF the RTS System is managed or monitored by the ARDIMSS or ESRS (DRSN), Find and select 'ARDIMSS' and/or 'ESRS'
    - OR**
    - Find and select 'DISN-DRSN' if the system can place or receive DRSN calls.

**OR**

- Skip this step if the RTS system or device is not managed by; is not part of; or does not communicate with a Program of Record (i.e., it is a private system)
- Click '>>' to move it to the 'Selected Systems' window
- o In the 'Available Enclaves' box:
  - Find and select the local enclave that the RTS system is part of. (i.e., your site/location) (These selections may not in the list as yet)  
**Note:** For registered enclaves, choose the enclave. If the enclave is not present, your IAM can determine if the enclave has been requested to be added. [(*Reviewer Only*) contact your team lead.] If the team lead or IAM has requested an enclave be added; 'Select Has Been Requested'. If the enclave has not been requested; 'Select Not Available'. There should not be any assets registered/updated that are not part of an enclave.
- o Click '>>' to move it to the 'Selected Systems' window
- o Click 'Save'
- xii. Click the 'Additional Details' tab and provide all of the requested information for the RTS asset; Building and room number should reflect the actual location of the RTS of the asset. Other information requested is Serial Number and Barcode, Make, Model and Manufacturer.
- xiii. Click 'Save'.
- xiv. Return to step vi to create another Computing asset or proceed to Reviewing Assets in the next section.

**Note:** (Reviewer) New assets created by a reviewer will be found under the 'Not Selected for Review' area of the visit tree for the site that the asset is registered to.

**Note:** (Reviewer) Changing the status of one vulnerability will move the asset from the 'Not Selected for Review' area or the 'Must Review' area to the 'Reviewed' area of the visit tree for the site that the asset is registered to.

**Note:** When creating a NEW asset it is recommended to run a VL03 report to identify the IAVMs that will be assigned to the new asset being created. (See instructions below). IAVMS that are assigned to an asset will default to an open status and must be acknowledged and fixed immediately. All other vulnerabilities will default to 'Not Reviewed'

**Note:** The following process may be used in the event that there is a need to create multiple assets having the **same** configuration or postures.

**CAUTION:** Extreme care must be exercised when performing this procedure. The identifying information **MUST** be changed (as listed under "minimum edit" below). If this information is not changed, the exported asset will be updated only.

- Create the first asset and save it.

- While displaying the first asset's registration information, export the asset. This will create a .xml file on your computer that contains the registration information.
- Open the .xml file in a text editor.
- Edit the identifying information for the asset.
  - At a minimum edit the following:
    - Asset name
    - Host name
    - Unique ID
    - MAC Address
    - IP address
  - Optionally edit the following:
    - Building
    - Room
    - Serial number
    - Barcode
- Save the edited information insuring that the file name is changed appropriately and the .xml extension is maintained.
- Return to VMS and click the XML icon to the right of the file folder icon nest to computing. Browse for the file and click submit.
- Open the newly created asset and update/validate all identification and posture information. Update as needed.

### 1.6.3 Procedures for Updating the Vulnerability Status of the Asset

If all registration tasks have been accomplished and/or verified, use the following procedures for updating the status of all assets, both computing and non-computing.

**Note:** (*Reviewer Only*) In the event that the Voice/Video/RTS asset just reviewed does not exist in VMS, the reviewer may create it. It is highly recommended that the reviewer have the Voice/Video/RTS SA create the asset and works with him/her to assure that the asset is fully and properly registered and named or identified in accordance with the Voice/Video/RTS asset registration instructions described above. If a reviewer must create an arbitrary asset to enter their vulnerability statuses, they must notify the team lead, any others on the team that may also have to update their statuses on the same asset, and the Voice/Video/RTS asset SA. The Voice/Video/RTS asset SA may update the registration information as needed.

Additionally, the reviewer should check with the Voice/Video/RTS asset SA before creating a new asset in the event that the asset does exist in VMS but shows up in a different part of VMS (i.e., identified differently or registered to a different organization). If a reviewer creates an asset, they become the SA or "owner" for the asset. "Ownership" of assets created by a reviewer must be transferred to the actual SA for the asset.

- c. *Steps*
  - i. **Expand 'Asset Findings Maint'**

- ii. **Click ‘Assets/Findings’**
- iii. **(SA) Expand ‘By Location’** and proceed to step vi.  
*(Reviewer Only)* Expand ‘Visits’ to display its sub-folders
- iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
- v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
- vi. **Expand ‘Computing’** and/or ‘**Non-Computing**’ and/or ‘**CNDS**’ as applicable
- vii. *(Reviewer Only)* **Expand ‘Must Review’**  
*SA will not see ‘Must Review’, but will proceed to step viii.*

**Note:** *(Reviewer Only)* Newly created assets will appear under “Not Selected for Review.”

- viii. **Expand the ‘Asset Name’** for the asset to be reviewed. The icon in front of “Ready to review” assets is colored in RED. Drill down until the list of vulnerabilities displays under the asset. If multiple postures were selected for the asset during registration, a list of the postures is displayed. Expand each posture to see the list of vulnerabilities under each.

**Note:** Determine what postures, if any, can be reviewed and updated using automation. This would apply to any posture/technology for which a Gold Disk or a set of review scripts exist. (i.e., Windows Gold disk and scripts for UNIX, Database, and Web Servers). It is highly recommended that this automation be used to review as many findings as possible before beginning a manual review or update of the remaining vulnerabilities. Once reviewed in this manner, the results are imported into VMS to update the status of the vulnerabilities for each set of automation or technology. All vulnerabilities may be updated manually.

**Note:** To review/update all vulnerabilities under all major postures or technologies other than Voice/Video/RTS, Refer to the Asset Review instructions found in the appropriate checklist for that technology.

**Note:** When you drill down into the lowest level of the asset tree, you will find the Vulnerabilities and IAVMs assigned to the asset.

- ix. **Click on a ‘Vulnerability Key’** in the tree that needs to be updated to open its status update area and tabs (scroll down to see if necessary).
- x. **On the ‘Status’ Tab**, Update the ‘Status’ of the vulnerability.

**Note:** If selecting a status of ‘O-Open’, a ‘Details’ and ‘Milestone’ must also be entered.

- xi. **Click the ‘Details’ Tab**, (Conditional) identify details on all open vulnerabilities/findings by adding to or modifying the default details displayed in the box.
- xii. **Click the ‘Comments’ Tab**, (Optional) Add ,any pertinent comments
- xiii. **Click the ‘Programs’ Tab**, (Conditional)

**Note:** This is a place holder for future instructions relating to Program Baselines.

- xiv. **Click the ‘POA&M’ Tab**, (*SA, not Reviewer*) (Conditional)
  - Note:** SAs performing self-assessments are required to enter a POA&M for all open vulnerabilities/findings before the status will save. This does not apply to a reviewer.
  - o Click the ‘New Milestone’ Button, Enter a ‘Milestone’ (description of a step in mitigating/fixing the finding) and a ‘Completion Date’.
  - o Click the ‘Disk/Save’ icon on the left to save the milestone
  - o Enter additional milestones as necessary.
- xv. **Click the ‘Apply to Other Findings’ Tab**, (Conditional) If applicable: Check ‘Choose Other Assets with the Same Finding in the Same Status’. Select the appropriate assets.

**Note:** If this feature of VMS is to be used, it must be used before clicking ‘Save’ or else no assets with similar postures/statuses will be found.

- xvi. **Click the ‘Save’ button** at the bottom of the form area
  - Note:** Alert messages will be shown below the ‘Save’ Button. If alert messages display, the status update information will not save until the alert message(s) is satisfied.
- xvii. Return to step ix above and select another ‘Vulnerability Key’. Repeat this until all ‘Computing’ and ‘Non-Computing’ asset vulnerability statuses are updated.

**Note:** System Administrators should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level.

#### 1.6.4 Verify that all necessary assets were reviewed

- d. *Steps*
  - i. **Expand ‘Asset Findings Maint’**
  - ii. **Click ‘Assets/Findings’**
  - iii. **(SA) Expand ‘By Location’** and proceed to step vi.  
(*Reviewer Only*) Expand ‘Visits’ to display its sub-folders
  - iv. (*Reviewer Only*) Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
  - v. (*Reviewer Only*) Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

- vi. **Expand ‘Computing’** and/or **‘Non-Computing’** and/or **‘CNDS’** as applicable
- vii. *(Reviewer Only)* **Expand ‘Must Review’**  
*SA will not see ‘Must Review’, but will proceed to step viii.*
- viii. **Expand Each ‘Asset Name’** to view the list of asset postures.
  - o If checkmarks are gone, the asset has been fully reviewed.
- ix. **Done**

The following reports can be used to verify the status of the site and its assets.

1. VC06 Asset Compliance Report
  - a. A Full report may be obtained
2. VC03 Severity Summary Report
  - a. Table of numbers only
3. VC01
  - a. Used for IAVM Compliance

See **Compliance monitoring** below for a quick set of instructions on generating these reports.

### 1.6.5 Add Comments to a Visit (Reviewer only)

- e. *Steps– Click the following:*
  - i. ‘Visit Maint.’
  - ii. Expand the Organization the visit is set up for.
  - iii. Expand the Visit
  - iv. Locate the visit you are working on. (Drill down till you find it)
  - v. Click on CCSD or enclave name. (Drill down till you find it)
  - vi. ‘Comments Tab’
    - a) Type your comments
  - vii. ‘Save Changes’

## 1.7 Reports – Step-by-Step

### 1.7.1 Compliance Monitoring

- **VC06** – provides a detailed report of all vulnerabilities that are assigned to an asset and its postures. There are many items that can be selected for display and the report can be filtered and sorted in multiple ways.

- f. *Steps– Click the following:*
  - i. ‘Reports’
  - ii. ‘VC06’
  - iii. Select an ‘Asset(s)’ or an ‘Organization(s)’.
  - iv. Select “open” status to see only “Open” findings (Select others as desired. Hold the Ctrl or Shift key to make multiple selections)
  - v. Select the sort order under ‘Sort By’
  - vi. Select the information to be displayed: Check the following boxes:
    4. ‘Finding Comments’

5. 'Finding Long Name' (Because it is truncated otherwise)
  6. 'Finding Details'
  7. 'Vulnerability Discussion'
  8. Others as desired
- vii. 'Generate Report'
- **VC03** – Provides a table of assets and technologies with the number and percentage of findings against each listed by severity category. The VC03 report contains numbers only.
    - a. *Steps– Click the following:*
      - i. 'Reports'
      - ii. 'VC03'
      - iii. Select an 'Organization(s)'
      - iv. Review other options and select as desired
      - v. 'Generate Report'
  - **VC01** - Used for IAVM Compliance (An SA may not see this option).
    - a. *Steps– Click the following:*
      - i. 'Reports'
      - ii. 'VC01'
      - iii. On the 'Organizations' Tab, Select an organization
      - iv. On the 'Vulnerabilities' Tab, Select IAVM(s) or year(s)
      - v. Review other options and select as desired
      - vi. 'Generate'

## 1.7.2 Additional Reports

The following reports can be used for identifying assets at a site or location and determine what IAVMs are related to specific assets. Quick step by step instructions for creating the reports follows.

- **AS01 - Identifying Assets**

**Note:** The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. These instructions are applicable to locating all assets but are geared toward Telecom/RTS assets.

  - a. *Steps – Click the following:*
    - i. 'Reports'
    - ii. 'AS01'
      - i. Select 'Computing', hold Ctrl key, and select 'Non-Computing' (SUBMIT)
      - ii. Select 'By Location' (SUBMIT)
    - iii. Select the location
      1. May want to do other reports if your site manages or owns assets that are not located at their site. Check the box for Child Locations if applicable. (SUBMIT)

- iv. Expand 'Non-Computing'
  1. Check the box for 'Telecom Policy'
- v. Expand 'Computing'.
  1. Check the box for 'Telecom'
- vi. Select 'Online', 'Offline', or 'Both'. Located under the right calendar ('Both' is recommended but 'Online' is the default)
- vii. Check the box for 'Show Detailed Asset Information' (Recommended - This will show a tree display of all postures that have been assigned to the asset during registration)
- viii. Check the box for 'Show System Administrator Information' (Recommended)
- ix. Submit to receive the Telecom/RTS Asset Report

**Note:** Reports are best displayed using the 'Output/Screen' option. The display may then be printed. Clicking the IE6 print function prints the report only without the surrounding frames. Using the 'Output/Export file' option produces a tab delimited text file. This file can be opened with excel to receive a database like table of the information. Use Right Click/Open With in Windows to open the file.

- **VL03 - Look at IAVMs assigned to an Operating System or Application**

**Note:** The VL03 report can assist the review by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. This can be accomplished by performing the following steps.

- a. *Steps– Click the following:*
  - i. 'Reports'
  - ii. 'VL03'
  - x. Select 'Select by Operating System/Application(s)'
  - xi. Select the OS(s) and Applications(s) to report on
  - xii. Select the environment (SUBMIT)
  - xiii. Select any additional display options or deselect the default selections
  - iii. 'Generate Report'

## 2 VULNERABILITIES AND IA REQUIREMENTS

**Note:** This STIG addresses configuration and operational requirements for VTC systems that use IP or ISDN or both for the transport of the VTC session. Not all requirements apply to both transport methods. Each vulnerability, check, and fix field is noted [IP], [ISDN], or [IP][ISDN] to indicate the applicability of the requirement to the transport method.

<b>STIG ID:</b> <b>RTS-VTC 1000.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017589</b>	<b>Severity:</b> <b>CAT III</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1000.00 [IP][ISDN]; DoD Access Control and Auditing Policy Compliance**

**Vul. Name:** VTC endpoints and other VTC system components do not comply with DoD 8500.2 IA Controls.

**Discussion:** DoD user/administrator account and password requirements are defined by the DoDI 8500.2 IA control IAIA-1, IAIA-2, IAAC-1, IAGA-1, as well as JTF-GNO Command Tasking Order (CTO) 06-02 as amended and any current INFOCON modifications. IA controls ECLO-1 and 2 provide policy for system/device logon controls, while IATS-1 and 2 provide policy requiring DoD Public Key Infrastructure (PKI) certificates along with physical tokens (i.e., Common Access Card (CAC) or Alternate Logon Token (ALT)) are used for system/device access, user identification, authentication, and non-repudiation. These policies address individual user/administrator accounts and user-IDs; two-factor authentication using CAC, other PKI based tokens (e.g., ALT), or the use of passwords, password strength, password history, password and account aging and lockout, account lockout for failed logon attempts, removal of unnecessary accounts, group accounts, and more.

IA controls ECPS-1 and ECLP-1 define policy for various levels of user and administrator authorization based on roles and the principal of least privilege. Additionally, IA controls ECAT-1, ECAR-1, 2, and 3, as well as ECTP-1 define DoD security auditing policy. Under these policies user and administrator actions that could affect security are to be recorded in a protected security or audit log. These IA controls rely on the successful implementation of individual user accounts and other required access control measures. Without individual user accounts and/or identities, to which actions can be tied, auditing of user/administrator actions becomes impossible. Examples of auditable actions include (but are not limited to) access to the system or device; access to, use of, or activation of services provided by the system or device; access to files on the system or device to include modification, deletion, name changes etc; access to configuration settings along with changes made. These auditing records are in addition to and separate from traditional telephony CDRs used for accounting purposes.

Based on the information presented in Table 3-1 in the STIG, we can see that VTC CODECs do not support most DoD requirements on all access points and features, if at all. This holds true for most other VTC system devices. As such, this does not negate the fact that all DoD ISs are subject to these policies that provide access controls, address vulnerabilities, and provide for user and administrator accountability. The purpose of the following requirement is to highlight the lack of such support in security readiness review as well as certification and accreditation reports. The balance of this document attempts to define mitigations to this lack of policy compliance to the greatest extent possible.

**Default Details:** A VTC device does not provide features or capabilities that would allow it to meet one or all of the following DoDI 8500.2 IA controls IAAC-1, IAIA-1 & 2, ECLO-1 & 2, ECWN-1, ECPA-1, ECPA-1, ECLP-1, ECAT-2, ECAR-1, 2, & 3, and ECTP-1

**Pot'l Impacts:** A DAA risks making an uninformed decision regarding the purchase and use of a VTC system or device because VTC endpoints or other VTC system components do not comply with DoDI 8500.2 IA controls.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 14.3 - Internal Enclave Network Security - Network Device Configuration

**Severity:** CAT III

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section, 3.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

- Checks:** RTS-VTC 1000.00 (Interview); [IP][ISDN] Interview the IAO to validate compliance with the following requirement:
- Ensure all VTC endpoints and other VTC system components comply with the following DoDI 8500.2 IA controls:
    - IAAC-1 Account Management
    - IAIA-1 & 2 Individual ID & Password
    - ECLO-1 & 2 lockout on logon failure
    - ECWN-1 Warning Banner
    - ECPA-1 Roles (privileged access)
    - ECLP-1 Least Privilege
    - ECAT-2 Security audit
    - ECAR-1, 2, & 3 Audit Content
    - ECTP-1 Audit Trail Protection
- Note:** The specific IA control deficiencies exhibited by a particular VTC system or device must be documented for use in the risk assessments that are necessary for a DAA to make an informed decision regarding the use of the system or device.
- APL Testing:** In the event an IA control on the above list fails when going through product review this check would be a finding.
- This check will result in a finding in most cases because VTC endpoints and other VTC system components have typically not provided support for IA beyond a password for access to configuration settings.
- The basic features for compliance with each IA control by any device are listed below. This list is not intended to be all inclusive nor does it contain all IA controls that might be applicable.
- IAAC-1 Account Management
    - Individual administrator and user accounts can be created and deleted.
    - Accounts age and lockout when age limits are exceeded.
  - IAIA-1 & 2 Individual ID & Password
    - Individual User ID and password required for logon by administrators and users alike in association with individual user accounts.
    - Strong passwords with specific configurable length and character type content
    - Passwords are required to be changed at regular configurable intervals and at first logon
    - Password history and aging
  - ECLO-1 & 2 Lockout on logon failure
    - User and admin accounts lockout after a configurable number of failed logon attempts
  - ECWN-1 Warning Banner
    - The standard DoD mandated warning banner must be displayed on the main VTC display prior to user or local admin logon
    - The standard DoD mandated warning banner must be displayed on all management interfaces, both local and remote.
  - ECPA-1 Roles (privileged access)
    - The system provides access to various functions and configuration levels based upon the role of the user or administrator as assigned to their user account.
    - The system minimally provides a user role and an administrator role
  - ECLP-1 Least Privilege
    - Works with ECPA in that users and administrators are provided access to only those commands and configuration settings required to perform their job.
  - ECAT-2 Security audit
    - The system records security related events in an audit log
  - ECAR-1, 2, & 3 Audit Content
    - The system records various types of security related events based upon the sensitivity of the system. Typically these include:
  - ECTP-1 Audit Trail Protection
    - The audit log is protected from access except by authorized persons
    - The audit log is encrypted
    - The audit log is not able to be edited or deleted.
- Fixes:** RTS-VTC 1000.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Purchase and implement VTC endpoints and other VTC system components that provide the IA features required by DoD policies. Encourage vendors to develop VTC systems and devices that provide robust IA features that support compliance with DoD policies for all devices.
- Responsibility:** DAA, IAM, IAO
- Mitigations:** N/A

**Not Reviewed:**  **Not Applicable:**  **Not A Finding:**  **Open Finding:**  **Fixed:**

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 1020.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017591</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1020.00 [IP][ISDN]; Power-Off the VTU When Inactive**

**Vul. Name:** Deficient SOP or enforcement regarding how to power-off the VTU when it is not actively participating in a conference.

**Discussion:** When the VTU is not active, it is best to power it off to mitigate its vulnerabilities. This may not be practical, particularly if the VTU is intended, or required, to receive un-scheduled incoming calls or is to be remotely managed and monitored in an un-scheduled manner. Receiving un-scheduled incoming calls that are automatically answered is, in itself, a vulnerability. This is an issue for IP and ISDN connected systems if auto-answer is on. The auto-answer feature is discussed later. Remote access and monitoring are also vulnerabilities due to the lack of strong access control mechanisms and the ease with which a VTU can be compromised if it is connected to an IP network. These vulnerabilities are discussed later. The point of this and the next requirement is to disable the capability of the VTU to "see and hear" information and activities located or occurring near the VTU when it is not actively participating in a call. While these vulnerabilities are of particular concern in an office or other work area, it may be of less concern in a conference room except if meetings occur in the facility that do not require the use of the VTC system.

**Default Details:** A VTU is not properly powered - off while not actively participating in a conference per the SOP.  
OR  
A VTU Standby/Power-off SOP is deficient, or non-existent, or is not enforced.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCSD-1 Security Design and Configuration/IA Documentation - All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).  
PEDI-1 Physical and Environmental/Data Interception - Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 12.1 - Configuration Management Policies - INFOCON Policy & Procedures

**Severity:** CAT II

**Sev. Override:** This can be deemed N/A or "Not a Finding" in the event there are validated, approved, and documented mission requirements; however, the VTU is still subject to RTS-VTC 1025.00. An example of a mission requirement needing validation, approval, and documentation would be a requirement for nightly testing of the VTU from a central location or a need to regularly answer incoming calls.

This is N/A if the VTU is located in a conference room that is only used for VTC conferences the room is empty when not preparing for or participating in a VTC; the room contains no sensitive or classified information when not in use; no other meetings are held there; and no other work or activities occur there.

**References:** DoD Video Tele-conference STIG, Section 3.2.2.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1020.00 (Interview); [IP][ISDN] Interview the IAO to validate compliance with the following requirement:

In the event the VTU is connected to an IP network and/or if auto-answer is on while connected to an ISDN network, ensure a policy and procedure is in place and enforced that requires users to power-off the VTU when it is not actively participating in a conference unless it is required to be powered-on to meet validated, approved, and documented mission requirements.

**Note:** While this requirement can be deemed N/A or "Not a Finding" in the event there are validated, approved, and documented mission requirements, the VTU is still subject to RTS-VTC 1025.00. An example of a mission requirement needing validation, approval, and documentation would be a requirement for nightly testing of the VTU from a central location or a need to regularly answer incoming calls.

**Note:** The documented and validated mission requirements along with their approval(s) are maintained by the IAO for inspection by auditors. Such approval is obtained from the DAA or IAM responsible for the VTU(s) or

system.

**Note:** This is not a requirement (i.e., N/A) if the VTU is located in a conference room that is only used for VTC conferences; the room is empty when not preparing for or participating in a VTC; the room contains no sensitive or classified information when not in use; no other meetings are held there; and no other work or activities occur there.

**Note:** Sleep mode does not fully mitigate the vulnerability addressed here unless it can be invoked by the user. Typically a VTU would go to sleep after a period of time. During this period, the vulnerability still exists and may exist in sleep mode depending upon what is required to wake the VTU. Sleep mode should be able to be initiated by the user. Exiting sleep mode should be initiated by user action and not an automated process. This functionality needs to be explored further and specific requirements defined.

**Note:** This requirement must be stated in user's guides and training because the user is the one that must implement these mitigations.

Inspect the SOP as well as user training materials, agreements, and guides to determine if the requirement is adequately covered. Interview the IAO to determine how the SOP is enforced. Interview a sampling of users to determine their awareness and implementation of the requirement and whether the SOP is enforced. Have a sampling of users demonstrate how to power-off the VTU when it is not actively participating in a conference. This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details. Have a sampling of users demonstrate how to power-off the VTU when it is not actively participating in a conference.

**Fixes:**

RTS-VTC 1020.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Define and enforce policy and procedure that when a VTU is connected to an IP network and/or if auto answer is on while connected to an ISDN network that the user is required and knows how to power-off the VTU when it is not actively participating in a conference unless it is required to be powered-on to meet validated, approved, and documented mission requirements.

Provide user training regarding this SOP and include it in user agreements and user guides.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1025.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017592</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1025.00 [IP][ISDN]; Disable the VTU When Powered & Inactive**

**Vul. Name:** Deficient SOP or enforcement for microphone and camera disablement when the VTU is required to be powered and inactive (in standby).

**Discussion:** In the event that mission requirements dictate the VTU be in a powered-on state when inactive (thereby making RTS-VTC 1020 N/A or "Not a Finding"), other measures are required to mitigate the vulnerability of possible VTU compromise and establish a defense in depth posture. These mitigations are, 1 - to mute the microphone and 2 - to disable the viewing capability of the camera in some manner. If the camera is movable, it could be aimed at the nearest corner of the room; however, this is no mitigation if the VTU is compromised or remotely controlled and the camera can be re-aimed into the room. The best mitigation for the camera is to cover the lens of the camera. This is applicable to both movable and fixed cameras.

**Default Details:** A VTU is not muted while not actively participating in a conference per the SOP.  
AND/OR  
The capability of the VTU's camera to view activities within the room has not been disabled per the SOP.  
OR  
A VTU Standby SOP is deficient, or non-existent, or not enforced.  
OR  
Documentation is deficient relating to Validated and approved mission requirements along with their DAA approval(s).

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCSD-1 Security Design and Configuration/IA Documentation - All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).  
PEDI-1 Physical and Environmental/Data Interception - Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices.  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 12.1 - Configuration Management Policies - INFOCON Policy & Procedures

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-conference STIG, Section 3.2.2.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1025.00 (Interview); [IP][ISDN] Interview the IAO to validate compliance with the following requirement:  
  
In the event the VTU is connected to an IP network and/or if auto-answer is on while connected to an ISDN network, AND the VTU is required to be powered-on to meet validated, approved, and documented mission requirements (that is RTS-VTC 1025.00 is "not a finding"); ensure a policy and procedure is in place and enforced that requires users to perform the following when the VTU is it is not actively participating in a conference:  
Mute the microphone.  
AND  
Disable the capability of the camera to view activities within the room as follows:  
Cover the camera(s) if its/their position/aim is fixed or able to be remotely controlled.  
OR  
Aim the camera(s) at a nearby corner where it/they cannot see room activities if the camera position/aim is movable but cannot be remotely controlled.

**Note:** The documented and validated mission requirements along with their approval(s) are maintained by the IAO for inspection by auditors. Such approvals are obtained from the DAA or IAM responsible for the VTU(s) or system. This documentation and validated mission requirements are the same documentation that renders RTS-

VTC 1020.00 N/A or "Not a Finding"

**Note:** This finding can be reduced to a CAT III in the event the camera(s) can be remote controlled but are aimed at the wall (e.g., a corner) where it/they cannot see room activities if the camera supports aiming or being moved. While the practice of aiming the camera at the side or back wall of the room where there is nothing to see and muting the microphone can mitigate normal operational issues, this measure is not a mitigation if the camera can be remotely controlled via auto-answer and Far End Camera Control (FECC) and/or the CODEC remote control/configuration feature is not configured properly, is compromised, or can be accessed by an administrator with the remote access password.

**Note:** This is not a finding in the event sleep mode provides the necessary disablement functions and is invoked by the user when the VTU is powered on or leaves the active state. This finding can be reduced to a CAT III finding in the event sleep mode provides the necessary disablement functions and the VTU enters sleep automatically within 15 minutes of when the VTU entered standby. This is still a finding because the vulnerability exists during the standby period.

**Note:** This is not a requirement (i.e., N/A) if the VTU is located a conference room that is only used for VTC conferences; the room is empty when not preparing for or participating in a VTC; the room contains no sensitive or classified information when not in use; no other meetings are held there; and no other work or activities occur there.

**Note:** A camera cover should be provided by the camera vendor and attached in such a manner that it is not easily detachable so that it cannot be easily lost. Alternately, the cover can be as simple as an opaque cloth of appropriate size or sewn such that it won't fall off easily. If the cover is detachable such that can be easily lost, a supply of replacement covers should be readily available.

**Note:** This requirement must be stated in site user's guides and training because the user is the one that must implement these mitigations.

Inspect the SOP as well as user training materials, agreements, and guides to determine if the items in the requirement are adequately covered. Interview the IAO to determine how the SOP is enforced. Interview a sampling of users to determine their awareness and implementation of the requirement and whether the SOP is enforced. This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

This is a finding if the VTU is found to be powered-on when inactive and the microphone and/or camera are not disabled.

This is a finding if there is no documented requirement that the VTU be powered-on or there are no approvals. Inspect the documentation relating to the DAA approvals for the validated, approved, and documented mission requirements that require the VTU to be powered-on while inactive.

This is a finding if there is no SOP regarding the disablement of the VTU microphone and camera when the VTU is not actively participating in a conference. Interview the IAO to determine if this requirement is covered in a SOP and user training/agreements. Interview a sampling of users to determine their awareness and implementation of the requirement.

**Fixes:**

RTS-VTC 1025.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Define and enforce policy and procedure that when a VTU is connected to an IP network and/or if auto answer is on while connected to an ISDN network AND the VTU is required to be powered-on to meet validated, approved, and documented mission requirements., that the user is required and knows how to disable the VTU microphone and camera when the VTU is not actively participating in a conference.

Provide user training regarding this SOP and include it in user agreements and user guides.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1027.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017593</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1027.00 [IP][ISDN]; Sleep Mode**

**Vul. Name:** Deficient VTU sleep mode configuration or operation.

**Discussion:** Sleep mode is the power conservation and semi-disabled state that some VTUs can enter after being on standby for a period of time. While in sleep mode, the VTU is still minimally powered and thereby could be remotely accessed, managed, compromised, or easily activated. For the purpose of our discussions, sleep mode is different from standby mode by the fact that in standby mode, by our definition, the VTU is not actively participating in a call but is ready to receive or place a call. Sleep mode, is a semi off state whereby most functions of the VTU are disabled to conserve power. If used to mitigate vulnerabilities and not just conserve power, sleep mode must have the characteristics noted in this requirement.

**Default Details:** Sleep mode is used to mitigate standby vulnerabilities but is deficient as follows:

- The CODEC's audio and video pickup/transmission capability is not disabled as follows:
  - > The microphone's audio pickup capability is not disabled.
  - > The camera's image capture capability is not disabled.
  - > The remote activation/control capabilities of the camera and microphone are not disabled.
- Auto-answer capabilities are not disabled.
- Exiting sleep mode does not require local user action such as pressing some button or key to activate the wakeup function.
- A wake-on-incoming-call feature wakes/activates the VTU to a fully active state without user action
- The VTU can be remotely accessed or managed during sleep mode, and one or more of the following controls are not in place:
  - > The VTU does not or is not configured to limit access to specific authorized IP addresses.
  - > Remote access permits the activation of the microphone and camera when this functionality is not required to meet validated, approved, and documented mission requirements.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices.  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 14.3 - Internal Enclave Network Security - Network Device Configuration

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section 3.2.2.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1027.00 (Interview); [IP][ISDN]; Interview the IAO to validate for CODEC compliance with the following requirement:

In the event sleep mode is to be used to mitigate standby vulnerabilities, ensure that sleep mode provides and/or is configured to provide the following functionality:

- The CODEC's audio and video pickup/transmission capability should be disabled as follows:
  - > Disable the microphone's audio pickup capability.
  - > Disable the camera's image capture capability.
  - > Disable remote activation/control capabilities of the camera and microphone.
- Auto-answer capabilities are disabled.
- Local user action is required to exit sleep mode such as pressing some button or key to activate the wakeup function.
- If a wake-on-incoming-call feature is available, it must not fully wake the VTU and may only provide an indication that there is an incoming call along with meeting the incoming call display requirement below so that the user can make an informed decision to wake the system and answer the call or not.
- In the event the VTU can be remotely accessed or managed during sleep mode, the following controls must be in place:
  - > The VTU must limit access to specific authorized IP addresses.
  - > Remote access must not permit the activation of the microphone and camera unless this functionality is required to meet validated, approved, and documented mission requirements.

**Note:** If the VTU meets the user activation/authentication and banner requirements stated later, these function

must be invoked when the VTU wakes.

**Note:** If the VTU has a sleep mode, in addition to the required capabilities noted above, it should have configurable settings that permit immediate user activation via a button press and an automatic activation with a configurable time frame that could be as short as 15 seconds or as long as several hours, or never. This would permit the sleep mode to be used as partial or full mitigation for the vulnerabilities addressed by the above two requirements. The various configurable settings could be used when the VTU is in different locations. For example, the short duration and/or user activation could be used in a classified environment.

APL Testing: This is a finding in the event this requirement is not supported by the VTU.

Have the IAO or SA demonstrate the configuration setting required to meet the individual features of this requirement.

Place the VTU in standby/sleep mode, place a call to the VTU, and view its responses.

**Fixes:**

RTS-VTC 1027.00 (Manual); [IP][ISDN]; Perform the following tasks:

Configure the VTU to provide the following functionality:

- The CODEC's audio and video pickup/transmission capability must be disabled as follows:
  - > Disable the microphone's audio pickup capability.
  - > Disable the camera's image capture capability.
  - > Disable remote activation/control capabilities of the camera and microphone.
- Auto-answer capabilities are disabled.
- Local user action is required to exit sleep mode such as pressing some button or key to activate the wakeup function.
- If a wake-on-incoming-call feature is available, it must not fully wake the VTU and may only provide an indication that there is an incoming call along with meeting the incoming call display requirement below so that the user can make an informed decision to wake the system and answer the call or not.
- In the event the VTU can be remotely accessed or managed during sleep mode, the following controls must be in place:
  - > The VTU must limit access to specific authorized IP addresses.
  - > Remote access must not permit the activation of the microphone and camera unless this functionality is required to meet validated, approved, and documented mission requirements.

**Note:** If the VTU meets the user activation/authentication and banner requirements stated later, these function must be invoked when the VTU wakes.

**Note:** If the VTU has a sleep mode, in addition to the required capabilities noted above, it should have configurable settings that permit immediate user activation via a button press and an automatic activation with a configurable time frame that could be as short as 15 seconds or as long as several hours, or never. This would permit the sleep mode to be used as partial or full mitigation for the vulnerabilities addressed by the above two requirements. The various configurable settings could be used when the VTU is in different locations. For example, the short duration and/or user activation could be used in a classified environment.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1030.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017594</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1030.00 [IP][ISDN]; Incoming Call Notification**

**Vul. Name:** Inadequate display of an incoming call notification such that the VTU user can make an informed decision to answer the call or not.

**Discussion:** In the event that mission requirements dictate the VTU be in a powered-on state when inactive the VTU becomes available to receive incoming calls (except possibly when sleeping). Additionally, if a VTU is connected to an IP network, it may be capable of receiving incoming calls while active. When a VTU receives an incoming call; the normal operation is that a notification of the incoming call is provided both audibly and visually. The visual notification typically includes a display of the source of the call. This can be a phone number or IP address. This information should be accompanied by an identification of the caller. While the source information is typically available from the network, the identity of the calling party associated with that information is typically contained in a locally accessible directory. If the source information is in the directory, the associated identity information is located and added to the display or displayed by itself. This directory is typically on the VTU or can be on a locally associated management or directory server. Directories must therefore be kept up to date with user information related to other VTUs with which any given VTU is expected to communicate. Ideally, the full identity of the caller is sent from the calling system for display on the called system even if there is no local directory entry.

Based upon the displayed information, the user of the VTU can make an informed decision and take appropriate action to answer the call, or not. Users must be trained to not answer calls from unknown sources in the event doing so could disclose sensitive or classified information in the area of the VTU or while engaged in a VTC session.

**Default Details:** The VTU DOES NOT display the source of the incoming call and to the extent possible, the identity of the caller, such that the user can make an informed decision to answer the call or not.  
OR  
Directories are NOT maintained with current information regarding user information related to other VTUs with which the VTU is expected to communicate unless calling VTUs provide the caller information along with the source information.  
OR  
Users are NOT trained to not answer incoming calls from unknown sources in the event doing so could disclose sensitive or classified information in the area of the VTU.  
OR  
Users are NOT trained to not answer incoming calls from unknown sources or sources that may not have appropriate clearance or a need-to-know during a conference since doing so could improperly disclose sensitive or classified information to the caller.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling – Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section 3.2.2.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1030.00 (Interview); [IP][ISDN] Interview the IAO to validate for compliance with the following requirement:

- If the VTU is capable of receiving incoming calls while inactive or while active, ensure the following:
  - The VTU displays the source of the incoming call and to the extent possible, the identity of the caller, such that the user can make an informed decision to answer the call or not.
  - Directories are maintained with current information regarding user information related to other VTUs with which the VTU is expected to communicate unless calling VTUs provide the caller information along with the source information.
  - Users are trained to not answer incoming calls from unknown sources in the event doing so could disclose sensitive or classified information in the area of the VTU.
  - Users are trained to not answer incoming calls from unknown sources or sources that may not have appropriate clearance or a need-to-know during a conference since doing so could improperly disclose sensitive or classified information to the caller.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU.

Interview the IAO and have him/her demonstrate on a sampling of the VTUs in the system

**Fixes:**

RTS-VTC 1030.00 (Manual); [IP][ISDN]; Perform the following tasks:

- Configure the VTU to display the source of the incoming call and to the extent possible, the identity of the caller, such that the user can make an informed decision to answer the call or not.
- Maintained directories with current information regarding user information related to other VTUs with which the VTU is expected to communicate unless calling VTUs provide the caller information along with the source information.
- Train users to not answer incoming calls from unknown sources in the event doing so could disclose sensitive or classified information in the area of the VTU.
- Train users to not answer incoming calls from unknown sources or sources that may not have appropriate clearance or a need-to-know during a conference since doing so could improperly disclose sensitive or classified information to the caller.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1040.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017595</b>	<b>Severity:</b> <b>CAT III</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1040.00 [IP][ISDN]; Auto-Answer Availability**

**Vul. Name:** Auto-answer feature is not administratively disabled.

**Discussion:** Some VTC endpoints have a user selectable feature that provides the capability to automatically answer an incoming call. This would be akin to your speakerphone picking up a call each time the phone rang allowing an ongoing conversation to be heard by the caller. This feature, if activated, is highly detrimental to the confidentiality of information in a room in which a VTU is installed. In fact, a security incident could result from "auto-answer" being enabled. Such would be the case in the event a VTU automatically answered a call when a classified meeting or discussion (not via VTC) was being held in a conference room or an office having VTC capability. The auto-answer feature must not be activated by a user unless the feature is required to satisfy mission requirements. Furthermore, users must be trained in the vulnerabilities associated with the auto-answer feature and in its proper use if it is to be used. The ideal mitigation for this vulnerability is for the auto-answer feature to not be supported by the VTU or there be an administrator setting that can disable the feature preventing a user from activating it.

**Default Details:** The auto-answer feature is enabled, but is not needed to fulfill validated, approved, and documented mission requirements  
OR  
Mission requirements are not validated, approved or documented regarding the use of an auto-answer feature  
OR  
An auto-answer feature exists that cannot be disabled.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling – Dissemination

**Severity:** CAT III

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section 3.2.2.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1040.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

If a VTC endpoint auto-answer feature is available, ensure it is administratively disabled, thus ensuring the feature is not selectable by the user, unless required to satisfy validated, approved, and documented mission requirements.

**Note:** The documented and validated mission requirements along with their approval(s) are maintained by the IAO for inspection by auditors. Such approval will be obtained from the DAA or IAM responsible for the VTU(s) or system.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU.

Verify that if the auto-answer feature is available on the VTU endpoint that it is administratively disabled. If the auto-answer is a mission requirement, verify that IAO has evidence/documentation that the DAA or IAM responsible has given written approval for its use.

**Fixes:** RTS-VTC 1040.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Administratively disable the auto-answer function on the VTU unless required to fulfill validated and approved mission requirements.

If auto-answer is required to fulfill validated and approved mission requirements, obtain written approval for the use of this function from DAA or IAM and maintain documentation on the validated requirement and approval.  
Train users in the proper use and vulnerabilities associated with the use of auto-answer

**Responsibility:** DAA and/or IAM, IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1060.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017596</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1060.00 [IP][ISDN]; Auto-Answer Use Mitigations**

**Vul. Name:** Deficient SOP for, enforcement, usage, or configuration of the auto-answer feature.

**Discussion:** In the event the auto-answer feature is approved for use or cannot be administratively disabled and thus is available for users to activate, several mitigating requirements must be met. The first of these is that the user(s) to which the feature is available must be trained in its proper use and in the vulnerabilities it presents because the user is the one that must implement the operational mitigations. The second is the VTU must answer the call with the microphone muted and with the camera covered or disabled. This will prevent an ongoing conversation from being heard and room activities seen by the caller. This will also prevent the room from being audibly and visually monitored if a call is automatically answered when the VTU is un-attended. The third mitigating requirement is that the user must be notified that the VTU has received and answered a call such that the user may be viewed if the camera is not/cannot be covered or listened to if the microphone is not/cannot be muted. This means that a noticeable visual indication must be provided and any available audible signal must be maintained at an audible level so that it can be heard.

**Default Details:** There is no SOP regarding the use of an approved auto-answer feature  
OR  
The "auto-answer with microphone muted" feature is not used or not available  
OR  
The user does not maintain the auto-answer signal at an audible level or such a feature is not available

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
DCSD-1 Security Design and Configuration/IA Documentation - All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and back-up, or emergency response).  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling – Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section 3.2.2.6

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1060.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

In the event the auto-answer feature is available and/or used, ensure a policy and procedure is in place and enforced such that, all of the following occurs:

- The auto-answer feature is configured to answer with the microphone muted.
- The camera is covered or otherwise disabled while waiting for a call.
- The VTU provides a visual indication that a call has been answered.
- The user will ensure the ringer or audible notification volume is set to an easily audible level or the VTU will automatically satisfy this requirement.
- The user(s) to which the feature is available is trained in its proper use as reflected in the SOP and in the vulnerabilities it presents.

**Note:** During APL testing, this is a finding in the event "auto-answer with microphone muted" is not configurable on the VTU. It is also desirable that this setting will ensure the audible notification is at a level to be easily heard.

Determine if this requirement is covered in a SOP and user training/agreements. Interview a sampling of users to determine their awareness and implementation of the requirement. Verify that, if supported, the VTU auto-answer feature is configured to answer with microphone muted.

**Fixes:** RTS-VTC 1060.00 (Manual); [IP][ISDN]; Perform the following tasks:

- In the event the auto-answer feature is approved for use, perform the following tasks:
  - Maintain full documentation on the validation of the mission requirement and the DAA approval to use the auto-answer feature
  - Develop and enforce a SOP regarding the proper use of the auto-answer feature.

- Configure the auto-answer feature to answer with the microphone muted.
- Ensure the camera is covered by the user or otherwise disabled automatically while waiting for a call.
- Ensure the VTU provides a visual indication that a call has been answered.
- Train users to ensure the ringer or audible notification volume is set and maintained at an easily audible level or the VTU automatically satisfies this requirement.
- Train the user(s) to which the feature is available in its proper use as reflected in the SOP and in the vulnerabilities it presents.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1080.01</b>	<b>VMS Vulnerability Key:</b> <b>V0016076</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1080.01 [IP][ISDN][PC]; SOP Microphone Operation**

**Long Name:** Deficient Policy or SOP regarding VTU and PC microphone operations and their pickup capability.

**Vulnerability Discussion:** Microphones used with VTC systems and devices are designed to be extremely sensitive such that people speaking anywhere within a conference room can be picked up and amplified so they can be heard clearly and understood at the remote location(s) on the call. This same sensitivity is included in VTUs that are used in office spaces. This has one disadvantage. The microphones can pick up sidebar conversations that have no relationship to the conference or call in progress. Likewise, in an open area, received conference audio can be broadcast to others in the area that are not part of the conference, and possibly should not be exposed to the conference information for need-to-know reasons. Speakerphones exhibit a similar vulnerability. This is the same confidentiality vulnerability posed to information in the environment as discussed above with the added twist that the conference audio is vulnerable to others in the environment. While this is more of an issue in environments where classified conversations normally occur, it is also an issue in any environment. This is of particular concern in open work areas or open offices where multiple people work in near proximity. Users or operators of VTC systems of any type must take care regarding who can hear what is being said during a conference call and what unrelated conversations can be picked up by the sensitive microphone(s). Where a VTU is used by a single person in an open area, a partial mitigation for this could be the use of a headset with earphones and a microphone. While this would limit the ability of others to hear audio from the conference and could also limit the audio pickup of unrelated conversations, it may not be fully effective. In some instances, such as when a VTU is located in a SCIF, a Push-to-Talk (PTT) handset/headset may be required.

Microphones embedded in or connected to a communications endpoint, PC, or PC monitor can be sensitive enough to pickup sound that is not related to a given communications session. They could pickup nearby conversations and other sounds. This capability could compromise sensitive or classified information that is not related to the communications in progress.

Speakers embedded in or connected to a communications endpoint or PC can be made loud enough to be heard across a room or in the next workspace (e.g., cube). This capability could compromise sensitive or classified information that is being communicated during a session.

Users must be aware of other conversations in the area and their sensitivity when using any communications endpoint, not only a PC based voice, video, or collaboration communications application. This awareness must translate into protecting or eliminating these other conversations. A short range, reduced gain, or noise canceling microphone may be required. A push to talk microphone may also be required for classified areas. The microphone should be muted when the user is not speaking as both a mitigation for this issue, and for proper etiquette when participating in a conference. The muting function should be performed using a positively controlled disconnect, shorting switch, or mechanism instead of a software controlled mute function on the PC.

Users must be aware of other people in the area that could hear what is being communicated. This is particularly an issue if the communicated information is sensitive or classified since the parties overhearing the information may not have proper clearance or a need-to-know. To mitigate this issue, a headset or speakers should be used and at a volume that only the user can hear.

**Default Details:** A policy and procedure is deficient or is not in place and/or enforced that addresses the operation of hardware based voice and video communications devices such as VTC endpoints and PC based voice, video, UC, and collaboration communications applications with regard to their audio pickup and broadcast capabilities in relation to the sensitivity of the information communicated.

**Pot'l Impacts:** The inadvertent transmission of sensitive or classified information within the pickup range of a microphone or broadcast range of a speaker used for audio communications resulting in the improper disclosure of sensitive or classified information.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECND-1 Enclave and Computing Environment/Network Device Controls - A network device control program/policies/SOPs/instructions/restrictions/protections/documentation

**Mgmt Category:** 11.2 - Information Handling – Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** Personal Computer Communications Client (PCCC) STIG v1r1, Section 2.4.2,  
Video Tele-Conference STIG, Section 3.2.3.1.

**Conditions:** Non-Computing – PC Communications Client Policy (Target: PC Communications Client Policy )  
Non-Computing – Video Tele-Conference Policy (Target: Video Tele-Conference Policy)

**Checks:** RTS-VTC 1080.01 (Interview); Interview the IAO to validate compliance with the following requirement:

Ensure a policy and procedure is in place and enforced that addresses the placement and operation of hardware based voice and video communications devices and PC based voice, video, UC, and collaboration communications applications with regard to their audio pickup and broadcast capabilities in relation to the sensitivity of the information communicated. Operational policy and procedures are included in user training and guides.

**Note:** This SOP should take into account the classification of the area where the VTU or PC supporting a PC based voice, video, UC, and collaboration communications applications is installed as well as the classification and need-to-know restraints of the information generally communicated via the facility or specific VTU. Along with those mentioned above, measures should be included such as closing office or conference room doors; muting of microphones before and after conference sessions, and during conference breaks; volume levels in open offices as well as muting the microphone when not speaking.

Inspect the applicable SOP.

Such an SOP should include policy on the use of headsets containing short range microphones and earphones in lieu of long range microphones and speakers in an open office environment. It should address the volume settings of speakers such that the session information is not heard by non-participants in a work area. It should also address the potential for the pickup of non-session related conversations in the work area.

Inspect user training materials and discuss practices to determine if information regarding the SOP is conveyed. Interview a random sampling of users to confirm their awareness of the SOP and related information.

This is a finding if the SOP or training is deficient.

**Fixes:** RTS-VTC 1080.01 (Manual); Produce an SOP that addresses the operation of hardware based voice and video communications devices and PC based voice, video, UC, and collaboration communications applications with regard to their audio pickup and broadcast capabilities in relation to the sensitivity of the information communicated.

Such an SOP should include policy on the use of headsets containing short range microphones and earphones in lieu of long range microphones and speakers in an open office environment. It should address the volume settings of speakers such that the session information is not heard by non-participants in a work area. It should also address the potential for the pickup of non-session related conversations in the work area.

Provide appropriate training such that users follow the SOP. Enforce user compliance with the SOP.

**Responsibility:** IAM, IAO

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1120.01</b>	<b>VMS Vulnerability Key:</b> <b>V0016074</b>	<b>Severity:</b> <b>CAT I</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1120.01 [IP][ISDN][PC]; SOP Camera Operation**

**Vul. Name:** Deficient Policy or SOP regarding VTC and PC camera operations and their pickup capability.

**Discussion:** Users of conference room or office based VTC systems and PC based communications applications that employ a camera must not inadvertently display information of a sensitive or classified nature that is not part of the communications session while the camera is active. This can happen if information in the form of charts, pictures, or maps are displayed on a wall within the viewing, or capture range of a camera. Any Pan, Tilt, and Zoom (PTZ) capabilities of the camera must be considered. One may consider visual information out of range, but it may be in range considering camera capabilities such as high definition, PTZ, and video enhancement possibilities for captured frames. Inadvertent display of classified information could also happen if the information is laying on a desk or table unprotected.

**Note:** Vulnerability awareness and operational training will be provided to users of VTC and video/collaboration communications related camera(s) regarding these requirements.

**Note:** This requirement is relevant no matter what the classification level of the session. In an IP environment the classification of VTC or PC communications is dependant upon the classification of the network to which the VTU or PC is attached, and the classification of the facility in which it is located. While classified communications can occur at the same level of classification as the network and facility, communications having a lower classification or no classification (e.g., unclassified or FOUO) may also occur in the same environment. As such, sensitive or classified information that is not part of the communications session might be improperly disclosed without proper controls in place.

**Default Details:** A policy and procedure is deficient or is not in place and/or enforced that addresses the operation of VTC or video/collaboration communications related cameras (e.g., PC webcams or VTC cameras) regarding their ability to inadvertently capture and transmit sensitive or classified information.

**Pot'l Impacts:** The inadvertent transmission of sensitive or classified information within view of a video camera used for video communications to individuals that have no need to see the communications resulting in the improper disclosure of sensitive or classified information.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment / Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration / Best Security Practices - system security design incorporates best security practices  
ECND-1 Enclave and Computing Environment / Network Device Controls - A network device control program / policies / SOPs / instructions / restrictions / protections / documentation

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT I

**Sev. Override:** NONE

**References:** Personal Computer Communications Client (PCCC) STIG v1r1, Section 2.4.1  
DoD Video Tele-Conference STIG, Section 3.2.3.2

**Conditions:** Non-Computing – PC Communications Client Policy (Target: PC Communications Client Policy)  
Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS- VTC 1120.01 (Interview); Interview the IAO to validate compliance with the following requirement:

Ensure a policy and procedure is in place and enforced that addresses the operation of video/collaboration communications related cameras (e.g., webcams or VTC cameras) regarding their ability to inadvertently capture and transmit sensitive or classified information such that:

- Conference room and office users do not display sensitive or classified information on walls that are within the view of the camera(s).
- Conference room and office users do not place sensitive or classified information on a table or desk within the view of the camera(s) without proper protection. (e.g., a proper cover)
- Conference room and office users do not read or view sensitive or classified information at such an angle that the camera(s) could focus on it.

**Note:** While covering such information mitigates disclosure when a camera is to be used, if the camera is activated unexpectedly or without taking action to cover the information prior to activating, the information can be compromised. Best practice is to not display it in view of the camera at all.

**Note:** Vulnerability awareness and operational training will be provided to users of video/collaboration communications related camera(s) regarding these requirements.

**Note:** This requirement is relevant no matter what the classification level of the session. In an IP environment the classification of PC communications is dependant upon the classification of the network to which the PC is attached, and the classification of the facility in which it is located. While classified communications can occur at the same level of classification as the network and facility, communications having a lower classification or no classification (e.g., unclassified or FOUO) may also occur in the same environment. As such, sensitive or classified information that is not part of the communications session might be improperly disclosed without proper controls in place.

Inspect the applicable SOP.

Inspect a random sampling of workspaces and conference rooms to determine compliance. Look for potentially sensitive information posted on the walls in view of the camera(s).

Interview the IAO to determine how the SOP is enforced. Inspect user training materials and discuss practices to determine if information regarding the SOP is conveyed. Interview a random sampling of users to confirm their awareness of the SOP and related information.

This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

**Fixes:**

RTS- VTC 1120.01 (Manual); Do not post potentially sensitive information posted on the walls in view of the camera(s).

Produce an SOP that addresses the operation of video/collaboration communications related cameras (e.g., webcams or VTC cameras) regarding their ability to inadvertently capture and transmit sensitive or classified information such that:

- Conference room and office users do not display sensitive or classified information on walls that are within the view of the camera(s).
- Conference room and office users do not place sensitive or classified information on a table or desk within the view of the camera(s) without proper protection. (e.g., a proper cover)
- Conference room and office users do not read or view sensitive or classified information at such an angle that the camera(s) could focus on it.

**Note:** while covering such information mitigates disclosure when a camera is to be used, if the camera is activated unexpectedly or without taking action to cover the information prior to activating, the information can be compromised. Best practice is to not display it in view of the camera at all.

Provide appropriate training such that users follow the SOP. Enforce user compliance with the SOP.

**Responsibility:** IAM, IAO

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1140.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017598</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1140.00 [IP][ISDN]; Incoming Calls While In a Conference**

**Vul. Name:** Deficient SOP or enforcement regarding handling of incoming calls while in a conference.

**Discussion:** Whether active or inactive, a VTU must display the source of an incoming call and the caller's identity so that the user can decide to answer the call or not. This decision must also be based upon what information would be made available to the caller when call is answered. The information that would be placed at risk is what can be picked up in the physical area of the VTU or what is being carried by the conference in which it is participating.

If the VTU is participating in a conference already, answering a call while in a conference would activate the VTU's integrated MCU and join the caller to the conference. The possibility of an incoming call being automatically joined to a meeting in progress in this manner places the confidentiality of that meeting at risk. The caller could become a participant of a meeting to which they were not invited and subsequently receive sensitive or classified information for which the caller may or may not have a need-to-know or appropriate security clearance.

As with a VTU in standby mode, an "auto-answer" feature is of great concern during a VTC session. A VTU must be configured in such a way that it cannot automatically answer a call and join the call to an active session without some form of access control. Either user intervention or a properly managed "local meeting" password is required to join such an incoming call to an active session. In some instances the "do-not-disturb" feature may be used by the user to block such calls by returning a "busy" signal. The capability of joining a conference on a VTU using its integrated MCU through the use of a "local meeting" password must be used only when the VTU user needs to pre-schedule and host a multipoint conference on his/her VTU. This capability must not be available at all times. The VTU should have the capability to disable this kind of access when it is not needed. Local meeting passwords must be used one time and not repeated. This requirement is discussed later.

**Default Details:** No SOP is in place and/or enforced that addresses the capability of a VTU to automatically answer a call during a conference  
OR  
The VTU does not support the automatic blocking of an incoming call during a conference as described in the requirement.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** PEDI-1 Physical and Environmental/Data Interception - Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.  
DCSD-1 Security Design and Configuration/IA Documentation - All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response).  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1140.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure the following regarding incoming calls while the VTU is engaged in a conference:  
- The VTU automatically rejects incoming calls, is administratively configured to return a "busy signal", or optionally does so through the use of a user selected "do-not-disturb" feature.  
OR  
- The VTU is configured to not automatically answer an incoming call and join it to an active conference (in progress) without user intervention. (i.e., the user must decide to answer the call or not based on the required source and caller information display. Answering the call affects the join).

OR

- A password, entered by the caller, is required to access the VTU's integrated MCU. This password must be unique among all other passwords used by the system. This capability must not be functional at all times, i.e., it is only to be functional when the capability is required to be used.

**Note:** In the event the VTU supports the "call-in/join via local meeting password" feature for the integrated MCU, the VTU should also have an administrative setting that disables this capability thereby forcing host action. In effect this setting would invoke an automatic "do-not-disturb" or return of a "busy" signal while the VTU is active. The various VTC vendors implement VTU integrated MCU access control differently.

Examples are as follows:

Tandberg – Dial out and dial in with host action only – no local meeting password option.

Polycom – Dial-out and Dial-in w/ "meeting password" which is required to join a multipoint call or streamed meeting. This is a memory location used to set the local MCU or streamed media access or join password for access to the VTU and to set the endpoint password given to another MCU when calling into it. "This field can also be used to store a password required by another system that this system calls."

**Note:** this pre-configurable "meeting password" violates unique and scripted password policies.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU as an administrator configurable option and/or as a default condition. The desired capability is to block incoming calls during a VTC session by default without requiring the user to set the condition since the user may forget to do so. The user may have the capability to set the condition that temporarily turns off the "do-not-disturb" feature such that the call can be answered externally to the conference and then manually joined.

Interview the IAO to determine if this requirement is covered in a SOP and user training/agreements. Interview a sampling of users to determine their awareness and implementation of the requirement. Place a call to an endpoint that is already in a conference and witness its response or reaction.

**Fixes:**

RTS-VTC 1140.00 (Manual); [IP][ISDN]; Perform the following tasks:

Ensure the following regarding incoming calls while the VTU is engaged in a conference:

- The VTU automatically rejects incoming calls, is administratively configured to return a "busy signal", or optionally does so through the use of a user selected "do-not-disturb" feature.

AND/OR

- The VTU is configured to not automatically answer an incoming call and join it to an active conference (in progress) without user intervention. (i.e., the user must decide to answer the call or not based on the required source and caller information display. Answering the call affects the join.)

AND/OR

- A password, entered by the caller, is required to access the VTU's integrated MCU. This password must be unique among all other passwords used by the system. This capability must not be functional at all times, i.e., it is only to be functional when the capability is required to be used.

**Responsibility:** IAM, IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 1160.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017599</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1160.00 [IP]; Disable VTU Remote Monitoring**

**Vul. Name:** Remote monitoring is not disabled while connected to an IP Network.

**Discussion:** Some VTC endpoints support the capability for an administrator or facilitator to view or monitor the VTU location (i.e., the room where it is located) remotely via a web interface. Some VTUs provide this feature via snapshots, while others provide the capability in real time. This feature can also include control capabilities and is used for troubleshooting, checking endpoints and rooms for operational readiness, or active monitoring of a call for quality control, etc. This capability poses a confidentiality issue for active conferences and the information in the proximity of the endpoints. Remote monitoring must be disabled as a general rule unless required to satisfy validated and approved mission requirements to prevent unauthorized access. This discussion also applies to administrator's endpoints fully participating in a call for reasons of troubleshooting or quality control.

**Default Details:** Remote monitoring is enabled but not required to satisfy validated and approved mission requirements.  
OR  
Remote monitoring is supported by the VTU but cannot be disabled while connected to an IP network.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a SA that is monitoring a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
PEDI-1 Physical and Environmental/Data Interception - Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1160.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:

In the event the VTU is connected to an IP network ensure remote monitoring of the VTU via IP is disabled unless required to satisfy validated, approved, and documented mission requirements.

**Note:** The documented and validated mission requirements along with their approval(s) are maintained by the IAO for inspection by auditors. Such approval is obtained from the DAA or IAM responsible for the VTU(s) or system.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU. i.e., remote monitoring must be able to be disabled or the feature/capability must not be supported.

Interview the IAO to determine if remote monitoring is required and approved to meet mission requirements. Have the IAO or SA demonstrate compliance with the requirement.

**Fixes:** RTS-VTC 1160.00 (Manual); [IP]; Perform the following tasks:  
- Obtain validation of mission requirements and DAA approval if remote monitoring of a VTU is to be used.  
OR  
- Configure the VTU to disable remote monitoring if the feature is not needed to satisfy validated, approved, and documented mission requirements.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1162.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017600</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1162.00 [IP]; VTU Remote Monitoring Password**

**Vul. Name:** Inadequate "operator/facilitator/administrator" access control for remote monitoring of a VTU connected to an IP network.

**Discussion:** Activation and use of remote monitoring and control features such as those discussed here and in RTS-VTC 1160.00 must be protected by access control. Minimally this must be the administrator password; however, access to this feature should not give full administrator access.

**Default Details:** Remote monitoring is required and enabled but does not require an administrator password for access control.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a SA that is monitoring a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems.  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.4.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1162.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:  
 In the event the VTU is connected to an IP network ensure access to IP remote monitoring and associated control functions of the VTU is minimally protected by a password.  
**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU. i.e., remote monitoring must be able to have a password set in order to access remote monitoring features.  
 Verify that an administrator password is required to access remotely accessible VTU. Have the IAO or SA demonstrate compliance with the requirement.

**Fixes:** RTS-VTC 1162.00 (Manual); [IP]; Perform the following tasks:  
 If IP remote monitoring is activated, configure the VTU to require a password before permitting access to the remote monitoring and associated control functions.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1164.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017680</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1164.00 [IP][ISDN]; Remote Monitoring Notification**

**Vul. Name:** Inadequate notification to conference participants (manual or automatic) of monitoring activity by someone that is not a direct participant in a VTC session/conference.

**Discussion:** Monitoring of a conference or VTC system can be performed in various ways. This can be by accessing the monitoring capabilities of a particular VTU via IP as discussed above, or using a capability of a centralized MCU, or an administrator or "operator/facilitator" can participate in a conference using a VTU. No matter how monitoring is being performed, participants in a call must be notified or be made aware that the call is being monitored by someone that is not a direct participant of the call or conference who therefore may not have a need-to-know regarding the conference information. This is a particular concern if the monitored conference contains classified information. If the monitoring is done by remotely accessing a VTU, typically, an automated notification is displayed on the VTU being monitored. This indication should also be displayed on all connected endpoints. Minimally, there is a SOP that requires the presence of a person monitoring a conference be announced to the conferees.

**Note:** This can minimally be accomplished via the enforcement of a SOP whereby the person performing the monitoring notifies the conference of their presence. Alternately, if an automated monitoring indicator is displayed on one VTU, the SOP must require that the participant or conferee seeing the indication announce the monitoring activity to the conference unless the indication appears on all participating endpoints.

**Default Details:** There is no automatic indicator or no SOP is in place or enforced to notify conferees of monitoring by someone that is not a direct participant of the conference.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a SA that is monitoring a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
PEDI-1 Physical and Environmental/Data Interception - Devices that display or output classified or sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information.

**Mgmt Category:** 11.2 - Information Handling – Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.4.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1164.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure conference participants are made aware that a conference is being monitored by someone that is not a direct participant of the call or conference.

Interview the IAO to determine if this requirement is covered by an automatic indicator that appears on all participating endpoints OR is covered in a SOP and user training/agreements. Interview the IAO and monitoring "operator/facilitator" to determine their awareness and implementation of the requirement.

**Fixes:** RTS-VTC 1164.00 (Manual); [IP][ISDN]; Perform the following tasks:  
- Configure the CODEC and/or MCU to automatically display an indication on all endpoints participating in a conference that the conference is being monitored.  
OR  
- Develop a SOP that addresses manual notification by SAs and chair persons that the conference is being monitored.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1168.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017681</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1168.00 [IP][ISDN]; Remote Monitoring Operator Clearance**

**Vul. Name:** Insufficient security clearance held by an "operator/facilitator/administrator" performing remote monitoring activities during a VTC session/conference.

**Discussion:** Administrators or "operators/facilitators" that perform monitoring as discussed in this section must have an appropriate security clearance commensurate with or higher than the classification level of the system and/or the information to which they are exposed.

**Default Details:** Remote monitoring "operator/facilitator" does not possess a security clearance that is the same or higher than the information to which they are exposed.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a SA that is monitoring a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** PRNK-1 Personnel/Access to Need-to-Know Information - individuals with a valid need-to-know granted access IAW Info owner restrictions.  
PRMP-2 Personnel/Maintenance Personnel - Classified IS - PRMP-1 + cleared to the highest level of IS, Cleared require an escort/authorized access. Lower cleared - a fully cleared and technically qualified escort monitors and records all activities. comply with DAA requirements for U.S. citizenship, which are explicit for all classified systems. PRMP-1 - Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel is documented.

**Mgmt Category:** 6.1 - Personnel - Clearance

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.4.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1168.00 (Interview); [IP][ISDN]; Interview the Administrator to validate compliance with the following requirement:  
 Ensure administrators that are required to monitor a conference or conferences possess a security clearance that is the same as or higher than the VTC system and the conference information to which they are exposed.  
 Verify with IAO that conference call operator/facilitator has security clearance commensurate with or higher than the classification level of the system and/or the information to which they are exposed.

**Fixes:** RTS-VTC 1168.00 (Manual); [IP][ISDN]; Perform the following tasks:  
 Ensure administrators that are required to monitor a conference or conferences possess a security clearance that is the same as or higher than the VTC system and the conference information to which they are exposed.

**Responsibility:** IAO, user

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1180.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017682</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1180.00 [IP][ISDN]; Far End Camera Control**

**Vul. Name:** Far end camera control is not disabled.

**Discussion:** Many VTC endpoints support Far End Camera Control (FECC). This feature uses H.281 protocol which must be supported by both VTUs. Typically, this is only available during an active VTC session but could be available if the VTU is compromised or if a call is automatically answered. Allowing another conference attendee to take control of your camera can place the confidentiality of non conference related information at risk. FECC should be disabled to prevent the control of the near end camera by the far end unless required to satisfy validated mission requirements.

**Default Details:** Far end camera control is enabled but not required to satisfy validated mission requirements.  
OR  
Far end camera control is supported by the VTU but cannot be disabled.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices.  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 – Information Handling – Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.3.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1180.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure far end camera control is disabled unless required to satisfy validated, approved, and documented mission requirements.

**Note:** The documented and validated mission requirements along with their approval(s) are maintained by the IAO for inspection by auditors. Such approval is obtained from the DAA or IAM responsible for the VTU(s) or system.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU. i.e., far end camera control must be able to be disabled or the feature must not be supported.

Determine if remote monitoring is required and approved to meet mission requirements. Have the IAO or SA demonstrate compliance with the requirement.

**Fixes:** RTS-VTC 1180.00 (Manual); [IP][ISDN]; Perform the following tasks:

Configure the CODEC to disable far end camera control

OR

Document and validate the mission requirements that require far end camera control to be enabled and obtain DAA approval. Maintain the requirement and approval documentation for review by auditors.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1220.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017683</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1220.00 [IP][ISDN]; Encryption of Media**

**Vul. Name:** VTC media is not encrypted.

**Discussion:** DoDI 8500.2 IA control ECCT-1 for “Enclave and Computing Environment/Encryption for Confidentiality (Sensitive Data in Transit) states “Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2).” [ed. DCSR-2 Specified Robustness – Medium; Type-3].

DoDI 8500.2 IA control ECCT-2 for “Enclave and Computing Environment/Encryption for Confidentiality (Classified Data in Transit) states “Classified data transmitted through a network that is cleared to a lower level than the data being transmitted are separately encrypted using NSA-approved cryptography (See also DCSR-3).” [ed. DCSR-3 Specified Robustness – High; NSA Type-1].

Furthermore, DoDI 8500.2 IA control ECNK-1 for “Enclave and Computing Environment/Encryption for Need-To-Know states “Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT. (ed. Encryption for confidentiality data in transit).”

DoDI 8500.2 IA control ECCT-2 primarily applies to classified data traversing the IP WAN (i.e., Defense Information Systems Network (DISN)) or other transport media such as a TDM based circuit switched network. The IP WAN is protected by NSA type 1 encryptors that bulk encrypt the circuits or links that interconnect the local classified enclaves or LANs. Separation of traffic for need-to-know purposes, while traversing these classified IP LANs and links, is covered by IA control ECNK-1. On the other hand, Dial-up VTUs that process classified information implement ECCT-2 by utilizing a NSA type 1 encryptor at each VTU and each port of a MCU if applicable.

The “NIST-certified cryptography” referred to by these IA controls is cryptography validated to Federal Information Processing Standard (FIPS) 140-2 as validated through the National Institute of Standards (NIST) Cryptographic Module Validation Program (CMVP).

In the early days of VTC, CODECs did not support confidentiality of the media or signaling streams directly. As security and conference confidentiality have become an IA issue in recent years, VTU vendors have standardized on DES and AES as encryption standards for VTC media streams. H.235 has been developed to help to secure the signaling protocols used in the H.323 suite of protocols. Most if not all VTC media traffic is considered to be sensitive information requiring protection under the IA controls discussed above. ECNK-1 applies to such traffic while traversing any network with any classification level (e.g., NIPRNet, SIPRNet, JWICS). ECCT-1 specifically applies to such traffic traversing any commercial or wireless network (e.g., Internet, 802.11 WLAN, or cellular network) but should also be considered as a requirement for traversal of the NIPRNet.

At minimum, and if supported by both endpoints in a point-to point conference, or all endpoints and the MCU in a multipoint conference, encryption must be used for media encryption. The encryption algorithm required is AES for two reasons. The first is that DES has been cracked and is no longer approved for Federal Government use, and the second is to satisfy DoDI 8500.2 IA control ECCT-1 and ECNK-1; Type-3 encryption of data in transit for confidentiality and need-to-know.

Unfortunately, there is a lot of legacy VTC gear in use today that either only supports DES or has no encryption capability at all. To support this situation, newer CODECs typically have three encryption options. ON, OFF, or automatic/negotiate. The preferred setting is ON and should be used if it is known that all other VTUs that a VTU needs to communicate with support encryption. Auto/negotiate is the preferred setting if this is not known.

In reality, however, any encryption, AES or DES, is better than no encryption at all and must be used if available. Many VTUs provide the capability to select the type of encryption used and may also provide an auto-negotiate mode. If it is known that all other VTUs that a VTU needs to communicate with uses AES encryption, AES should be selected. DES should never be selected if AES is available. Auto/negotiate is the preferred setting if it is not known which algorithm the other VTUs will use.

**Note:** The sensitivity of conference information is determined by the information owner(s), (that is the organizer and/or the presenting participants in the conference). As such, information owners might decide that their conference information is not sensitive enough to warrant confidentiality through the use of commercial encryption. Even so, encryption should be used and configured if available for those information owners that need to protect their information. Using encryption by default will provide the desired protection for those information owners that need it and will provide additional protection for those that don't feel it is necessary due to the non sensitive nature of their information.

**Default Details:** The VTC media (audio, video, presentation, whiteboard) is not encrypted even though encryption is supported.  
OR  
All communicating VTUs support type-3 encryption however encryption is to NOT set to ON.

OR  
It is unknown that all communicating VTUs support encryption however encryption is to NOT set to Auto/Negotiate.  
OR  
All communicating VTUs support AES encryption however AES is to NOT the selected algorithm.  
OR  
It is unknown that all communicating VTUs support AES encryption however the encryption algorithm to NOT set to Auto/Negotiate.  
OR  
[ISDN only] A legacy MCU or VTU will not interoperate using native/internal encryption.  
OR for APL testing:  
The CODEC does not support encryption or it supports DES encryption only.  
OR  
The CODEC does not support auto-negotiation of encryption capabilities.  
AND/OR  
The CODEC does not provide a FIPS 140-2 validated encryption module.

**Pot'l Impacts:** The disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECCT-1 Enclave and Computing Environment/Encryption for Confidentiality (SBU Data in Transit - in commercial OR wireless network) NIST-certified cryptography (Type 3 = FIPS) + Medium Robustness (DCSR-2 )  
ECNK-1 Enclave and Computing Environment/Encryption for Need-To-Know (SBU or classified info in Transit - at same class level as network) Min. NIST-certified cryptography (Type 3 = FIPS)DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 8.1 - Encryption & Data Integrity - Encrypted Data in Transit

**Severity:** CAT II

**Sev. Override:** [ISDN] This can be reduced to a CAT III for legacy ISDN/dialup MCU(s) and/or VTU(s) in the event they will not interoperate using native/internal encryption. This is typical between equipment of different vendor's legacy equipment. This can be mitigated using external encryption devices as with a secure/non-secure VTC system.  
[Classified IP] Understanding that classified IP networks are only protected with NSA type-1 encryption on WAN links between classified enclaves (LANs/CANs); This is "Not a Finding" if the VTU is connected to a classified IP network(s) AND conference information owner(s) have determined that the conference information does not require confidentiality or protection for need-to-know from others connected to the same network(s) AND conference information owner(s) have provided written confirmation of the decision that encryption is not necessary within the classified enclave (LAN/CAN).  
[Unclassified IP] Due to the fact that unclassified networks such as NIPRNet connected enclaves (LANs/CANs) are generally accessible to, and able to be compromised from, a public network like the Internet, native encryption is required if supported by the CODEC unless one of the following conditions are met:  
- The entire VTC system to include endpoints and MCUs are on a physically separate network from the enclave's general business (or other) LAN with dedicated point-to-point circuits outside the enclave to interconnect to MCUs and other endpoints. In this case, this is "Not a Finding" because the VTC information is protected.  
- The entire VTC system to include endpoints and MCUs are on a logically separate network on the enclave's general business (or other) LAN using a dedicated and closed VTC VLAN and protected on the WAN using an encrypted VPN between endpoints directly and/or between endpoints and the MCU. In this case, this is "Not a Finding" because the VTC information is protected.  
- Every possible user of the VTC system who is an information owner (that is meeting owner/organizer or presenter) designates that their information is publicly releasable or agrees that that their non-public information will not be protected from compromise via the use of encryption. (That is conference information owner(s) have provided written confirmation of the decision that encryption is not necessary.) In this case, this is a CAT III due to the fact that the VTC information is NOT protected.  
During APL testing:  
- This is a CAT I finding in the event the CODEC does not support multi-vendor interoperable encryption or it supports DES encryption only. (This applies only to new, non-legacy products submitted for testing.)  
- This is a CAT II finding in the event the CODEC does not support auto-negotiation of encryption capabilities and/or the CODEC does not provide a FIPS 140-2 validated encryption module.

**References:** DoD Video Tele-Conference STIG, Section: 3.2.4.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1220.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure the strongest type-3 (commercial grade) encryption algorithm is used to protect all VTC media streams as supported by all communicating VTUs and associated MCUs.

**Note:** It is recognized that legacy devices with which an endpoint might communicate may not support encryption or may only support DES instead of AES as preferred. Therefore the VTU must be configured in such a manner that if AES is available on all communicating VTUs the endpoint will use, or negotiate the use of, AES. If AES is not available on all communicating VTUs the endpoint may negotiate to use DES or no encryption. While the use of DES in lieu of no encryption is preferred, it is not required in this situation unless already supported by the VTU. This is because the use of DES is somewhat better than no encryption at all, even if marginally so.

**Note:** [ISDN] This can be reduced to a CAT III for legacy ISDN/dialup MCU(s) and/or VTU(s) in the event they will not interoperate using native/internal encryption. This is typical between equipment of different vendors. This can be mitigated (and considered not a finding) using external encryption devices as is historically done with secure/non-secure VTC systems.

**Note:** [Classified IP] Understanding that classified IP networks are only protected with NSA type-1 encryption on WAN links between classified enclaves (LANs/CANs); This is not a finding if the VTU is connected to a classified IP network(s) AND conference information owner(s) have determined that the conference information does not require confidentiality or protection for need-to-know from others connected to the same classified network(s) AND conference information owner(s) have provided written confirmation of the decision that encryption is not necessary within the classified enclave (LAN/CAN).

**Note:** [Unclassified IP] Due to the fact that unclassified networks such as NIPRNet connected enclaves (LANs/CANs) are generally accessible to, and able to be compromised from, a public network like the Internet, native encryption is required if supported by the CODEC unless one of the following conditions are met:

- The entire VTC system to include endpoints and MCUs are on a physically separate network from the enclave's general business (or other) LAN with dedicated point-to-point circuits outside the enclave to interconnect to MCUs and other endpoints. In this case, this is "Not a Finding" because the VTC information is protected.
- The entire VTC system to include endpoints and MCUs are on a logically separate network on the enclave's general business (or other) LAN using a dedicated and closed VTC VLAN and protected on the WAN using an encrypted VPN between endpoints directly and/or between endpoints and the MCU. In this case, this is "Not a Finding" because the VTC information is protected.
- Every possible user of the VTC system who is an information owner (that is meeting owner/organizer or presenter) designates that their information is publicly releasable or agrees that their non-public information will not be protected from compromise via the use of encryption. That is conference information owner(s) have provided written confirmation of the decision that encryption is not necessary. In this case, this is a CAT III due to the fact that the VTC information is NOT protected.

**Note:** During APL testing,

- This is a CAT I finding in the event the CODEC does not support encryption or it supports DES encryption only. This applies only to new, non-legacy products submitted for testing.
- This is a CAT II finding in the event the CODEC does not support auto-negotiation of encryption capabilities and/or the CODEC does not provide a FIPS 140-2 validated encryption module.

Determine if the various VTUs with which the system under review is expected to communicate and support Type-3 (commercial grade) encryption and/or the AES algorithm. From this information, determine the appropriate settings required to fulfill the requirement. Have the IAO or SA demonstrate the appropriate settings.

**Fixes:**

RTS-VTC 1220.00 (Manual); [IP][ISDN]; Perform the following tasks:

If it is known that all VTUs and MCUs that are expected to communicate support AES encryption; Configure VTUs and MCUs to encrypt media using AES.

OR

If it is NOT known if all VTUs and MCUs that are expected to communicate support AES encryption; Configure VTUs and MCUs to auto-negotiate encryption capabilities with AES as the preferred method.

OR

If it is known that all VTUs and MCUs that are expected to communicate cannot be configured to interoperate using encryption:

> Implement external (to the CODEC) encryption devices as is done with ISDN only secure/non-secure VTC systems

OR

> Develop a segregated/dedicated network infrastructure to protect sensitive VTC media (information)

OR

> Obtain, in writing, a statement from all users of the VTU(s) or MCU(s) that either their information is not sensitive enough to warrant encryption protection for confidentiality and/or need-to-know OR an acknowledgment that they are aware that their sensitive information will not be protected by encryption.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1230.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017684</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1230.00 [IP][ISDN]; Use FIPS 140-2 Validated Encryption**

**Vul. Name:** VTU does not use or provide FIPS 140-2 validated encryption module.

**Discussion:** The current DoD requirement for commercial grade encryption is that the encryption module, which includes a FIPS 197 validated encryption algorithm plus "approved functions" (i.e., key management and sharing/distribution functions), be NIST validated to FIPS 140-2. It must be noted that legacy equipment validated to FIPS 140-1 may still be used and FIPS 140-3 is in development.

While many VTU vendors support AES, they have only validated the algorithm to FIPS-197, if at all. This does not meet the FIPS 140-2 requirement because the additional "approved functions" have not also been addressed.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU.

**Default Details:** A VTU does not use or provide a FIPS 140-2 validated encryption module.

**Pot'l Impacts:** The disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECCT-1 Enclave and Computing Environment/Encryption for Confidentiality (SBU Data in Transit - in commercial OR wireless network) NIST-certified cryptography (Type 3 = FIPS) + Medium Robustness (DCSR-2 )  
ECNK-1 Enclave and Computing Environment/Encryption for Need-To-Know (SBU or classified info in Transit - at same class level as network) Min. NIST-certified cryptography (Type 3 = FIPS)DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 8.1 - Encryption & Data Integrity - Encrypted Data in Transit

**Severity:** CAT II

**Sev. Override:** For APL testing and new installations of new (non-legacy) equipment, this finding can be reduced to a CAT III in the event the crypto module in use is in the FIPS validation process as listed on the NIST CMVP "modules in Process" web site. <http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>. The POA&M for closing the finding must indicate the expected date that the module will achieve validation and the process to ensure the module in use is the validated module.

**References:** DoD Video Tele-Conference STIG, Section: 3.2.4.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1230.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure VTUs under his/her control employ encryption module(s) validated to FIPS 140-2.

Determine if the various VTUs with which the system under review is expected to communicate support and are using FIPS 140-2 validated encryption modules and that they are operated in FIPS mode. Have the IAO or SA demonstrate and verify that the VTU is using 140-2 encryption in FIPS mode. Review documentation from the vendor designating the encryption modules in use and verify that they are listed on the NIST CMVP "validated modules" web site. <http://csrc.nist.gov/groups/STM/cmvp/validation.html>

**Note:** For APL testing and new installations of new (non-legacy) equipment, this finding can be reduced to a CAT III in the event the crypto module in use is in the FIPS validation process as listed on the NIST CMVP "modules in Process" web site. <http://csrc.nist.gov/groups/STM/cmvp/inprocess.html>. The POA&M for closing the finding must indicate the expected date that the module will achieve validation and the process to ensure the module in use is the validated module.

**Fixes:** RTS-VTC 1230.00 (Manual); [IP][ISDN]; Perform the following tasks:

Purchase and install only those VTUs and MCUs that employ an encryption module(s) validated to FIPS 140-2 standards. Upgrade/replace old non compliant devices.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1250.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017685</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1250.00 [IP][ISDN]; Encryption Indicator**

**Vul. Name:** VTU encryption indicator is not enabled.

**Discussion:** In support of the need for encryption and the need for the VTU user to be aware that in fact his/her conference session is being encrypted, the VTU must display an indicator that encryption is indeed occurring.

**Default Details:** VTU visual indicator that encryption is occurring is not enabled.  
OR  
VTU is not capable of visually displaying an encryption indicator.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** This is not a finding in the event encryption is provided by external devices (not the CODEC), AND an external indicator is used to display encryption status in place of an on-screen indicator provided by the CODEC.

**References:** DoD Video Tele-Conference STIG, Section: 3.2.4.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1250.00 (Manual); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure all VTU's under IAO's control display a visual indicator that encryption is in fact taking place.  
**Note:** During APL testing, this is a finding in the event this requirement is not supported by the CODEC i.e., an on screen visual indicator displaying that encryption is indeed occurring.  
**Note:** In the event encryption is provided by external devices (not the CODEC), an external indicator meets this requirement in place of the on-screen indicator.

**Fixes:** RTS-VTC 1250.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Implement VTU CODECs that provide an on screen indicator that encryption is occurring and active.  
OR  
If the encryption is provided by external devices (not the CODEC), implement an external indicator to display encryption status in place of an on-screen indicator provided by the CODEC.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 1260.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017686</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 1260.00 [IP][ISDN]; User Validation Of Encryption**

**Vul. Name:** Deficient SOP or enforcement for user validation that encryption is on when required

**Discussion:** When encryption is enabled via automatic/negotiate, and one endpoint does not support encryption or supports DES and not AES, the entire conference defaults to the lower capability level. This is not acceptable for some conferences depending upon the sensitivity of the information discussed or presented. As noted above, the stated DoD IA controls require encryption. To ensure this requirement is met, when it is unknown whether all endpoints in a conference support encryption and whether it is turned on, the VTU user must provide the final check that encryption is being used. If a conference is to be encrypted, the user must check that all participants are using encryption and have enabled the encryption on their devices. When the conference has begun, the user must ensure that the conference is encrypted. The alternate to this is to exclude the endpoint that does not support the required encryption or not proceed with the conference session.

**Default Details:** A user validation SOP for VTU encryption is deficient, non-existent, or is not enforced.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 8.3 - Encryption & Data Integrity - Encryption Boundary

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.2.4.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 1260.00 (Manual); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure a policy and procedure is in place and enforced that addresses user activation and verification of encryption use when encryption is required based on the sensitivity of the information discussed or presented.

The following must be included:

- The user must check that all participants are using encryption and have enabled the encryption on their devices if manual activation necessary.
- When the conference has begun, the user must ensure that the VTU is displaying the “conference is encrypted” indication.

**Note:** This requirement must be reflected in user training, agreements and guides.

Verify that there is a policy and procedure in place that enforces and guides users on how and what to check when participants are required to use encryption.

**Fixes:** RTS-VTC 1260.00 (Manual); [IP][ISDN]; Perform the following tasks:

Define and enforce policy and procedure that addresses user activation and verification of encryption use when encryption is required based on the sensitivity of the information discussed or presented. The following must be included:

- The user must check that all participants are using encryption and have enabled the encryption on their devices if manual activation necessary.
- When the conference has begun, the user must ensure that the VTU is displaying the “conference is encrypted” indication.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2020.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017687</b>	<b>Severity:</b> <b>CAT I</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2020.00 [IP][ISDN]; Change Default Passwords**

**Vul. Name:** Default passwords are not changed.

**Discussion:** DoDI 8500.2 IA controls IAIA-1 and IAIA-2 state, in part: "Ensure all factory set, default, standard or well-known user-IDs and passwords are removed or changed."

Factory default, well-known, and/or manufacturer backdoor accounts and their associated passwords provide easy unauthorized access to system/device. Leaving such accounts and passwords active on a system/device makes it extremely vulnerable to attack and/or other unauthorized access. As such, they need to be removed, changed, renamed, or otherwise disabled.

Also covered by this policy are "community strings", which act as passwords for monitoring and management of network devices and attached systems via SNMP. The universal default SNMP community strings are "public" and "private" and are well known.

Default access for VTC operation, local and remote control, and management/configuration purposes is typically unrestricted or minimally protected by well known and well published default passwords. It has been demonstrated that not changing these passwords is the most common cause of VTC system compromise.

**Default Details:** Default passwords have not been changed providing an easy access and means of compromise of the VTU configuration or VTC session

**Pot'l Impacts:** Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT I

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2020.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure all default/factory passwords and SNMP community strings are changed or replaced prior to the VTU being placed into service

**Note:** New passwords will be in compliance with the individual password requirements defined in this document.

**Note:** During APL testing, this is a finding in the event default passwords cannot be changed on VTC/VTU.

Have the IAO or SA demonstrate logging onto the VTU via local and remote access methods. Look for the use of the following typical default passwords: "TANDBERG", the serial number, "admin", "1234", "none", etc.

**Fixes:** RTS-VTC 2020.00 (Manual); [IP][ISDN]; Perform the following tasks: Change all system passwords to non-default settings before placing the VTU into service.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2022.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017688</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2022.00 [IP][ISDN]; Password Display during Logon**

**Vul. Name:** Passwords are displayed in clear text when logging onto a VTU.

**Discussion:** As any information is entered on a keyboard, the keyboard sends each keystroke to the processing unit which, typically, echoes the character represented by the keystroke to the display device as feedback to the system's user. Such echoing is done in what is called "clear text" in that you can read what was entered. This process is used for normal typing, but must be changed when entering passwords. When passwords are displayed (echoed) during logon, the risk of password compromise is increased and password confidentiality is greatly reduced. If the password is displayed during logon, it can easily be compromised through the use of a simple technique of shoulder surfing, i.e., a third party witnessing the logon could view the echoed password and remember it or write it down. This could also happen through surveillance methods. This presents a major vulnerability to the security or confidential nature of the password. To mitigate this, when entering a password, the characters that are echoed to the display must be something other than the clear text characters. Typically an asterisk or other punctuation character is used to replace the actual characters in an echoed password. The prevention of shoulder surfing is in support of DoDI 8500.2 IA control IAIA-1's requirement to protect passwords from disclosure.

**Default Details:** Passwords are displayed in the clear when logging in, providing for risk of password compromise.

**Pot'l Impacts:** Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2022.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure users' or administrators' passwords are not displayed in the clear (i.e., echo a single alternate symbol instead of the actual characters used as they are entered) when logging onto a VTU locally or remotely.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU.

Have the IAO or SA demonstrate logging onto the VTU via local and remote access methods. Look for passwords that are displayed in the clear.

**Fixes:** RTS-VTC 2022.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Implement VTUs that do not display password in the clear when logging in via any interface. If existing devices do not support this behavior, upgrade as soon as possible.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2024.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017689</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

## RTS-VTC 2024.00 [IP][ISDN]; Password/PIN Strength or Complexity

**Short Name:**

**Vul. Name:**

Passwords do not meet complexity or strength.

**Discussion:**

DoD policy mandates the use of strong passwords. IA control IAIA-1&2 item 2 states "For systems utilizing a logon ID as the individual identifier, ensure passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!)."

DoDI 8500.2, therefore, sets the minimum complexity requirement for a character based password. This minimum complexity is reiterated by CJCSM 6510.01, C-A, Section 4 which adds the recommendation that "If technically feasible, 12 to 16 characters using a mix of all four-character sets is recommended (e.g., 14 characters using a mix of all four-character sets in the first 7 characters and the last 7 characters)."

In some circumstances, policies change as is the result of JTF-GNO CTO 06-02 which has set the minimum password complexity (for systems not using DoD PKI) to 9 characters with "a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters. This policy may again be updated to require 15 characters for some systems or devices that do not support CAC/PKI logon where required.

Additionally, in situations such as when INFOCON levels are raised, additional requirements can be implemented. An example of this is that in the recent past, the minimum password length was raised from 9 to 15 characters. When the INFOCON level returned to normal, password length reverted to 9 characters. IA requirements can be increased and decreased in conjunction with adjustments in INFOCON levels. Such adjustments in policy and INFOCON level changes will first be reflected in the checklist associated with an effected STIG and subsequently in a STIG update if the change is permanent.

While VTC endpoints today typically do not require a username, they do require a password for user access and authentication. The strength of these passwords is an issue for VTUs and is dependant upon the method of entry.

The local VTU passwords are entered using the hand-held remote control. The remote control typically has a dial-pad like a telephone and not a full QWERTY keyboard. Using the dial-pad, a user is capable of entering numbers, letters, and two special characters, the \* and # signs. Letter entry requires pressing a number key multiple times to scroll through the number and three or four associated letters until the correct letter is accessed. This is the same as text entry on a cell phone. To ensure accuracy of this process, the characters must be displayed on the screen as they are entered. Another method is to utilize an on-screen keyboard that is navigated using arrow keys on the remote control. While these methods are usable for entering names and other information in places such as the directory, it is not usable for password entry. This is because passwords must not be echoed to the screen to prevent password compromise by another person having a view of the screen while entry is taking place. Additionally, password characters can be shoulder surfed as they are entered if the on-screen keyboard method is used. This reduces the password to a number. It is better to protect a number from shoulder surfing than to require a strong password entered locally. Such a number is considered a Personal Identification Number (PIN) not a password. While there is the possibly of using the \* and # characters, these characters typically signal special functions in some types of systems, particularly telephone systems. These could be used if, during PIN entry, they do not trigger some other function.

Strong passwords along with other measures, as noted in DoD policy, are required for any access method that is received by the VTU across a network. This is because of the potential that a password could be broken by a variety of high speed cracking attacks. Due to the inability to use letters, PINs are very weak passwords. One would think that a PIN should be extra long to make them harder to break. This is not the case if they are not required to be used to access a device remotely across a network. PINs associated with a bank card are only 4 characters because the card is a token that is associated with the PIN. Similarly, DoD CAC cards are tokens with an associated 6 to 8 digit PIN for higher security. Typically, a local VTU PIN entered from a hand-held remote control can support 5 characters, while others can support more, which is preferable.

By contrast, most instances of password entry from a remote device or system (e.g., management application/server/terminal/PC, PC for streaming access, pre-configured machine passwords, etc) can utilize a full keyboard. In this case such passwords must be in compliance with DoD policy. VTU password/PIN strength or complexity is therefore dependent upon the entry device. In some cases, a VTU user must enter a "password" through their VTU. In this case, this must be a PIN because of the entry device limitations posed by the hand-held remote control. The mitigation for sending a PIN across the network could be to use it one time and change it. This may not be necessary due to an additional requirement for passwords sent across a network to a remote device per DoDI 8500.2 IA control IAIA-1, which is that they must be encrypted in transit.

**Default Details:**

Passwords do not meet DoD complexity or strength, providing for risk of password and VTU compromise.

**Pot'l Impacts:**

Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information

to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** This requirement can be reduced to a CAT III in the event a 5 digit PIN is entered to the VTU (local access) from the hand-held remote control, or (remote access), if entered from a QWERTY keyboard, a password is used having a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!).

This requirement can be reduced to a CAT III in the event the site/owner develops and enforces a SOP to manage password length and complexity to mitigate deficiencies in VTU enforcement of password complexity and length requirements.

**References:** DoD Video Tele-Conference STIG, Section: 3.3.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2024.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure the following regarding all VTU passwords and PINs:

- PINs normally entered to the local VTU from the hand-held remote control will contain 6 to 15 or more digits.
- Passwords that can be entered from a keyboard (local or remote access) are compliant with current DoD minimum password complexity policy. (e.g., 9 to 15 or more characters with a mix of at least two lowercase letters, two uppercase letters, two numbers, and two special characters (e.g., 3mP@gD2!c).
- Passwords/PINs sent across a network are encrypted per DoD standards.
- PINs sent across the network to another device using the hand-held remote control will contain 9 to 15 or more digits.

**Note:** This requirement can reduced to a CAT III in the event a 5 digit PIN is entered to the VTU (local access) from the hand-held remote control, or (remote access), if entered from a QWERTY keyboard, a password is used having a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!)

**Note:** During APL testing, this is a finding in the event this requirement is not fully supported and enforced by the VTU. This finding can be reduced to a CAT III in the event the VTU provides support for the requirement but does not enforce password strength and length.

Have the IAO or SA demonstrate logging onto the VTU via local and remote access methods. For additional verification, have SA or IAO create an account for auditor and verify that password complexity requirements are met.

**Fixes:** RTS-VTC 2024.00 (Manual); [IP][ISDN]; Perform the following tasks:

Implement VTUs that enforce password requirements when logging in via any interface. If existing devices do not support this behavior, upgrade as soon as possible.

**Responsibility:** IAO, SA, User

**Mitigations:** In the event the VTU supports password complexity and length requirements but does not enforce them, the site/owner must develop and enforce a SOP to manage password length and complexity.

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2026.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017690</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2026.00 [IP][ISDN]; Passwords for Different VTU Functions**

**Vul. Name:** Different VTU passwords are not used for different VTU functions.

**Discussion:** Passwords are required for access control to various functions provided by a VTU. The following is a list of possible functions:

1. Local user device use/activation (not typically supported).
2. Local user call accounting code.
3. Local user access to user configurable settings.
4. Local user or machine access from the VTU to the user's networked or otherwise attached PC running a presentation or desktop sharing application (or visa versa i.e., PC to VTU) (discussed later).
5. Local administrator access to configuration settings.
6. Remote administrator access to configuration settings.
7. Remote/centralized VTU management/control system access to the VTU (identifies the management server to the VTU, alternately restricted by IP address).
8. Remote caller access to a VTU integrated MCU conference without local user intervention.
9. Remote user access to media streamed from a VTU CODEC.
10. Local VTU access to a centralized MCU for joining conferences hosted remotely (i.e., the password sent to the remote MCU).
11. Local VTU access to gatekeeper services (automatically identifies the VTU to the gatekeeper).

The passwords or PINs used for various differing functions must be logically grouped and be unique among other passwords implemented on the system. For example, local user password/PINs such as those in items 1, 2, and 3 could be the same. These would be entered manually using the hand-held remote control. Another logical grouping might be items 10 and 11. The other functions are logically separate because they perform different functions and are used by different entities. One vendor uses a single password pre-configured in the VTU for functions 8 (bi-directionally), 9, 10 and possibly 11. This is a problem for two reasons. The first was stated above, it is used for different functions, and secondly, it is preprogrammed into the VTU which is in violation of DoDI 8500.2 IA control IAIA-1 that states in part passwords "are not embedded in access scripts or stored on function keys." While a machine can have an identity or password that identifies itself to another machine for passing control information (e.g., routing between the machines (e.g., passing routing tables between routers), such a password cannot be used to provide user level access to information. The user must enter this password manually. A VTC related application of machine to machine authentication would be the VTU identifying itself to a gateway or a centralized VTU management/control system to a VTU.

**Default Details:** Different VTU passwords are not used for different VTU functions, resulting in a risk that if one VTU function is compromised; all functions can be compromised.

**Pot'l Impacts:** Access to functions of the VTU by unauthorized individuals could lead to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2024.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure the following:  
- Passwords are required for access to all functions and services of the VTU. This includes, but may not be limited to, the following:  
> Local user device use/activation and access to user configurable settings.  
> Local user or machine access to the user's networked or otherwise attached PC running a presentation or desktop sharing application (if used or permitted; discussed later under PC Data and Presentation Sharing).

- > Local administrator access to configuration settings.
- > Remote administrator access to configuration settings and for remote software or firmware upgrade via IP or ISDN.
- > Remote caller access to a VTU integrated MCU conference if local user intervention is not required.
- > Remote user access to media streamed from a VTU CODEC.
- Passwords used by VTU users, administrators, and devices are logically grouped by entity and roles (human or machine), type of access provided (information vs. control), and device accessed.
- Passwords are unique across these logical groups. (i.e., a single password will not be used for multiple functions or to access multiple devices from a given VTU with the exception of a user's local access to the VTU or its user accessible settings).
- Passwords that provide user or administrator level access to another device or information will not be stored on the VTU for automated entry in lieu of the person entering the required password.

Have the IAO or SA demonstrate logging onto the VTU via local and remote access methods using different passwords/PINS for different VTC functions.

**Fixes:**

RTS-VTC 2026.00 (Manual); [IP][ISDN]; Perform the following tasks:

Implement VTUs that support different password for different functions as follows:

- Passwords are required for access to all functions and services of the VTU. This includes, but may not be limited to, the following:
  - > Local user device use/activation and access to user configurable settings.
  - > Local user or machine access to the user's networked or otherwise attached PC running a presentation or desktop sharing application (if used or permitted; discussed later under PC Data and Presentation Sharing).
  - > Local administrator access to configuration settings.
  - > Remote administrator access to configuration settings and for remote software or firmware upgrade via IP or ISDN.
  - > Remote caller access to a VTU integrated MCU conference if local user intervention is not required.
  - > Remote user access to media streamed from a VTU CODEC.
- Passwords used by VTU users, administrators, and devices are logically grouped by entity and roles (human or machine), type of access provided (information vs. control), and device accessed.
- Passwords are unique across these logical groups (i.e., a single password will not be used for multiple functions or to access multiple devices from a given VTU with the exception of a user's local access to the VTU or its user accessible settings).
- Passwords that provide user or administrator level access to another device or information will not be stored on the VTU for automated entry in lieu of the person entering the required password.

If existing devices do not support this behavior, upgrade as soon as possible.

Configure different password for different functions as described above.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 2028.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017691</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2028.00 [IP][ISDN]; VTC Endpoint User Access Control**

**Vul. Name:** Classified VTU activated without unique user login

**Discussion:** There are numerous DoD policy statements that require a user of a DoD IS to identify themselves to the IS so that it can authenticate and authorize the user before being used or before service is provided. This is primarily so that accesses to, and usage of, the IS and access to DoD information can be controlled and monitored based on the user's privileges or authorizations. These requirements range from a minimum of a user-id and password to token based two factor authentication and work in combination with security auditing to create a record of user activities that are tied to the user's identification.

VTC endpoints today do not provide any identification, authorization, or auditing capabilities with regard to their activation and use, whether stand alone or in conjunction with an authentication server. Any user can turn an endpoint on and make or receive calls. While at least one vendor's system can be configured to require the entry of a PIN to place a call, the feature is only a call accounting feature and not a security feature.

While gatekeepers and gateways provide some access control, this control only relates to access to their services. They do not play a part in endpoint activation or use of the endpoint for point-to-point calls.

The International Telecommunications Union (ITU) has developed H.235, which is the security recommendation for H.323 and other H.245 based systems. This recommendation provides for user identification rather than device identification. User identification can be simple or utilize Public Key Infrastructure (PKI). The latter being the goal of the DoD PKI policy. H.235 also has the capability and purpose of negotiating encryption and key exchange.

The ITU has also developed H.350. Unlike other H. series protocols, H.350 is a schema using Lightweight Directory Access Protocol (LDAP) to store directory and identity management information. The use of H.350 can improve security by providing standardized management and storage of authentication credentials, as well as multilevel authorization.

The use of H.245 and H.350 in combination could be the solution to the endpoint activation and user identification deficiency currently exhibited by VTC endpoints.

While it seems debatable whether a VTC endpoint is, or should be, subject to DoD access control and auditing policies, particularly in unclassified environments, there are use cases where such compliance would be beneficial to the protection of DoD information. This is particularly in cases where a VTU is located in an area where classified materials, information, and/or discussions occur because an active VTU could generate a security incident. This issue could be more of a concern if the VTU was located in a classified work area while connected to an unclassified network or network having a lower classification than the work area. Compliance would also be beneficial for VTUs in areas processing sensitive information.

To protect the information discussed in the previous paragraph, the VTU should remain dormant (even while powered on) and not capable of placing or answering a call unless it is activated by a user logging onto the system.

**Default Details:** Different VTC passwords are not used for different VTC functions, allowing for a risk that if one VTC function is compromised; all functions have the potential to be more easily compromised.

**Pot'l Impacts:** Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2028.00 (Manual); [IP][ISDN]; Verify compliance with the following requirement:

Ensure the VTU is not capable of placing or answering a call (i.e., is locked) unless it is activated by a user logon. Furthermore such activation will automatically deactivate after a configurable time period (typically 15

minutes) unless the VTU is actively participating in a conference. Incoming call notifications are provided while the VTU is locked so that a user may log in to activate the VTU and answer the call.

**Note:** While requiring a user to logon to the VTU before it can be used to place and/or receive calls may detract from the VTUs "ease-of-use" and the "user experience", (something vendors are concerned about,) the capability should exist and be usable where needed. Application of the capability could be different in various situations. This capability should be configurable. In other words, it can be turned on or off. There should be one setting to activate the requirement that a user logon to activate the VTU for general use and/or to make a call. There should be another setting to activate the requirement that a user logon to activate the VTU to answer a call. If these settings are turned on, authentication must minimally be a password that is unique to the user that is placed in CDRs. More in line with DoD policy, user-ID and password should be required as well as entry of the access into the audit log. Furthermore, the VTU should support the use of DoD PKI for user authentication. To comply with DoD access control requirements for both users and administrators, a VTU could, and in fact probably should, utilize a remote authentication server that can provide centralized management of passwords and accounts.

**Note:** During APL testing, this is a finding in the event Unique User Identification is not supported by the VTU.

If VTC endpoints are located in classified work areas or connected to a classified IP network, perform the following checks for each tested device:

- 1 - Attempt to initiate a call without logging in. If menu or directory access is provided and a number can be dialed, this is a finding.
- 2 - Interview the IAO or SA to determine the site's inactivity timeout period policy: Have the IAO or SA log onto the VTU using a unique user ID (not an admin ID) to activate the VTU. Verify VTU activation will automatically deactivate or lock, when the VTU is inactive (i.e., not active in a VTC session) in excess of the specified timeout period. This is a finding if the VTU does not require reactivation after the configured time period.
- 3- Verify that while a VTU is locked that an incoming call notification is provided so that the user may log onto VTC an answer the call. This is a finding if no incoming call notification is provided.

Check all VTUs if possible or minimally select a random sampling of units to test.

Alternately, if documentation exists indicating that the VTU operation has been verified to support these requirements via pre-deployment testing (e.g., APL testing/report), have the IAO or SA demonstrate the configuration settings on all VTUs required to implement this functionality. As an additional step, one VTU could be verified via the process defined above.

**Fixes:**

RTS-VTC 2028.00 (Manual); [IP][ISDN]; Perform the following tasks:

Implement/upgrade to VTUs that support the configuration requirements described below.

Configure the VTU to provide the following functionality:

- 1 - Configure unique (non-default/non-shared) user identities for both privileged (admin level) and non-privileged (user level) users. Provide multiple accounts as necessary in each level. Administrators should have a test user level account in addition to their admin level account.
- 2 - Configure the VTU such that a unique user ID is required to activate the VTU.
- 3 - Configure the VTU to automatically lock at the end of a specified period of inactivity. (typically 15 minutes or less).
- 4 - Configure the VTU to display an incoming call notification while deactivated so that a unique user ID is required to activate the VTU and answer the call.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b>	<input type="checkbox"/>	<b>Not Applicable:</b>	<input type="checkbox"/>	<b>Not A Finding:</b>	<input type="checkbox"/>	<b>Open Finding:</b>	<input type="checkbox"/>	<b>Fixed:</b>	<input type="checkbox"/>
----------------------	--------------------------	------------------------	--------------------------	-----------------------	--------------------------	----------------------	--------------------------	---------------	--------------------------

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2040.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017692</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2040.00 [IP][ISDN]; Manual Password Management**

**Vul. Name:** Deficient SOP or enforcement of the SOP for manual password management.

**Discussion:** DoD password and account management policies and requirements that are not supported by the CODEC must be addressed and enforced by a site policy or SOP that provides compliance to the greatest extent possible within the capabilities of the system/device. Typically a CODEC supports only one administrative password and therefore a group administrator account/password must be used. Some CODECs can support multiple user passwords or PINs for accounting purposes. Additionally, there are other passwords used to access certain features of the system and for the system and user to access other systems and devices.

**Default Details:** No SOP is in place and/or enforced that addresses manual password management for VTU passwords

**Pot'l Impacts:** Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
 IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
 IAGA-1 Identification and Authentication/Group authenticators for application or network access  
 IAAC-1 Identification and Authentication/Account Control - Management process or access and account deactivation/removal  
 ECLO-1 Enclave and Computing Environment/Logon - Limits - successive attempts, #, time delay, Active sessions - Sensitive Systems  
 DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
 ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.6

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2040.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

- In the event a system/device does not support all DoD IA requirements for password/PIN and account management or logon requirements, ensure a policy and procedure is in place and enforced that minimally addresses the following:
- Strong passwords/PINs will be used to the extent supported by the system/device. Each access point and password will be addressed separately.
  - Password/PIN reuse will be limited and will be in compliance with policy and INFOCON requirements
  - Password/PIN change intervals will be defined for each access point based upon policy, INFOCON levels, and operational requirements.
  - Passwords/PINs will be changed when compromised or personnel (users or administrators) leave the organization.
  - Passwords/PINs that are no longer needed will be removed in a timely manner. A periodic review will be performed as scheduled by the SOP.
  - SNMP community strings will be managed like passwords/PINs.
  - A password/PIN change/removal log will be maintained and stored in a secure access controlled manner (such as in a safe or encrypted file on an access controlled server or workstation) for each device noting each access point, its password, and the date the password was changed. Such a log will aid in such things as SOP enforcement, password history compliance, and password recovery.

**Note:** If and when VTC systems provide support for user and administrator accounts, this SOP is extended or modified to cover account management as necessary to manage non-automated functions.

Inspect the SOP as well as user training materials, agreements, and guides to determine if the items in the requirement are adequately covered. Interview the IAO to determine how the SOP is enforced. Interview a sampling of users to determine their awareness and implementation of the requirement and whether the SOP is enforced. This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

**Fixes:** RTS-VTC 2040.00 (Manual); [IP][ISDN]; Perform the following tasks:  
 Define and enforce policy and procedure that addresses password/PIN and account management that includes the

following:

- Strong passwords/PINs will be used to the extent supported by the system/device. Each access point and password will be addressed separately.
- Password/PIN reuse will be limited and will be in compliance with policy and INFOCON requirements.
- Password/PIN change intervals will be defined for each access point based upon policy, INFOCON levels, and operational requirements.
- Passwords/PINs will be changed when compromised or personnel (users or administrators) leave the organization.
- Passwords/PINs that are no longer needed will be removed in a timely manner. A periodic review will be performed as scheduled by the SOP.
- SNMP community strings will be managed like passwords/PINs.
- A password/PIN change/removal log will be maintained and stored in a secure access controlled manner (such as in a safe or encrypted file on an access controlled server or workstation) for each device noting each access point, its password, and the date the password was changed. Such a log will aid in such things as SOP enforcement, password history compliance, and password recovery.

Provide user training regarding this SOP and include it in user agreements and user guides.

**Responsibility:** IAM, IAO,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2320.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017693</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2320.00 [IP][ISDN]; One Time Use “Local Meeting Password”**

**Vul. Name:** Deficient SOP or enforcement of One Time Use local meeting password

**Discussion:** A “local meeting password” must be used one time only. Once any meeting password is distributed to conferees, it is known by them. If a different and unique meeting password is not used for subsequent meetings, someone that has knowledge of (i.e., remembered or recorded) a previously used password could join a conference to which they were not invited to or in which they should not be included. This capability could violate requirements for access to information based on need-to-know and/or could lead to the disclosure of sensitive or classified information.

While the setting of the “local meeting password” password could be an administrator function, most often it is set by the VTU user hosting the conference since the integrated MCU may be used in an ad hoc manner. Ideally, its use would be prescheduled. As noted above, the capability that uses this password should not be functional at all times.

Of additional concern is; in the event a local meeting password is not set on the VTU, the VTU might provide no access control to the services that use it. This cannot be permitted if the VTU performs in this manner. As such this issue must be mitigated by configuration of a “blocking” password that is kept confidential.

An additional consideration when using a “meeting password” is that such passwords should be used one time only. Once a meeting password is distributed to conferees, it is known by them. If a different and unique meeting password is not used for subsequent meetings, someone that has knowledge of a previously used password could join a conference that they were not invited to or should not be included. This capability could violate access to information based on need-to-know which could lead to the disclosure of sensitive or classified information.

**Note:** This requirement applies to VTC CODECs that can host a multipoint meeting or conference using an integral MCU. This is typically capable of supporting four to six endpoints. A “local meeting password” typically controls access to the MCU. In some cases, this password is also used to access conference streaming.

**Default Details:** No SOP and/or user training is in place or enforced that addresses the use of one time “local meeting passwords” on CODECs with integrated MCUs and streaming interface.  
AND/OR  
A blocking password is not installed and kept confidential between or after usage of a one-time “local meeting password” for a given session to prevent access to the integrated MCUs and streaming interface when they are not intended to be used.

**Pot’l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
IAAC-1 Identification and Authentication/Account Control - Management process or access and account deactivation/removal  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.1 - I&A - Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.7

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2320.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

- If the use of a local meeting password is required because it is supported by the VTU, ensure a “local meeting password” policy and procedure is in place and enforced along with user training that addresses the following:
  - Implementation and distribution of a temporary password for the session when use of the feature is required. This password is used one time and not repeated. This password must not match any other user or administrative password on the device.
  - Disablement of the feature when its use is not required or the installation of a strong blocking password that is kept confidential. This password could be distributed as the temporary password when use of the feature is required if it is changed and kept confidential following the session.
  - User instructions on how to properly set and manage the password if site policy permits the user to set the

password instead of calling an administrator.

- User awareness training regarding the vulnerabilities associated with the reuse of meeting passwords.

**Note:** In some instances, the local meeting password is also used for gaining access to media streamed from the VTU. While these are two different functions or entry points, and should not have the same password, the passwords for these functions are to be managed and used similarly. Streaming is discussed later in this document.

Inspect the SOP as well as user training materials, agreements, and guides to determine if the items in the requirement are adequately covered. Interview the IAO to determine how the SOP is enforced. Interview a sampling of users to determine their awareness and implementation of the requirement and whether the SOP is enforced. This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

**Note:** This requirement applies to VTC CODECs that can host a multipoint meeting or conference using an integral MCU. This is typically capable of supporting four to six endpoints. A "local meeting password" typically controls access to the MCU. In some cases, this password is also used to access conference streaming.

**Note:** This requirement applies to VTU CODECs that contain an integrated MCU

**Note:** During APL testing, this is a finding in the event one time "meeting passwords" are not supported by the MCU.

**Fixes:**

RTS-VTC 2320.00 (Manual); [IP][ISDN]; Perform the following tasks:

Define and enforce policy and procedure that addresses the management and use of a "local meeting password" for access to meetings hosted or streamed by a CODEC. The SOP will include the following:

- Implementation and distribution of a temporary password for the session when use of the feature is required. This password is used one time and not repeated. This password must not match any other user or administrative password on the device.
- Disablement of the feature when its use is not required or the installation of a strong blocking password that is kept confidential. This password could be distributed as the temporary password when use of the feature is required if it is changed and kept confidential following the session.
- User instructions on how to properly set and manage the password if site policy permits the user to set the password instead of calling an administrator.
- User awareness training regarding the vulnerabilities associated with the reuse of meeting passwords.

Provide user training regarding the SOP and include it in user agreements and user guides.

**Responsibility:** IAM, IAO,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2325.00</b>	<b>VMS Vulnerability Key:</b> <b>V0016557</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2325.00 [IP][ISDN]; Configuration/Administration Session Timeout**

**Vul. Name:** Administrative sessions with the VTU do not timeout within a maximum of 15 minutes.

**Discussion:** An established and/or open configuration/administration (user or administrator) session that is inactive, idle, or unattended is an avenue for unauthorized access to the management port/interface of the VTU. This can lead to compromise of the system's/device's configuration and/or denial of service. Idle sessions can be caused simply by a user or administrator being distracted or diverted from a configuration/administration session/task or by forgetting to log out of the management session when finished with his/her tasks. To ensure that the capability for unauthorized access in the event of an idle/inactive session is mitigated; an idle/inactive session timeout/logout capability must exist and be used. The timeout duration must be configurable to adjust for changing policies and requirements. Typically this duration should be set for 15 minutes as a maximum; however it can be shortened for tighter security. This requirement applies to all types of local and remote management connections/sessions and all management session protocols.

While not specifically related to VTC, this requirement can work against or inhibit certain management functions. System/device configuration backups or software upgrades requiring file transfers may exceed the idle timeout duration. In this case, the operation might fail if the idle timer disconnected the session midway through. During such events, the idle timer should recognize this activity as the session not being idle. Alternately, the idle timer duration may be extended or may be disabled as long as it is re-enabled/reset after the file transfer. Another management function that can be inhibited by an idle session timeout is when a session is required to be established for the continuous monitoring of the system/device. In this case, the idle timer may be disabled as long as it is re-enabled after the monitoring is no longer needed.

**Default Details:** Administrative sessions with the VTU do not timeout within a maximum of 15 minutes or a longer time period as documented and approved by the responsible DAA.

**Pot'l Impacts:** Access to the VTU by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 1.4 - I&A - Authentication Services

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.3.8

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2325.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure a configurable "idle/inactive session timeout/logout feature" is available and used to disconnect idle/inactive management connections or sessions. The idle timer is set to a maximum of 15 minutes. Longer time periods are documented and approved by the responsible DAA. This requirement applies to all types of physical and logical management connections and all management session protocols.

NOTE 1: This is not a finding in the event an approved management connection/session must be established for permanent full time monitoring of a system/device or the production traffic it processes.

NOTE 2: This is not a finding during management operations where the disconnection of the connection/session due to idle session timeout would inhibit the successful completion of a management task. A SOP must be established and enforced, or an automated process used, to ensure the idle/inactive session timeout feature is re-enabled and reset following such activity

NOTE 3: During APL testing, this is a finding in the event this requirement is not supported by the VTU.

> Determine if a configurable "idle/inactive session timeout/logout feature" is available and used to disconnect idle/inactive management connections or sessions.

- > Determine if the timeout is set to a maximum of 15 minutes.
- > If the timeout is set to a longer period, determine if the extended time period is documented and approved by the responsible DAA and a SOP is in place and enforced that will insure that the idle/inactive session timeout feature is re-enabled and reset following monitoring/testing activity.

**Fixes:**

- RTS-VTC 2325.00 (Manual); [IP][ISDN]; Perform the following tasks:
- > Implement a VTU with a configurable "idle/inactive session timeout/logout feature" for management sessions.
  - > Configure/set the idle timer to a maximum of 15 minutes.
  - > If longer periods are necessary, obtain approval from the responsible DAA. Document approval for inspection by auditors. Develop and enforce a SOP that will insure that the idle/inactive session timeout feature is re-enabled and reset following monitoring/testing activity. Include this SOP in administrator training, agreements and guides.

**Responsibility:** DAA, IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 2340.00</b>	<b>VMS Vulnerability Key:</b> <b>V0016560</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2340.00 [IP]; Use of Streaming in General**

**Vul. Name:** Use of media streaming is not documented properly or is not configured securely.

**Discussion:** Media Streaming as it is related to VTC systems permits a VTU to engage in a normal IP or ISDN connected conference with other VTUs while broadcasting (streaming) the conference audio and video to PC workstations over an IP based LAN to which it is connected. This permits a workstation user to view the conference in near real time but not to participate in it. VTUs may also stream other content such as pre-recorded media played from a VCR or similar media source and some VTUs support streaming while others do not. It seems that as vendors mature their streaming server technology and more products become available, they are removing the streaming capability from the CODEC where it presents greater vulnerability.

Streaming from a VTU's CODEC can also be used to record a conference by sending the stream to a recording/streaming server that can perform the recording function. These servers also serve as streaming distribution points. Recording/Streaming servers are discussed later.

While streaming from a CODEC most often uses IP multicast, streams can also be sent to one receiver (e.g., PC or recording/distribution server), or to multiple receivers in the local broadcast domain

IP multicast or broadcast streaming works best within a LAN where ample bandwidth is available and IP multicast is supported. While multicast streaming is conceivable across a WAN such as the Internet, it is much less feasible and less reliable due to limited multicast support and access circuit bandwidth constraints. To use IP multicast, the network elements must be configured to support it.

To enable streaming, the following configuration items are needed:

- Destination address, unicast (address of specific destination, client or server), broadcast (local subnet or global), multicast (address configured on a router in the range 224.0.0.1-239.255.255.255)
- IP port(s) (some CODECs may require one port for audio and one for video)
- Time-To-Live (TTL) (i.e., number of router hops or routers to traverse)

VTU Streaming can typically be activated by a user selecting it from a menu. It could also be possible to activate it by the simple press of a button on the remote control. As such, it could be possible to activate streaming by accident when it is not desired or required. Additionally, some VTUs permit a remote user to activate the feature.

The "broadcast" or stream is received by a compatible client running on a PC. Examples of clients used are RealMedia Player™, Apple Quicktime™, VIC, or Cisco IP/TV.

To receive a multicast stream, the recipient can do one of the following two things:

- First, they can use a web browser to access the IP address of the CODEC that is streaming. The user accesses the CODEC's web page and clicks a link to receive the stream. This causes the browser to download an .sdp file (e.g., filename.sdp) that contains information about the stream and launch the streaming client. The .sdp file tells the client what IP address and port the stream can be found on as well as the compression types (protocols) being used. Accessing the streaming web page or .sdp file typically requires the use of a password before gaining access. Some vendors use the administrator password (not acceptable) while others use a "meeting password" In some cases the recipient (remote user) can also activate streaming (i.e., cause the CODEC to begin streaming) from this web page if it is not already activated.
- The second method of access is essentially direct. The recipient uses the streaming client to retrieve the .sdp file from the CODECs IP address. Some streaming clients can access a multicast stream without the use of an .sdp file.

The only access control for streaming is that imposed by the CODEC for accessing its web page and/or retrieving the .sdp file. While this is effective using clients such as RealMedia Player™, Apple Quicktime™, which require the .sdp file information to function, there are other clients that do not. Using a client that does not, once the CODEC is streaming, anyone knowing the IP address and port for the stream can view the stream. There is no access control for viewing a media stream in this manner because IP provides no access control for joining an IP multicast group.

When streaming, there is no way of knowing who or how many recipients are viewing a conference. The number of possible recipients is virtually unlimited. Typically, there is only an indication on the VTU screen that the CODEC is streaming. Again, some VTUs permit streaming to be activated remotely by anybody who knows the IP address of the VTU and can access its streaming web page. As such, it could be possible for an unauthorized person to activate streaming and eavesdrop on the room or a conference in session. These vulnerabilities can greatly jeopardize the confidentiality of any given conference by broadcasting it on the connected LAN to indeterminate numbers of unknown recipients.

An additional vulnerability that streaming presents to any conference, whether hosted on a central MCU, point-to-point, or a MCU integrated unto a VTU is that any meeting participant could accidentally or maliciously stream the meeting from their VTU if their VTU supports streaming. For these reasons, the activation and use of streaming from

a VTU/CODEC is discouraged and must be tightly controlled by all IAOs who are responsible for any streaming capable VTU that might participate in a conference. CODECs must be configured in such a way that if streaming is activated, the stream can only be accessed by authorized individuals or be non-functional or inaccessible if activated by accident.

Generally speaking, the use of streaming to an IP multicast or broadcast address should never be used or activated unless it is required to fulfill a specific, validated, authorized, and documented mission requirement. This applies to both streaming from a CODEC or a recording/streaming server because of the inherent lack of full user/recipient access control. Streaming to a unicast address, i.e., one recipient, from a CODEC should be the only method used. The one recipient should only be a recording/streaming server. The best method for streaming to a number of recipients is to use a recording/streaming/web server where media can be encrypted and DoD compliant access control and auditing can be enforced via individual (unicast) viewer sessions with the server. IP multicast or broadcast should not be used. In the event IP multicast must be used, the media stream must be encrypted and a secure key exchange process employed. Full DoD compliant access control and auditing is required to gain access to the .sdp file that contains the information required to decrypt the stream. Encryption will prevent a streaming client that does not require the .sdp file from viewing the content after accessing the stream.

- Default Details:** One or more of the following issues exist regarding VTC media streaming:
- The documentation regarding the validated and approved mission requirement to use VTC media streaming is deficient or non-existent.
  - IP multicast or IP broadcast is being used as the streaming media distribution method and the media stream is not encrypted; and/or a secure key exchange process is not employed; and/or DAA approval documentation for the use of IP multicast or IP broadcast is deficient.
  - An approved streaming server implementation does not provide the streaming service via an authenticated and audited client to server (unicast) session or authenticated and audited access to an .sdp file; and/or does not use DoD PKI for access control; and/or does not provide an encrypted client server connection or encryption of the media stream.
- Note:** the reviewer should detail which of these deficiencies exist.
- Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.
- 8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
IAAC-1 Identification and Authentication/Account Control - Management process or access and account deactivation/removal  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.
- Mgmt Category:** 11.2 - Information Handling - Dissemination
- Severity:** CAT II
- Sev. Override:** NONE
- References:** DoD Video Tele-Conference STIG, Section: 3.4.1
- Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)
- Checks:** RTS-VTC 2340.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:
- Ensure the following regarding VTC streaming:
    - Streaming of VTC content will not be implemented unless required to fulfill a specific, validated, authorized, and documented mission requirement.
    - Streaming from a VTU/CODEC is to the unicast addresses of a streaming/recording server only, not to an IP multicast or broadcast address due to the lack of user/recipient access control.
    - A streaming server is used that provides the streaming service via an authenticated and audited client to server (unicast) session or authenticated and audited access to an .sdp file.
    - Streaming server access control will use DoD PKI.
    - Streaming server to client connection is encrypted for confidentiality of the streamed media.
    - If approved, and IP multicast must be used, the media stream must be encrypted and a secure key exchange process employed.
- Determine if VTC media streaming is being used. If not, this is not a finding. If so, additionally determine the following:
- Inspect the documentation regarding the validated and authorized/approved mission requirement. This is a finding if the documentation or approval is deficient or non-existent.
  - If IP multicast or IP broadcast is being used as the distribution method. If so, this is a finding unless the use is approved (inspect DAA approval documentation) and the media stream is encrypted and a secure key exchange process employed.

- If streaming from a CODEC is being used, this is a finding if the media stream is not limited to the single IP address of a streaming/recording server.
- If a streaming server is being used, this is a finding if the stream is not delivered via an authenticated and audited client to server (unicast) session or authenticated and audited access to an .sdp file; and/or Streaming server access control does not use DoD PKI; and/or the server to client connection is not encrypted.

**Fixes:**

- RTS-VTC 2340.00 (Manual); [IP]; Perform the following tasks:
- Discontinue the use of VTC media streaming OR obtain approval for the validated mission requirement, the distribution method, and fully document the requirement, distribution method, and the approval.
  - If streaming from a CODEC is approved, configure the codec for a unicast connection such that the media stream is limited to the single IP address of a streaming/recording server.
  - If IP multicast or IP broadcast is approved as the distribution method. Configure the streaming server/CODEC to encrypt the media stream and use a secure key exchange process.
  - If streaming from a streaming/recording server is approved, configure the server to provide the streaming service via an authenticated and audited client to server (unicast) session or authenticated and audited access to an .sdp file; additionally configure the server to use DoD PKI for access control; and to provide an encrypted client server connection or encryption of the media stream.

**Responsibility:** IAM, IAO

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2350.00</b>	<b>VMS Vulnerability Key:</b> <b>V0016562</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2350.00 [IP]; Streaming Indicator**

**Vul. Name:** No indicator is displayed on the VTU screen when CODEC streaming is activated.

**Discussion:** It is imperative that the operator of a VTU know if his/her CODEC is streaming. This is due the ease with which streaming can be activated accidentally or intentionally and that it can be activated remotely by various methods or individuals with different privilege levels. The VTU must display an indication on the screen if it is actively streaming so that the VTU user/operator can be aware of the fact and take action to stop the streaming or disconnect the call if the CODEC should not be streaming.

**Note:** For additional information regarding the vulnerabilities associated with VTC streaming, see the discussion under RTS-VTC 2340

**Default Details:** There is no indicator displayed on the VTU screen when CODEC streaming is activated alerting the operator of a session compromise due to the accidental or inappropriate activation of streaming.

**Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 - For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.4.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2350.00 (Interview); [IP]; Validate compliance with the following requirement:

Ensure an on-screen indicator is displayed when the VTU/CODEC is actively streaming. Include awareness of the indicator and its meaning in user training and user guides.

**Note:** This is a requirement whether streaming from a CODEC is approved or not.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the CODEC.

This is a finding if an on-screen indicator is not displayed when the VTU/CODEC is actively streaming. Validate compliance via inspection of the device manuals or activate streaming and look for the on-screen indicator. Activating the streaming feature may require applying a streaming configuration. If so, be sure to remove/disable the configuration following the indicator test.

**Fixes:** RTS-VTC 2350.00 (Manual); [IP]; Perform the following tasks:  
- Purchase VTC equipment that either does not support streaming from the CODEC or provides an indicator that the CODEC is actively streaming.  
AND/OR  
- Configure the CODEC to provide the required on-screen indicator in the event such display does not occur by default.  
AND  
Include awareness of the indicator and its meaning in user training and user guides.

**Responsibility:** SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2360.00</b>	<b>VMS Vulnerability Key:</b> <b>V0016564</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2360.00 [IP]; SOP for CODEC Streaming**

**Vul. Name:** Deficient SOP or enforcement for VTC/CODEC streaming.

**Discussion:** To control streaming from a VTU/CODEC, the site must have a policy and procedure regarding the use of streaming. This could be very simple if streaming will never be used or more complex if there is the potential for its use. Such an SOP will reflect the requirements of this STIG regarding streaming.

**Note:** For additional information regarding the vulnerabilities associated with VTC streaming, see the discussion under RTS-VTC 2340

**Default Details:** Deficient SOP addressing the control of VTC/CODEC streaming.

**Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
IAAC-1 Identification and Authentication/Account Control - Management process or access and account deactivation/removal  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.4.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2360.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:

In the event the VTU/CODEC is connected to an IP based LAN, and if the CODEC supports streaming, ensure a "Streaming" policy and procedure is in place and enforced that addresses the following:

- The approval of conference streaming on a case by case basis prior to it being configured by an administrator and activated.
- Implementation and distribution of temporary one-time "streaming passwords", and other session information, to control recipient access to the media stream. For best protection of the system, this password must be used one time and not repeated. This password must not match any other user or administrative password and must be configured to meet or exceed DoD password complexity requirements since entry from a keyboard is expected.
- Requirements for implementing an appropriate streaming configuration to limit the reach of the stream across the network.
- Re installation of the "blocking" configuration and password (as required below) following any given streaming session.
- Changes to the "access blocking" configuration and password in the event it is compromised or if administrative staff changes.

**Note:** The details of this SOP will be included in user's training, agreements, and guides.

**Note:** This is a requirement whether streaming from a CODEC is approved or not.

Inspect the SOP as well as user training materials, agreements, and guides to determine if the items in the requirement are adequately covered. Interview the IAO to determine how the SOP is enforced. Interview a sampling of users to determine their awareness and implementation of the requirement and whether the SOP is enforced. This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

**Fixes:** RTS-VTC 2360.00 (Manual); [IP]; If the CODEC supports streaming, Perform the following tasks:

- Develop and enforce the SOP, train users, and include the SOP in user agreements and guides.
- The SOP will address the following:
  - > The approval of conference streaming on a case by case basis prior to it being configured by an administrator and activated.
  - > Implementation and distribution of temporary "streaming passwords", or other session information, to control recipient access to the media stream. For best protection of the system, this password must be used one time and not repeated. This password must not match any other user or administrative password and must be configured to meet or exceed DoD password complexity requirements since entry from a keyboard is expected. A temporary, one

- time password is implemented during streaming enablement and configuration of the given streaming session.
- > Requirements for implementing an appropriate streaming configuration to limit the reach of the stream across the network.
- > Re installation of the "blocking" configuration and password (as required below) following any given streaming session.
- > Changes to the "access blocking" configuration and password in the event it is compromised or if administrative staff changes.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2365.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017694</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2365.00 [IP]; User Training for CODEC Streaming**

**Vul. Name:** Deficient user or administrator training regarding the vulnerabilities with, and operation of, CODEC streaming

**Discussion:** In conjunction with the SOP for VTU/CODEC streaming, users must be trained in the vulnerabilities of streaming, how to recognize if their CODEC is streaming, and how to deactivate streaming if it should not be active.  
**Note:** For additional information regarding the vulnerabilities associated with VTC streaming, see the discussion under RTS-VTC 2340

**Default Details:** Deficient or no VTC/CODEC user training has been provided to administrators and/or users on the vulnerabilities of streaming, recognition of CODEC streaming, and how to deactivate streaming when it is active.

**Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
IAAC-1 Identification and Authentication/Account Control - Management process or access and account deactivation/removal  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
PRTN-1 Personnel / Information Assurance Training - A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery

**Mgmt Category:** 6.4 - Personnel - Training

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.4.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2365.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:  
In the event the VTU/CODEC is connected to an IP based LAN, and if the CODEC supports streaming, ensure users/operators and administrators of a VTU receive training regarding streaming that addresses the following:  
- User awareness regarding the vulnerabilities streaming from a CODEC presents to conference confidentiality.  
- User awareness regarding accidental activation of streaming.  
- How to recognize the displayed indication provided by the VTU that it is in streaming mode.  
- How to terminate streaming, particularly if the CODEC should not be streaming.  
- The implementation and distribution of a temporary password for an approved CODEC streaming session using a one-time password that is not repeated and does not match any other user or administrative password.  
**Note:** This is a requirement whether steaming from a CODEC is approved or not.  
Interview VTC/CODEC administrators and user/operators to verify that they have received training on the vulnerabilities of streaming, recognition of CODEC streaming, and how to deactivate streaming when it is active. Have a sampling of these individuals demonstrate their knowledge.  
This is a finding if deficiencies are found in any of these areas. Note the deficiencies in the finding details.

**Fixes:** RTS-VTC 2365.00 (Manual); [IP]; In the event the VTU/CODEC is connected to an IP based LAN, and if the CODEC supports streaming, Perform the following tasks:  
- Train CODEC user/operators and administrators regarding CODEC streaming addressing the following:  
> User awareness regarding the vulnerabilities streaming from a CODEC presents to conference confidentiality.  
> User awareness regarding accidental activation of streaming.  
> How to recognize the displayed indication provided by the VTU that it is in streaming mode.  
> How to terminate streaming, particularly if the CODEC should not be streaming.  
Additionally include this information in user's agreements and guides.

**Responsibility:** SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2380.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017695</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2380.00 [IP]; Blocking Configuration for VTU/CODEC Streaming**

**Vul. Name:** CODEC streaming is not disabled when it is not required.

**Discussion:** When a CODEC is not required to be streaming, the capability will be disabled. The preferred method for this is via an administrator configurable setting. Both user activation and remote start must be addressed. In lieu of this, a streaming configuration must be implemented on the VTU that inhibits the ability to stream such that streaming will not be able to effectively be used to view a room or conference.  
**Note:** For additional information regarding the vulnerabilities associated with VTC streaming, see the discussion under RTS-VTC 2340

**Default Details:** Conference streaming is not blocked or inhibited in the event of accidental or malicious activation.  
OR  
The VTU does not support disablement of conference streaming by an administrator.

**Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 3.4.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2380.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:  
Ensure the following streaming configuration settings are implemented as prudent to further minimize the effect of accidental or unwanted streaming activation when streaming is not required to be activated:  
- Disable streaming and/or user activation of streaming  
- Disable remote start of streaming (if remote start is supported)  
OR if the above settings do not exist or do not work properly:  
- Clear the streaming destination or multicast address(s)  
- Set TTL/router hops to 0 or a maximum of 1 if 0 is not accepted.  
- Set the password used to access the CODEC for streaming to a strong password that meets or exceeds minimum DoD password requirements. This password is kept confidential.  
**Note:** If clearing the IP address or IP port does not prevent the CODEC from streaming to a default address or port, set a unicast addresses that will never be used by a device and set a very high IP port.  
**Note:** This requirement is applicable whether the CODEC is normally connected to an IP based LAN or not. If not normally connected to an IP based LAN, these settings will mitigate the vulnerability in the event the CODEC does become connected to a LAN via un-authorized or clandestine means  
**Note:** During APL testing, this is a finding in the event the product does not support the ability to disable conference streaming.  
Have the IAO or SA demonstrate the streaming configuration on a random sampling of CODECs.

**Fixes:** RTS-VTC 2380.00 (Manual); [IP]; Perform the following tasks when CODEC streaming is not required to be use:  
Configure the CODEC as follows:  
- Disable streaming and/or user activation of streaming  
- Disable remote start of streaming (if remote start is supported)  
OR if the above settings do not exist or do not work properly:  
- Clear the streaming destination or multicast address(s)  
- Set TTL/router hops to 0 or a maximum of 1 if 0 is not accepted.  
- Set the password used to access the CODEC for streaming to a strong password that meets or exceeds minimum DoD password requirements. This password is kept confidential.  
**Note:** If clearing the IP address or IP port does not prevent the CODEC from streaming to a default address or port,

set a unicast addresses that will never be used by a device and set a very high IP port.

**Note:** This requirement is applicable whether the CODEC is normally connected to an IP based LAN or not. If not normally connected to an IP based LAN, these settings will mitigate the vulnerability in the event the CODEC does become connected to a LAN via un-authorized or clandestine means

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2420.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017696</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2420.00 [IP]; VTU/CODEC Streaming Configuration**

**Vul. Name:** VTU/CODEC is not properly configured to support streaming.

**Discussion:** In the event conference streaming directly from a VTU/CODEC is approved for a given conference, the administrator will need to properly configure the VTU to support the streamed conference. One of these measures is to set a one-time-use password for the streamed media. Another measure is to install configuration settings to limit the reach of the streamed media across the network to only those portions that are to receive it. This is done by setting the TTL as low as possible. A mitigation that can be used for the lack of access control for IP multicast is to use different multicast addresses and IP ports each time a streaming session is configured. First these should never be the default address(es) or ports used by the vendor's system and they should be randomly selected.

**Note:** Streaming is a feature of the VTU that could be turned on and configured for monitoring purposes by an adversary if the administrative access to the VTU is compromised. This is another reason why it is imperative to change all access codes and passwords on the VTU as required earlier. Additionally, users must be trained to recognize any displayed indication provided by the VTU that it is in streaming mode.

**Note:** For additional information regarding the vulnerabilities associated with VTC streaming, see the discussion under RTS-VTC 2340

**Default Details:** The streaming configuration does not limit the reach of the streamed media  
OR  
A one-time password is not implemented for the session

**Pot'l Impacts:** The inadvertent or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section 3.4.6

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2420.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:

- If and when implementing streaming, ensure the following streaming configuration settings are implemented as prudent to minimize accessibility to the media stream:
- Implement and distribute a temporary password for the session. For best protection of the system, this password is used one time and not repeated. This password must not match any other user or administrative password.
  - Enter an appropriate address and IP port for delivery of the media stream. If multicast is used, these are different from the default settings used by the vendor, and are randomly different each time they are used.
  - Set TTL/router hops to an appropriate number to limit the range of distribution of the media stream to within the local LAN or Intranet as required. This number should be limited to 1 for the local network, 15 or 16 for the campus, 25 for the adjoining site. Never enter a high number such as 64 and above since this will extend the reach to a region or the world as the number goes higher.

Determine/review site policy/procedure for the implementation of approved VTC CODEC streaming. Review configuration settings to be used. If any CODECs are currently approved for and configured to stream, inspect or have the SA demonstrate the configuration used. This is a finding if the policy/procedure and/or configuration does not match or support the requirement items listed above.

**Fixes:** RTS-VTC 2420.00 (Manual); [IP]; Perform the following tasks if streaming of a VTC CODEC session is approved and is to be implemented:

- Implement and distribute a temporary password for the session. This password is used one time and never repeated. This password must not match any other user or administrative password.
- Configure the CODEC by entering an appropriate address and IP port for delivery of the media stream. If multicast is used, these must be different from the default settings used by the vendor, and are randomly different each time they are used.
- Configure the CODEC by setting TTL/router hops to an appropriate number to limit the range of distribution of the media stream to within the local LAN or Intranet as required. This number should be limited to 1 for the local network,

15 or 16 for the campus, 25 for the adjoining site. Never enter a high number such as 64 and above since this will extend the reach to a region or the world as the number goes higher.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2440.01</b>	<b>VMS Vulnerability Key:</b> <b>V0016078</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2440.01 [IP][ISDN][PC]; SOP Presentation Sharing**

**Long Name:** Deficient SOP or enforcement regarding presentation and application sharing via a PC or VTC.

**Vulnerability Discussion:** Visual collaboration often requires the sharing or display of presentations, open documents, and white board information to one or more communicating endpoints. While the technology for doing this is different between hardware based VTC endpoints and PC based application endpoints, the vulnerability is the same. In both cases, the displayed information typically resides on a PC.

While in presentation/sharing mode, care must be exercised so that the PC user does not inadvertently display and transmit information on their workstation that is not part of the communications session and not intended to be viewed by the other communicating parties. Users must be aware that anything they display on their PC monitor while presenting to a communications session may be displayed on the other communicating endpoints. This is particularly true when the PC video output is connected to a VTC CODEC since the information will be displayed on all of the conference monitors. This presentation/sharing feature could result in the disclosure of sensitive or classified information to individuals that do not have a validated need-to-know or have the proper clearance to view the information. Thus the presentation/sharing feature presents a vulnerability to other information displayed on the PC if the feature is misused. This is a problem when sharing and displaying a PC desktop via any collaboration tool using any connection method.

There is little that can be done to mitigate this vulnerability other than to develop policy and procedures to present to collaborative communications sessions. All users that perform this function must have awareness of the issues and be trained in the proper operational procedures. Such procedures may require that there be no non-session related documents or windows open or minimized on the PC while presenting or sharing. An additional requirement may be that the user may not permit others in a session to remotely control their PC.

A SOP is needed that addresses mitigations for the vulnerabilities posed by PC data and presentation sharing. Such an SOP could include the following discussion. If a user needs to view non meeting related information while presenting to a conference, the PC external display port must be turned off or better yet, the cable disconnected. Dual monitor operation of the PC could mitigate this problem somewhat. The second monitor output would be connected to the CODEC which would serve as the second monitor. Using this method, any information may be viewed on the native PC monitor while the presentation can be displayed on the VTU presentation screen.

**Default Details:** A policy and procedure is deficient or is not in place and/or not enforced that addresses the proper implementation and use of the "Presentation and Sharing" features of collaboration applications and devices.

**Pot'l Impacts:** The inadvertent and/or improper disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices

**Mgmt Category:** 11.2 - Information Handling - Dissemination

**Severity:** CAT II

**Sev. Override:** NONE

**References:** Video Tele-Conference STIG, Section: Section: 3.5.1  
Personal Computer Communications Client (PCCC) STIG v1r1, Section 2.4.4

**Conditions:** Non-Computing – PC Communications Client Policy (Target: PC Communications Client Policy )  
Non-Computing – Video Tele-Conference Policy (Target: Video Tele-Conference Policy)

**Checks:** RTS-VTC 2440.01 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:

Ensure a policy and procedure is in place and enforced that addresses the proper implementation and use of the "Presentation and Sharing" features of collaboration applications and devices. This policy and SOP will be based on the specific application's or device's capabilities and will address mitigations for the possible inadvertent disclosure of information to conferees that have no need to see or have access to such information. Operational policy and procedures must be included in user training and guides.

Interview the IAO and inspect the applicable SOP. The SOP should address the proper implementation and use of the "Presentation and Sharing" features of collaboration applications and devices. This policy and SOP will be based

on the specific application's or device's capabilities and will address mitigations for the possible inadvertent disclosure of information to conferees that have no need to see or have access to.

Inspect user training materials and discuss practices to determine if information regarding the SOP is conveyed. Interview a random sampling of users to confirm their awareness of the SOP and related information.

This is a finding if the if the SOP or training is deficient.

**Fixes:**

RTS-VTC 2440.01 (Manual); [IP][ISDN]; Produce an SOP that addresses the proper implementation and use of the "Presentation and Sharing" features of collaboration applications and devices. This policy and SOP will be based on the specific application's or device's capabilities and will address mitigations for the possible inadvertent disclosure of information to conferees that have no need to see or have access to. Operational policy and procedures must be included in user training and guides.

Provide appropriate training such that users follow the SOP. Enforce user compliance with the SOP

**Responsibility:** IAM, IAO, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 2460.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017697</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2460.00 [IP][ISDN]; PC Data and Presentation Sharing User Training**

**Vul. Name:** Inadequate user training for pc presentation sharing that could lead to compromise of other information on the presenting PC

**Discussion:** Users must be trained regarding the display of information that is not part of the conference. Such training must be based on the SOP discussed under RTS-VTC 2440.01 that is designed to mitigate the vulnerability.

**Default Details:** User training is inadequate or is not provided that addresses the vulnerabilities associated with presentation, application, and desktop sharing to a VTU from a PC.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
PRTN-1 Personnel / Information Assurance Training - A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery

**Mgmt Category:** 6.4 - Personnel - Training

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.5.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2460.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure VTU users receive training in the proper use and operation of PC to CODEC connections and understand the vulnerabilities associated with such interconnections regarding inadvertent or improper information disclosure.  
Interview a sampling of VTU administrators and users to verify that training has been provided for proper use and operation of PC to CODEC connections and that they understand the vulnerabilities associated with such interconnections regarding inadvertent or improper information disclosure. This is a finding if deficiencies are found. List these deficiencies in the finding details.

**Fixes:** RTS-VTC 2460.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Train users and administrators in the proper use and operation of PC to CODEC connections and provide an understanding of the vulnerabilities associated with such interconnections regarding inadvertent or improper information disclosure.

**Responsibility:** IAM, IAO

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2480.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017698</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2480.00 [IP]; PC Data and Presentation Sharing Software**

**Vul. Name:** Deficient SOP or enforcement regarding the use of software based virtual connection between the PC and the VTC CODEC.

**Discussion:** VTC CODECs provide various means and methods to permit the display of presentations and various other forms of data to all of the endpoints in a conference. Typically, this involves connecting a PC workstation, on which the presentation is displayed and controlled, to a CODEC which distributes the presentation to the conferees. Care in operating this feature must be exercised so that the PC user does not inadvertently display information on their workstation that is not part of the conference and is not intended to be viewed by the conferees. Users must be aware that anything that they display on their PC workstation display while connected to the CODEC will be displayed on all of the conference monitors. This collaboration/display feature could result in the disclosure of sensitive or classified information to individuals that do not have a validated need-to-know or have the proper clearance to view the information. This is a problem when sharing a PC desktop via any collaboration tool using any connection method.

The first of the PC-CODEC interconnection methods, supported by most (but not all) CODECs, is the direct connection of the PC video output to an external video input on the CODEC. This method is most common interconnection method, is most secure, and is the recommended method for DoD. This is the only method available to users of VTUs connected to ISDN only (i.e., not connected to an IP network in addition to the ISDN lines). The second method for PC-CODEC interconnection for data/presentation sharing is to establish a virtual connection between the CODEC and PC workstation across an IP based LAN. While this method is implemented in different ways by different vendors, most if not all methods require the installation of an application or a utility on the PC workstation that is to share its data or display. While this method is convenient, since it does not require a cable connected to the CODEC, it presents varying degrees of vulnerability to the PC and the data it contains depending upon the particular application or utility installed. Additionally, the installation of such software is contrary to most DoD policy regarding approved workstation applications. All such software must be thoroughly evaluated and approved before installation.

Most vendors provide a proprietary application or utility that is loaded on the PC workstation to establish the virtual connection between the PC and CODEC. The main purpose and capability of this utility is to capture the PC's display graphics and send it to the CODEC. Typically, these utilities require only the IP address of the CODEC. The CODEC may or may not require a password to accept this input. When reading the documentation on these utilities there is no indication that the media stream generated by these utilities is encrypted. This may or may not be an issue depending upon the protocols used by the utility. Sniffing the stream may or may not reveal the displayed information. One vendor provides a utility to upload MS PowerPoint files to the CODEC and display them using an embedded viewer. This same vendor provides another utility to integrate with MS NetMeeting on the PC and stream content from there using T.120 protocol.

An additional feature of some of these utilities is the capability of conferees to share and work on files across the connection between CODECs. This feature brings a larger set of collaboration tool features to the VTC arena.

At least one vendor's virtual connection method requires the installation of PC remote control desktop sharing software on the PC. Once the remote control/access server application is running, anybody with the matching or compatible viewer/control application and the access password can connect to the PC workstation from another PC workstation. This provides full control of its resources and access to all of its files since this is the purpose of this type of application. This type of application can receive remote keyboard and mouse inputs as if the user was sitting at the PC itself controlling it. As such this method is capable of much more than capturing the graphics displayed on the PC monitor and sending it to a CODEC. As such an adversary could gain full control of the PC workstation at any time when the server application is running, whether there is a conference being displayed or not. Many such server applications are started as a service when the workstation is booted. This means that the connection is available to an adversary any time the PC is running. This is a huge vulnerability for the PC workstation.

As such, the use of virtual connection methods must first be approved by the DAA and must be tightly controlled. Another issue that must be addressed is the access control between the VTU and the PC. This discussion and/or requirements are dependant upon the direction of the access. (i.e., PC to VTU or VTU to PC) Access to a PC (from a VTU), by policy, requires a strong policy compliant password (and other measures, supported or not). Such a password cannot be entered from a VTU remote control unless an on screen keyboard (or cell phone text entry requiring password display) is used thus opening the password to shoulder surfing or being viewed by a conference room full of people (discussed earlier). If the VTU is to initiate the connection to the PC, it is best to store a strong password on the VTU that will identify the VTU to the PC sharing application. The sharing application is only run when needed when the PC is required to interface with the VTU; it is not run as a service that is constantly available. Other constraints could apply. The recommended alternative is to initiate all VTU - PC connections from the PC and

implementing the appropriate access control in the VTU in compliance with password policy if a virtual connection is to be used. Better yet, use a direct connection using a video out connection on the PC. Furthermore, it is recommended that, if the remote control/access method is used, a PC workstation be dedicated to the purpose of displaying presentations on the CODEC. No other information should be placed on this PC. The PC should be turned off or disconnected from the LAN when a presentation is not being displayed to a conference. In this way, the installation of the remote control/access software will not place non conference information at risk.

- Default Details:** User training is inadequate or is not provided that addresses additional vulnerabilities associated with presentation, application, and desktop sharing to a VTU from a PC. Additional vendor specific procedures and policies have not been implemented. Assessments have not been performed and documented to validate additional VTU application does not invalidate the security of the workstation. A risk assessment has not been performed and documented. DAA has not approved in writing the installation of additional VTU software to PC nor has the DAA approved the implementation and procedures to mitigate the applications vulnerabilities
- Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.
- 8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
ECSD-2 Enclave and Computing Environment/Software Development Change Controls - ECSD-1 + review and approval of change requests and technical system features to assure that changes are executed by authorized personnel and are properly implemented.  
VIVM-1 Vulnerability and Incident Management/Vulnerability Management - A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.  
ECND-1 Enclave and Computing Environment/Network Device Controls - A network device control program/policies/SOPs/instructions/restrictions/protections/documentation
- Mgmt Category:** 12.9 - Configuration Management Policies - Documentation
- Severity:** CAT II
- Sev. Override:** NONE
- References:** DoD Video Tele-Conference STIG, Section: Section: 3.5.3
- Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)
- Checks:** RTS-VTC 2480.00 (Interview); [IP]; Interview the IAO to validate compliance with the following requirement:
- In the event a software based virtual connection between a PC/workstation and a CODEC is to be used for presentation display, file transfer, or collaboration, the IAO will ensure the following:
    - Additional appropriate policy and procedures for this type of connection are added to the required "Presentation/PC workstation display sharing" policy and procedure. These are based on the particular vendor's solution to be implemented.
    - Additional appropriate user training is added to the training requirement noted above.
    - Perform and document an assessment of the application to be used to verify that it performs only those functions that are necessary, that the application behaves properly on the platform, and that it does not invalidate the security of the workstation.
    - Perform and document a risk assessment regarding the use of the application in light of the application assessment and the defined operational policy/procedures.
    - The responsible DAA approves, in writing, the installation of the additional software to the PC workstation(s) required to use this method.
    - The responsible DAA approves, in writing, the implementation and use procedures that mitigate the application's vulnerabilities.
- Note:** Assessments should be performed and DAA approvals should be obtained prior to purchase.
- Note:** The IAO will maintain the policy, procedures, assessment documentation, risk assessment, and DAA approvals for inspection by IA auditors as evidence of compliance.
- Verify that additional and appropriate user training is added to the training requirement as noted in RTS-VTC 2460.00 that addresses additional vulnerabilities associated with presentation, application, and desktop sharing to a VTU from a PC.  
AND  
Verify additional vendor specific procedures and policies have been implemented.  
AND  
Verify that assessments have been performed and documented to validate additional VTU application(s) has not invalidated the security of the workstation. Verify with the IAO that a risk assessment has been performed and documented.  
AND

Verify that DAA has approved in writing the installation of additional VTU software and the DAA is aware and approved the implementation and procedures used to mitigate the VTU application(s) vulnerabilities

This is a finding if deficiencies are found. List these deficiencies in the finding details.

**Fixes:**

RTS-VTC 2480.00 (Manual); [IP]; Perform the following tasks:

- Develop additional appropriate policy and procedures for this type of connection are added to the required "Presentation/PC workstation display sharing" policy and procedure. These are based on the particular vendor's solution to be implemented.
- Provide additional appropriate user training to the training requirement noted under RTS-VTC 2460.
- Perform and document an assessment of the application to be used to verify that it performs only those functions that are necessary, that the application behaves properly on the platform, and that it does not invalidate the security of the workstation.
- Perform and document a risk assessment regarding the use of the application in light of the application assessment and the defined operational policy/procedures.
- Obtain approval from the responsible DAA in writing for the installation of the additional software to the PC/workstation(s) required to use this method.
- Obtain approval from the responsible DAA in writing for the use and implementation procedures that mitigate the application's vulnerabilities.
- Maintain the policy, procedures, assessment documentation, risk assessment, and DAA approvals for inspection by IA auditors as evidence of compliance

**Note:** Assessments should be performed and DAA approvals should be obtained prior to purchase.

**Responsibility:** IAM, IAO, SA, USER

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2820.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017699</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2820.00 [IP][ISDN]; Password for API Configuration Administrative Command Access**

**Vul. Name:** A CODEC's local Application Programmers Interface (API) provides unrestricted access to user or administrator configuration settings and CODEC controls without the use of an appropriate password.

**Discussion:** Large conference room VTC systems may be built into the conference room in such a way that a hand-held remote control cannot directly access or control the CODEC because it is located in another room such as an AV control room. While there are systems and methods for extending the control signals from the hand-held remote control to the CODEC, many times the CODEC is connected to an AV control panel (typically called a "touch panel") that sits on the conference table or possibly a podium. While this panel can be connected to the CODEC wirelessly (as discussed later) or via a wired IP connection, typically the connection is via an EIA-232 serial connection on the CODEC. To give the "touch panel" the ability to control the CODEC, the CODEC contains an Application Programmers Interface (API) control program. All functions that are available on the hand-held remote control are typically duplicated on the "touch panel"

Typically a VTC CODEC's API provides full access to all configuration settings and control commands supported but the CODEC. This can be a big problem if the command channel is compromised because this would give the attacker the ability to reconfigure the CODEC or its features and capabilities and not just control them. To mitigate this problem, the CODEC's API must provide a separation of the commands that control the system from the commands related to user and administrator configuration settings. If a password/PIN is implemented for user settings as required above, the touch panel must support the manual entry of the user configuration password/PIN assuming they will need to be accessed via the touch panel. Similarly, administrator settings should not be accessible from the touch panel or the interface on the CODEC that it uses without the use of an administrator password/PIN. Such separation/segregation of access to privileged commands is required by DoDI 8500.2 IA controls ECLP-1 and ECPA-1.

**Default Details:** A CODECs local Application Programmer's Interface (API) provides unrestricted access to user or administrator configuration settings and CODEC controls without the use of an appropriate password.

**Pot'l Impacts:** Access to the CODEC API by unauthorized individuals possibly leading to the disclosure of sensitive or classified information to a caller of a VTU that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECLP-1 Enclave and Computing Environment/Least Privilege per duties.  
ECPA-1 Enclave and Computing Environment/Privileged Account Control - use a role-based access scheme, IAM tracks privileged role assignments.  
IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems

**Mgmt Category:** 1.1 - I&A – Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.6.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2820.00 (Interview); [IP][ISDN]; Interview the IAO to validate compliance with the following requirement:  
Ensure a CODEC's API does not provide unrestricted access to user or administrator configuration settings and without the use of an appropriate password in addition to any regular user activation password/PIN.  
Review the vendor documentation on the API. Look for information on restricting access to user or administrator configuration settings. Determine what user or administrator configuration settings are accessible or programmable via the API. Determine all API access methods and communications protocols, meaning local serial connection or "remotely" via a network.  
AND  
Establish a connection to the CODEC's API using the information gained above and a PC; disconnect any AV control panel if necessary. Attempt to gain access and to change various user or administrator configuration settings via the API.  
This is a finding if the user or administrator configuration settings are unprotected and/or easily changeable.

**Fixes:** RTS-VTC 2820.00 (Manual); [IP][ISDN]; Perform the following tasks:

Purchase and implement VTC CODECs that support the restriction of access to user or administrator configuration settings via the API.  
AND  
Configure VTC CODECs to restrict access to user or administrator configuration settings via the API.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 2840.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017700</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 2840.00 [IP][ISDN]; API Command Encryption and Authentication**

**Vul. Name:** CODEC control / configuration messages received via the local Application Programmer's Interface (API) are not encrypted or authenticated

**Discussion:** The commands passed between the "touch panel" and CODEC are typically in a human readable clear text format. While older touch panels required a physical and direct connection to the EIA-232 serial connection on the CODEC, newer models are being developed to make use of Ethernet networks and associated IP protocols. Wireless models are also becoming available using wireless networking technologies. Sending clear text commands across these types of connections is an issue because it places the CODEC at risk of hijack i.e., being controlled by an entity other than the authorized touch panel in the conference room. Due to these issues, if the touch panel is implemented using a networking technology, the API commands must be encrypted in transit and the CODEC must authenticate the source of the commands.

**Default Details:** API connection to CODECs via Ethernet or wireless does not provide password encryption and authenticated access.

**Pot'l Impacts:** Unencrypted and unauthorized access to the CODEC via API Ethernet or wireless connection by unauthorized individuals, could possibly lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 - For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

**Mgmt Category:** 1.4 - Authentication Services

**Severity:** CAT II

**Sev. Override:** This finding can be reduced to a CAT III (as opposed to not-a finding) for direct connections using the Ethernet connection on the CODEC. This is because, in this case, direct connection is only a partial mitigation since there is the potential that the VTU could still be connected to a LAN.  
This is not a finding for direct connections using the EIA-232 serial connection on the CODEC.

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.6.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 2840.00 (Interview); [IP][ISDN]; Validate compliance with the following requirement:  
Ensure control command communications between a CODEC and an audio visual control panel (touch panel), implemented using a wired or wireless networking technology, or is via a wired network (i.e., LAN), is encrypted and the CODEC authenticates the source of the commands.  
**Note:** This finding can be reduced to a CAT III (as opposed to not-a finding) for direct connections using the Ethernet connection on the CODEC. This is because, in this case, direct connection is only a partial mitigation since there is the potential that the VTU could still be connected to a LAN  
**Note:** This is not a finding for direct connections using the EIA-232 serial connection on the CODEC.

Determine if the API connection between a CODEC and its AV control panel is via wired or wireless networking technology or a LAN. This is a finding if the control panel does not encrypt its commands and the CODEC does not authenticate the source of the commands. Have the SA demonstrate or Inspect the CODEC's configuration settings regarding the encryption and authentication methods for the API communications with the AV control panel.

**Fixes:** RTS-VTC 2840.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Purchase and implement VTC CODECs and AV control panels that support the encryption and authentication of API messages from the AV control panel.  
AND  
Configure VTC CODEC to only accept authenticated and encrypted API messages from the AV control panel.  
AND  
Configure the AV control panel to encrypt its control messages and to include authentication information for each message such that the CODEC can authenticate the source of the message before acting upon it.

**Responsibility:** IAO, SA

**Mitigations:** Use the direct connect method using the EIA-232 serial connection between the CODEC and the AV control panel

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3120.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017701</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3120.00 [IP]; Use Secure Management Protocols**

**Vul. Name:** Secure protocols are not used for CODEC remote control and management

**Discussion:** Many VTC Endpoints are remotely accessed across a LAN via non-secure IP protocols such as telnet, FTP, and HTTP. This poses another confidentiality issue since these protocols do not meet DoD requirements for password encryption while in transit per DoDI 8500.2 IA control IAIA-1 and IAIA-2, nor do they meet the encryption requirements for sensitive information in transit as required by IA controls ECCT-1 and ECNK-1. Therefore, if possible, non-secure protocols should not be used. Some devices provide the option to select the secure versions of these protocols such as HTTPS, FTPS, and TelnetS, and/or SSH for remote access. Secure protocols are required over non-secure protocols if available.

Of additional concern is that remote control/management/configuration is performed in-band. In other words, it is performed using the same Ethernet port as the VTC traffic utilizes. If non-secure protocols must be utilized, the VTC production and CODEC remote access traffic must be segregated on the LAN from the normal data traffic. This is so that the confidentiality of the remote access password and sensitive management/configuration information is protected to the greatest extent possible by limiting access to it. Segregation requirements are discussed later under the LAN configuration section.

**Note:** During APL testing, this is a finding in the event encryption protocols are not supported by the VTC\VTU\CODEC.

**Default Details:** Device management is performed using unencrypted protocols that do not protect administrator logon credentials and management information.

**Pot'l Impacts:** Unencrypted management/configuration traffic to the CODEC could lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECSC-1 - For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied.

**Mgmt Category:** 8.1 - Encryption & Data Integrity - Encrypted Data in Transit

**Severity:** CAT II

**Sev. Override:** This is not a finding if unencrypted management protocols are passed through an encrypted VPN between the managing PC/workstation/server and the managed device.

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.7.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3120.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

Ensure secure (encrypted) remote access protocols are used for CODEC "Remote Control/Management/Configuration" (e.g., HTTPS, FTPS, TelnetS, or SSH)

Determine what protocols are in use for device management and configuration. This is a finding if the protocols used are not encrypted.

**Note:** This is not a finding if unencrypted management protocols are passed through an encrypted VPN between the managing PC/workstation/server and the managed device.

**Note:** During APL testing, this is a finding if the device does not support encrypted management protocols (e.g., HTTPS, FTPS, TelnetS, or SSH) OR an encrypted VPN between the managing PC/workstation/server and the managed device.

**Fixes:** RTS-VTC 3120.00 (Manual); [IP]; Perform the following tasks:  
Purchase and implement VTC CODECs and other VTC devices that support encryption of "Remote Control/Management/Configuration" protocols via the use of encrypted protocols or encrypted VPN tunnels between the managing PC/workstation and the managed device.

AND

Configure VTC CODECs and other VTC devices to use encrypted "Remote Control/Management/Configuration" protocols or an encrypted VPN tunnel between the managing PC/workstation/server and the managed device.

**Responsibility:** IAO, SA

**Mitigations:** Pass unencrypted management protocols through an encrypted VPN between the managing PC/workstation/server and the managed device.

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3130.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017702</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3130.00 [IP]; Disable Unnecessary Protocols**

**Vul. Name:** Unnecessary/unused remote control/management/configuration protocols are not disabled.

**Discussion:** Management or other protocols, secure or not, that are not required or used for management of, or access to, a device in a given implementation, but are active and available for a connection, places the device at risk of compromise and unauthorized access. These protocols must be disabled or turned off.

**Default Details:** Unnecessary/ unused "Remote Control/Management/Configuration" protocols are not disabled providing an avenue for system/device compromise.

**Pot'l Impacts:** The availability of unused or unneeded ports, protocols, and services used to configure and manage or otherwise access a VTC system/device could lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices

**Mgmt Category:** 14.4 - Internal Enclave Network Security - Unneeded Ports, Protocols, and Services

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.7.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3130.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:  
Ensure remote access ports, protocols, and services used for VTC system/device "Remote Control/Management/Configuration" are disabled, turned off, or removed if not required in the specific implementation of the device.  
  
Determine what ports, protocols, and services are required for in the specific implementation of the device. Have the SA demonstrate the device configuration regarding these protocols or independently validate that only the required ports, protocols, and services are active. Validation can be performed by performing a scan of the network and management interface of the system/device. This is a finding if it is determined that there are ports, protocols, and services active that are not needed for the specific implementation of the device.

**Fixes:** RTS-VTC 3130.00 (Manual); [IP]; Perform the following tasks:  
Configure the VTC system/device such that unused or unneeded ports, protocols, and services are disabled or removed from the system.

**Responsibility:** IAO, SA

**Mitigations:**

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3140.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017703</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3140.00 [IP]; SNMP Requirements**

**Vul. Name:** SNMP is not being used in accordance with the Network Infrastructure STIG.

**Discussion:** Some VTC endpoints can be monitored using SNMP. It is also possible that if not today, in the future, VTC endpoints could be configured via SNMP. SNMP is typically used by vendor's VTU/MCU management applications but it is conceivable that SNMP traps could be sent to any SNMP compatible network management system. At the time of this writing, applicable STIG requirements for the use of SNMP are contained in the Network Infrastructure STIG.

**Default Details:** SNMP is not being used in accordance with the Network Infrastructure STIG .

**Pot'l Impacts:** Improperly configured SNMP monitoring and management protocols used to monitor or control/manage/configure a VTC system/device could lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices

**Mgmt Category:** 14.1 - Internal Enclave Network Security - Network Management Services (NMS)

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.7.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3140.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

If SNMP is used to monitor or remotely control/manage/configure a VTC system/device, ensure the use of SNMP is performed in compliance with the applicable SNMP requirements found in the Network Infrastructure STIG.

This is a finding if SNMP is not being used in accordance with the Network Infrastructure STIG.

**Note:** During APL testing, this is a finding in the event SNMP configuration cannot come into compliance with the Network Infrastructure STIG.

**Fixes:** RTS-VTC 3140.00 (Manual); [IP]; Perform the following tasks:

If SNMP is used to monitor or remotely control/manage/configure a VTC system/device, implement and configure SNMP in compliance with the applicable SNMP requirements found in the Network Infrastructure STIG.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3160.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017704</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3160.00 [IP]; Management/Configuration IP addresses**

**Vul. Name:** Remote management access and SNMP access and reporting is not restricted by IP address and/or subnet.

**Discussion:** In any network device management system, it is best practice to limit the IP address or addresses from which a network attached device can be accessed and to which device status information can be sent.

**Default Details:** The source and/or destination of VTC system/device "Remote Control/Management/Configuration" and monitoring/status traffic is not limited to authorized IP address.

**Pot'l Impacts:** Not limiting the source and/or destination of VTC system/device "Remote Control/Management/Configuration" traffic to/from authorized IP addresses could lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices

**Mgmt Category:** 14.1 - Internal Enclave Network Security - Network Management Services (NMS)

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.7.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3160.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:  
If the VTU is connected to an IP based LAN, ensure remote management access (administrator and management system/server/application) and SNMP access and reporting is restricted by IP address and/or subnet.  
Determine what IP addresses or subnets are authorized to send VTC system/device "Remote Control/Management/Configuration" messages and what IP addresses or subnets are authorized to receive monitoring or status messages from the VTC system/device. Have the SA demonstrate how the VTC system/device is configured to restrict "Remote Control/Management/Configuration" messages to and from these authorized IP addresses or subnets. This is a finding if there is no limitation on either sending or receiving these messages.  
**Note:** During APL testing, this is a finding in the event the VTC system/device does not support the limiting of all management traffic to authorized IP addresses or subnets.

**Fixes:** RTS-VTC 3160.00 (Manual); [IP]; Perform the following tasks:  
Configure the VTC system/device to restrict The source and/or destination of VTC system/device "Remote Control/Management/Configuration" and monitoring/status traffic to/from authorized IP addresses or subnets.

**Responsibility:** IAO, SA

**Mitigations:**

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3320.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017705</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3320.00 [IP][ISDN]; Use Latest Firmware, Software, and Patches**

**Vul. Name:** A VTC system/device is not running the latest DoD approved patches/firmware/software from system/device vendor.

**Discussion:** Some of today's VTUs do not appropriately protect their passwords or access codes. Best practice and DoD policy dictates that authenticators are to be protected. This includes user account names, passwords, PINs, access codes, etc. The primary method used to protect these bits of information is encryption in transit for both the username and the password, and encryption of passwords in storage. It has been found that some VTC endpoint vendors do not provide this protection for passwords in storage, or at least, have not in the past.

The first such vulnerability to be aware of is one where the administrator password can be obtained across the network by requesting certain files from the CODEC using a web browser. Once the file is accessed, the admin password is displayed in the clear within the source code for the page.

The second such vulnerability to be aware of is one where, in one vendor's product line, the user access codes are stored in a clear text file that is uploaded to the CODEC. This file is accessible from the FTP server on the CODEC. Access is, however, protected by the remote access password. One can only assume the vendor does not value these access codes as an IA measure since the discussion of their use relates to call accounting.

Vulnerabilities like these and other issues are typically addressed by vendors like most issues are addressed, via patches to software, firmware upgrades, and major new releases of code. As such, it is good practice and a widely used DoD requirement that DoD systems should be running the latest version of software and install all patches to mitigate IA issues. Such is the purpose of the DoD IAVM program as required by DoD 8500.2 IA control VIVM-1 as well as mentioned in ECND-1 and ECND-2.

**Default Details:** A VTC system/device is not running the latest DoD approved patches/firmware/software from system/device vendor.

**Pot'l Impacts:** Out-dated software or firmware could lead to denial of service or the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECND-1 Enclave and Computing Environment/Network Device Controls  
ECND-2 Enclave and Computing Environment/Network Device Controls  
VIVM -1 Vulnerability and Incident Management/Vulnerability Management  
DCBP-1 Security Design and Configuration/Best Security Practices

**Mgmt Category:** 3.1 - Patch Management - Security Patches

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.8.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3320.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
Ensure all VTC systems/devices within his/her control are running the latest DoD approved patches, firmware, and/or software from the VTC system/device vendor to ensure the most current IA vulnerability mitigations or fixes are employed.

**Note:** It is highly recommended that all patches, firmware, and/or software applied to DoD ISs be digitally signed and appropriately hashed by the vendor to ensure its authenticity and integrity.

This is a finding if a CODEC and other VTC equipment are not using latest software/firmware/patches from the VTC system/device vendor as tested and/or approved by the DoD. Validate that the latest software/firmware/patches are installed and inspect the documentation regarding DoD testing and approval of the installed versions.

**Fixes:** RTS-VTC 3320.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Ensure updates to software firmware are patched, tested, and approved by a DoD entity prior to installation of such updates and patches per DoD policy.  
AND  
Install the latest DoD approved patches/firmware/software from system/device vendor.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3420.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017706</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3420.00 [IP][ISDN]; DoD Logon “Electronic Notice (Warning) and Consent Banner”**

**Vul. Name:** A DoD logon Electronic Notice (Warning) and Consent Banner is not displayed prior to logon and acknowledged by the user.

**Discussion:** DoDI 8500.2 IA control ECWM-1 regarding “Warning Message”; requires “users” to be warned that “they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.” This requirement applies to all user and administrative access points or interfaces to a DoD IS. Additionally the DoD CIO has issued new, mandatory policy standardizing the wording of “notice and consent” banners and matching user agreements for all Secret and below DoD information systems, including stand-alone systems by releasing DoD CIO Memo, “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement”, dated 9 May 2008. The Banner is mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance. Implementation of this banner verbiage is further directed to all DoD components for all DoD assets via JTF-GNO CTO 08-008A. This also applies to all management ports or interfaces to system or network devices as well as OAM&P/NM workstations must display a DoD approved warning banner at login regardless of the means of connection or communication.

The purpose of the logon warning or “Electronic Notice and Consent Banner” is two-fold. First, it warns users that unless they are authorized they should not proceed. It is like an electronic “No Trespassing” sign that allows prosecution of those who do trespass. Secondly, it warns both authorized and unauthorized users that they are subject to monitoring to detect unauthorized use and access if they do logon or attempt to logon. This provides the informed consent that again allows prosecution of those who abuse or damage the system. Not displaying the properly worded banner will hamper the sites legal authority or ability to monitor the given device. Failure to display the required login banner prior to logon attempts will also limit the sites ability to prosecute unauthorized access which has the potential of criminal and civil liability for systems administrators and information systems managers who fail to cause the banner to be displayed.

Specifics for compliance with this requirement are defined in the DoD CIO Memorandum noted above. It states the warning banner must present specific verbiage as defined in the memorandum and be associated with a specifically worded user agreement. Furthermore it states “Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating “OK.”]

**Note:** the memorandum specifies two banners; banner A having 1300 characters for use on most systems and one for use on devices with severely limited display capability such as a PDA, and banner B having only 49 characters. Both reference the user agreement and their verbiage must not be altered.

The required verbiage for most systems including VTC systems is as follows:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.

See User Agreement for details.

Banner requirements are applicable to any and all DoD information systems, and more specifically those requiring a logon for access.

All user and administrator access requires a logon per DoD policy. Acknowledgment of the banner with a keystroke or mouse click before receiving the logon screen is the preferred display and acknowledgment method which can be

supported on most if not all user and management terminals/workstations and many managed systems/devices. Unfortunately, some managed systems/devices cannot support this due to limitations in memory and/or processing power. In this case, the banner must minimally be displayed on the logon screen. Continuing to login, implies acknowledgement and consent based upon the login being the acknowledgement keystroke.

In order for VTC systems and devices to properly comply with the warning banner requirement, the banner must be displayed and acknowledged in the following situations:

When a normal user or administrator logs-in to or activates the VTU locally. i.e., when the VTU is initially powered on and when it comes out of sleep mode (selectable) in the event sleep mode is used instead of powering off the VTU.

When an administrator remotely accesses/ logs-in to a VTU or any other VTC system device (e.g., MCU, gateway, any server) over any network connection whatever the purpose, access method, application, or protocol used.

When an administrator accesses/ logs-in to a management suite/application and/or its supporting platform(s).

When a user is required to logon to a multipoint conference via a MCU.

When a user accesses/ logs-in to an independent scheduling system. i.e., a stand alone scheduling application hosted on a server or appliance (e.g., application or web server). This would not be required if the scheduling process was performed through another application that the user was running on their platform such as a collaboration or unified communications tool/application to which they had already logged in.

When a user accesses/ logs-in to a streamed conference whatever the source. e.g., VTU or streaming media server.

Regarding the inclusion of the MCU in the above list; it is debatable whether a MCU (centralized or VTU integrated) needs to comply with this requirement. While the MCU and VTU-MCU are DoD ISs, the argument can be made that a user accessing the MCU should have already logged into a VTU which is the endpoint of the VTC system (viewing and acknowledging the banner). This argument works if the VTU and MCU are part of the same organization or integrated system. However, the argument does not work if the MCU is, or can be, accessed by someone from a different organization than the one that operates the MCU and more so if the person accessing the MCU is a non-DoD entity. Therefore the access control mechanism for the MCU must present the user with the banner and require its acknowledgement. In some cases this function could be handled by a device external to the MCU (if used) that authenticates the user and controls access to the MCU.

VTC endpoints (and MCUs) typically do not support this requirement (that is, at the time of this writing). No "warning banner/message" is displayed on configuration interfaces or to a user. Some VTUs provide a capability that permits the use of a customized company logo in place of the vendor's logo on the welcome or possibly some other screen. This is implemented by uploading a graphics image file such as a .jpg to the VTU. This feature can and should be used, in lieu of a better method, to install a warning banner that is shown to the user on initial startup of the VTU and while it is not participating in a conference. This feature could provide partial and minimal compliance with the DoD banner requirement, but only for VTU users and administrators using the local access method with the remote control.

A suggested process for this non-compliance mitigation follows: Banner text can be written and formatted in a text editor as appropriate to fit the display parameters of the CODEC for its logo display. This formatted text can be converted to .jpg or other compatible graphics file using a screen capture program such as PrintKey v3.0. Experimentation may be necessary to get the banner to display cleanly in a readable size. VTC administrators who successfully implement a banner in this manner are encouraged to send their file to the FSO helpdesk [fso\\_spt@disa.mil](mailto:fso_spt@disa.mil) along with the make and model of VTU on which it was installed so that it may be shared with others.

**Note:** While the mitigation suggested above is a partial solution, it does not solve the problem and vendors need to build this functionality into their products that are sold to the DoD to meet DoD policy.

**Default Details:** One or more of the following interfaces on one or more VTC system devices do not present a warning and consent banner to the user or administrator prior to allowing access during and/or during logon.

- Local display for local user or administrator logon
- Remote administrative interface
- Conference streaming interface on the VTU or a streaming server
- Centralized management application
- Scheduling system interface

OR

The banner does not utilize banner text that conforms to current DoD policy and is legally approved.

**Pot'l Impacts:** The inability to perform legal monitoring and to properly prosecute violations

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

ECWM-1 - All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.

**Mgmt Category:** 11.6 - Information Handling - Warning Banners

**Severity:** CAT II

**Sev. Override:** NONE

- References:** DoD Video Tele-Conference STIG, Section: Section: 3.9
- Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)
- Checks:** RTS-VTC 3420.00 (Interview); [IP][ISDN]; Have the IAO or SA demonstrate compliance with JTF-GNO CTO 08-008A and DoD CIO Memo, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement", dated 9 May 2008 or attempt login from each interface and method. Validate that the user interface and management ports or interfaces to system or network devices as well as OAM&P/NM workstations display the mandatory warning banner verbiage at login regardless of the means of connection or communication. The required verbiage follows:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

If the system is incapable of displaying the required banner verbiage due to its size, a smaller banner must be used. The mandatory verbiage follows: "I've read & consent to terms in IS user agreem't."

Note: if the application and server comprise a purpose built appliance, the application or platform operating system may perform the function.

- All management ports/interfaces on managed systems/devices/servers. Displayed before logon regardless of the port/interface (physical or logical), means of connection (e.g., serial modem or dumb terminal, Ethernet, workstation, local or remote connection, etc), or communication protocol (e.g., serial and/or IP protocols, etc); and acknowledged with a keystroke or mouse click before receiving the logon screen; Or minimally in the event a managed system/device cannot support a keystroke acknowledgement, the banner must minimally be displayed on the logon screen/page. Continuing to login, implies audited acknowledgement and consent assuming the logon is audited as required.
  - The banner text conforms to current DoD policy and is legally approved.
- User agreements include verbiage in support of the warning banner as necessary to comply with current DoD policy.

Note: For VTC systems and devices to comply with this requirement, a warning banner is to be displayed and acknowledged prior to logon under the following circumstances:

- When a normal user or administrator logs-in to or activates the VTU locally. i.e., when the VTU is initially powered on and/or when it comes out of sleep mode in the event sleep mode is used instead of powering off the VTU.
- When an administrator remotely accesses/logs-in to a VTU or any other VTC system device over any network connection whatever the purpose, access method, application, or protocol used.
- When an administrator accesses/ logs-in to a management suite/application and/or its supporting platform(s)
- When a user accesses/ logs-in to an independent scheduling system. i.e., a stand alone scheduling application hosted on a server or appliance (e.g., application or web server). This would not be required if the scheduling process was performed through another application that the user was running on their platform such as a collaboration or unified communications tool/application to which they had already logged in.
- When a user accesses/ logs-in to a streamed conference whatever the source. e.g., VTU or streaming media server.

Note: It is understood that this requirement will generate a finding for most if not all VTC devices in use or available today. Vendors are encouraged to provide the required functionality to meet this requirement in future products, not only for their DoD customers but also for other Federal government customers that most likely need to comply with NIAP SP 800-53 AC-8. Vendors are also encouraged to produce patches or firmware/software upgrades to add this functionality to products that are already deployed and in use throughout the DoD and federal government today.

Note: During APL testing, this is a finding in the event this requirement is not supported by the VTC system devices

Inspect VTC/VTU equipment and verify that the Logon Consent Banner is displayed on all user and administrator workstations, all NMS/EMS servers, and/or applications. Additionally verify banner text conforms to current DoD

policy and is legally approved. Verify that warning banners are displayed prior to the following:

- When a normal user or administrator logs-in to or activates the VTU locally. i.e., when the VTU is initially powered on and/or when it comes out of sleep mode in the event sleep mode is used instead of powering off the VTU.
- When an administrator remotely accesses/logs-in to a VTU or any other VTC system device over any network connection whatever the purpose, access method, application, or protocol used.
- When an administrator accesses/ logs-in to a management suite/application and/or its supporting platform(s)
- When a user accesses/ logs-in to an independent scheduling system. i.e., a stand alone scheduling application hosted on a server or appliance (e.g., application or web server). This would not be required if the scheduling process was performed through another application that the user was running on their platform such as a collaboration or unified communications tool/application to which they had already logged in.
- When a user accesses/ logs-in to a streamed conference whatever the source. e.g., VTU or streaming media server.

**Fixes:**

RTS-VTC 3420.00 (Manual); [IP][ISDN]; Comply with JTF-GNO CTO 08-008A and DoD CIO Memo, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement", dated 9 May 2008.

Configure the user interface and management ports and interfaces to the network device to display the DoD mandated warning banner verbiage at login regardless of the means of connection or communication. The required banner verbiage that must be displayed verbatim is as follows:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

If the system is incapable of displaying the required banner verbiage due to its size, a smaller banner must be used. The mandatory verbiage follows: "I've read & consent to terms in IS user agreem't.

Ensure the specifically worded (per policy) warning and consent banner is displayed and acknowledged when a user or administrator accesses or logs-on to any interface or service provided by the VTC system minimally as follows:

- When a normal user or administrator logs-in to or activates the VTU locally. i.e., when the VTU is initially powered on and/or when it comes out of sleep mode in the event sleep mode is used instead of powering off the VTU.
- When an administrator remotely accesses/logs-in to a VTU or any other VTC system device over any network connection whatever the purpose, access method, application, or protocol used.
- When an administrator accesses/ logs-in to a management suite/application and/or its supporting platform(s)
- When a user accesses/ logs-in to an independent scheduling system. i.e., a stand alone scheduling application hosted on a server or appliance (e.g., application or web server). This would not be required if the scheduling process was performed through another application that the user was running on their platform such as a collaboration or unified communications tool/application to which they had already logged in.
- When a user accesses/ logs-in to a streamed conference whatever the source. e.g., VTU or streaming media server.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 3460.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017707</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3460.00 [IP]; Compliance with all applicable STIGs**

**Vul. Name:** All VTC system management systems/servers are not configured in compliance with all applicable STIGs

**Discussion:** Most VTC system vendors offer a range of centralized VTC system management applications and application suites. These include VTC endpoint and MCU managers, gatekeeper, gateway, and scheduling software. Gateways, gatekeepers, and scheduling systems are discussed later in this document.

The advantage of implementing a management system for the management of VTC endpoints is that all endpoints can be managed from a central location and their configuration can be standardized. This is a good thing in that configuration changes made on any given endpoint for temporary purposes can be discovered and corrected easily.

The disadvantage is that their use makes all managed VTC endpoints vulnerable and at risk of compromise if the management system is compromised.

While compliance with all applicable STIGs is covered in the next subsection, additional guidance may be provided in a future release of this or a related document.

Typically, VTC vendors provide their management applications and other infrastructure products on appliances with embedded operating systems (modified/scaled down, general purpose, or proprietary) and other application and database code (proprietary or otherwise). Some of these applications may be provided to run on a general purpose platform.

In general, to mitigate risks, all VTC system management applications and application suites, including endpoint and MCU managers, gateways, gatekeepers, and scheduling systems must be operated on secure or hardened platforms and comply with all applicable DoD STIGs with specific emphasis on user accounts, roles/permissions, access control, and auditing.

**Default Details:** All applicable STIGs are not being used to secure VTC system/device management suites/applications, gateways, and/or scheduling systems.

**Pot'l Impacts:** Not using DoD STIG guidance to secure VTC system/device management systems/servers could lead to denial of service or the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 14.3 - Internal Enclave Network Security - Network Device Configuration

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 3.10.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3460.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

Ensure all VTC system management suites/applications, gateways, and scheduling systems are configured in compliance with all applicable STIGs and are operated on STIG compliant platforms.

**Note:** The following is a listing of, but possibly not all, applicable STIGs:

- Operating system e.g., Windows, UNIX
- Web Server, Application Services
- Database
- Application Development, Application Security Checklist

Determine the STIGs that are applicable to the site's VTC system management suites/applications, gateways, and scheduling systems. Inspect documentation regarding the IA review of these systems and applications against the applicable STIGs. This is a finding only if the site's VTC system management suites/applications, gateways, and scheduling systems have not been reviewed against all applicable STIGs. This is not a finding if all applicable reviews have been performed regardless of the number of findings determined during those reviews. The IA posture of the reviewed system is based on the results of those reviews.

**Fixes:** RTS-VTC 3460.00 (Manual); [IP]; Perform the following tasks:

- Determine the STIGs that are applicable to the VTC system's management suites/applications, gateways, and scheduling systems.
- Configure these systems in accordance with the requirements in the applicable STIGs

**Responsibility:** IAO, SA

Mitigations: N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3620.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017708</b>	<b>Severity:</b> <b>CAT III</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3620.00 [IP][ISDN]; VTC Endpoint Office Installation Policy**

**Vul. Name:** Deficient SOP or enforcement regarding the approval and deployment of VTC capabilities.

**Discussion:** Due to the various IA issues surrounding VTC endpoint operation, they should only be installed or deployed where there is a validated requirement for their use. Conference room systems are easily justified and beneficial to an organization. General deployment to every desk in an organization is more difficult to justify. Deployments of office-based VTUs, desktop VTUs, and PC software based VTC applications must be considered on the basis of a validated need for the user to have this capability. Such needs should be revalidated annually.

In general, when VTC systems are implemented, consideration must be given to mission benefit weighed against the operational risks and the possibility of improper disclosure of information as discussed throughout this document. While this is important for ISDN only connected VTUs, this is most important for IP connected VTUs.

The site must develop policies and enforce them regarding the deployment of VTC endpoints in support of IA control DCSD-1, which requires IA documentation be maintained, and IA control DCPR-1 which requires a change management process be instituted.

**Default Details:** There are no local policies developed and/or enforced regarding the approval and deployment of office-based VTUs, desktop VTUs, and PC software based VTC applications.  
AND/OR  
Such policies do not include and/or address the following:  
- Validation and justification of the need for VTC endpoint installation to include annual revalidation.  
- Approval of VTC endpoint deployment on a case by case basis.  
- Documentation regarding the validation, justification, and approvals.

**Pot'l Impacts:** Without a local policy giving guidance to proper use and deployment of office-based VTUs, desktop VTUs, and PC software based VTC applications could lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECND-1 Enclave and Computing Environment/Network Device Controls - A network device control program/policies/SOPs/instructions/restrictions/protections/documentation

**Mgmt Category:** 12.1 - INFOCON Policy & Procedures

**Severity:** CAT III

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 4.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3620.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
Ensure local policies are developed and enforced regarding the approval and deployment of office-based VTUs, desktop VTUs, and PC software based VTC applications. Such policies will include and/or address the following:  
- Validation and justification of the need for VTC endpoint installation to include annual revalidation.  
- Approval of VTC endpoint deployment on a case by case basis.  
- Documentation regarding the validation, justification, and approvals.

Inspect the documentation regarding the policy for justifying the installation of office-based VTUs, desktop VTUs, and PC software based VTC applications. Inspect the documentation regarding the justification and re-justification of the need for all VTC endpoint installations. This is a finding if there is no documented policy, or if installation justifications have not been documented.

**Fixes:** RTS-VTC 3620.00 (Manual); [IP][ISDN]; Perform the following tasks:  
- Develop, document and enforce a policy regarding the justification for the installation of office-based VTUs, desktop VTUs, and PC software based VTC applications  
- Document the justification for the installation of all office-based VTUs, desktop VTUs, and PC software based VTC applications  
- Maintain this documentation for inspection by auditors.

**Responsibility:** IAO, SA

Mitigations: N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3640.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017709</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

## RTS-VTC 3640.00 [IP][ISDN]; DAA Approval for VTC Implementation

**Short Name:**

**Vul. Name:**

A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.

**Discussion:**

DoDI 8500.2 IA control DCII-1 regarding "Security Design and Configuration/IA Impact Assessment" states "Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation."

IA control DCII-1 essentially requires that the risk of operating any DoD system or application be assessed, defined, and formally accepted before use. The person responsible for the enclave's network and system's or application's accreditation is the DAA. The DAA is also "the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk" per the definition of the DAA in DoDD 8500.1.

For the above reasons, the DAA must approve changes to an existing system or the implementation of a new system or application that can affect the IA posture and therefore the accreditation of the system(s) for which he/she is responsible.

The IA issues surrounding the use of VTC endpoints warrant DAA approval. The DAA responsible for the network supporting a VTC endpoint and area in which it is installed must be made aware of the issues and vulnerabilities presented to the network, the area, and information processed as well as the mitigations for same. Once informed, the DAA can approve operation with "an acceptable level of risk" if so inclined. Approval by the DAA responsible for the locally effected enclave/network/area must be obtained in addition to accreditation received from the DISN DAAs represented by the DISN Security Accreditation Working Group (DSAWG) through the DoD APL or other pre-deployment approval process such as the Information Support Plan (ISP) or Tailored Information Support Plan (T-ISP) process.

The DAA approval required here is for the addition of IP based VTC endpoints or VTC infrastructure devices (MCUs, gatekeepers, gateways etc) to the base network and/or organization's intranet. This is not intended to require separate approval for each individual endpoint in a multi-endpoint system; however, if the system is a single endpoint, it may require an individual approval.

**Default Details:**

A VTC management system or endpoint use does not have written approval and acceptance of risk by the responsible DAA.

**Pot'l Impacts:**

DAA risks making an uninformed decision regarding the purchase and use of VTC system or device. And The inability to legally connect a VTC system to the network.

**8500.2 IA Cont:**

DCII-1 IA Security Design and Configuration/Impact Assessment - Changes to the IS are assessed for IA and accreditation impact prior to implementation.

**Mgmt Category:**

12.6 - Configuration Management Policies - CAP

**Severity:**

CAT II

**Sev. Override:**

NONE

**References:**

DoD Video Tele-Conference STIG, Section: Section: 4.2

**Conditions:**

Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:**

RTS-VTC 3640.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:

Ensure the DAA responsible for the network and/or for the operation and use of a VTC system or endpoint(s) provides written approval or acceptance of risk for such usage and operation on the network. Approval is based upon the documented risks and use case justifications with a full understanding of the issues, vulnerabilities, and mitigations surrounding VTC system implementation.

**Note:** maintain justification, implementation, and approval documentation pertaining to such use and implementation for inspection by auditors.

**Note:** Appropriate documentation is added to the Site Security Authorization Agreement (SSAA) or other documentation that exists for the accreditation of the supporting network and the accreditation is adjusted accordingly. Stand alone VTC systems or endpoints such as those that connect using ISDN only may have their own accreditation or may be added to the site accreditation.

Inspect documentation to ensure that if VTC and VTU endpoints are in use, they have been approved by the responsible DAA in writing. This documentation should reference the risk assessment performed with the DAA's acknowledgement that he/she has a full understanding of any risk, vulnerabilities, and mitigations surrounding the

VTC implementation

**Fixes:** RTS-VTC 3640.00 (Manual); [IP][ISDN]; Perform the following tasks:  
- Fully document the risks and vulnerabilities associated with the connection to the network and operation of a VTC endpoint and/or management system. Additionally document the justifications for use in light of the risks as well as any mitigations and the residual risk.  
- Obtain written approval from the responsible DAA for the operation of the VTC endpoint and/or management system in question.

**Responsibility:** IAO

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3660.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017710</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3660.00 [IP][ISDN]; VTC Endpoint User/Administrator Training**

**Vul. Name:** Deficient IA training for VTC system/endpoint users, administrators, and helpdesk representatives.

**Discussion:** DoDI 8500.2 IA control PRTN-1 regarding "Personnel/Information Assurance Training" states "A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery."  
An "assigned IA responsibility" of any user or administrator of a DoD Information System (IS) is to operate the system or device in a secure and IA conscious or aware manner. This means that administrators have an "assigned IA responsibility" to configure systems and devices in a manner that mitigates vulnerabilities and other IA issues to the greatest extent possible. This also means that users have an "assigned IA responsibility" to use and operate systems and devices in the same manner.  
Under this IA control, users and administrators of VTC systems and endpoints must receive training that covers the vulnerabilities and other IA issues associated with operating a VTC system and/or endpoint. Additionally, users and administrators must be trained in the proper configuration, installation techniques, and approved connections for the VTC system and/or endpoint that are applicable to their exposure to the system. Furthermore, users and administrators must be trained in the proper operating procedures for the system so that meeting information is properly protected as well as other non-meeting related information in the area near a VTC endpoint is not improperly disclosed or compromised. Helpdesk representatives supporting a VTC system or endpoints must also be appropriately trained in all aspects of VTC operation and IA. This may be accomplished within a typical tiered helpdesk organization, but all representatives must be made aware of the IA vulnerabilities and issues.

**Default Details:** Deficient IA training for VTC system/endpoint users, administrators, and helpdesk representatives.

**Pot'l Impacts:** Without proper and periodic training to those directly responsible for VTC/VTU equipment and applications could lead to improper use and eventually lead to the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance..

**8500.2 IA Cont:** PRTN-1 Personnel / Information Assurance Training - A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery

**Mgmt Category:** 6.4 - Personnel – Training

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: 4.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3660.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
 Ensure VTC system/endpoint users, administrators, and helpdesk representatives receive training as follows:  
 - Administrators, helpdesk representatives, and users are trained in all VTC system and endpoint vulnerabilities, IA issues, risks to both meeting and non-meeting related information, and "Assured Service" capabilities.  
 - Users, administrators, and helpdesk representatives are trained in all aspects of VTC system and endpoint vulnerability/risk mitigation and operating procedures. This training may be tailored to the specific VTC system or devices the user is receiving, will receive, (e.g., office VTU, desktop VTU, or PC soft-VTU) or is authorized to use (e.g., a conference room system).  
 - Administrators and helpdesk representatives are trained in all aspects of VTC system and endpoint configuration and implementation to include approved connections.  
 Furthermore ensure such training includes the requirements in this STIG and other DoD policies that address acceptable use and secure/proper operation and configuration of the various VTC endpoint types and their associated systems. Topics to be covered in such training are, but are not limited to, the following:  
 -The details contained in the SOPs intended to mitigate the vulnerabilities and risks associated with the configuration and operation of the specific VTC system or devices to include:  
 > Protection of the information discussed or presented in the meeting such as the technical measures to prevent disclosure as well as the inadvertent disclosure of sensitive or classified information to individuals within view or earshot of the VTU.  
 >The inadvertent disclosure of non-meeting related information to other conference attendees while sharing a presentation or other information from a PC workstation.

- >The inadvertent capture and dissemination of non-meeting related information from the area around the VTC endpoint to the other conference attendees.
- >The ability of the specific VTC system and network to provide or not to provide "Assured Service".
- Other training topics mentioned elsewhere in this document, are not listed here.

**Note:** Documentation is maintained regarding users, administrators, and helpdesk representative's receipt of training. Training is refreshed annually and may be incorporated into other IA training received annually.

**Note:** The site may modify these items in accordance with local site policy however these items must be addressed in the training materials.

**Note:** The site may adopt or incorporate appropriate training materials developed by another organization providing the required topics are covered.

- Inspect training materials to assess the coverage of the topics listed in the requirement.
- Inspect training records to determine if training is being provided on a recurring basis to all users, administrators, and helpdesk representatives.
- Interview a random sampling of users, administrators, and helpdesk representatives to determine if training has been received as required.

**Fixes:**

RTS-VTC 3660.00 (Manual); [IP][ISDN]; Perform the following tasks:

Develop training materials that cover the following:

- Administrators, helpdesk representatives, and users are trained in all VTC system and endpoint vulnerabilities, IA issues, risks to both meeting and non-meeting related information, and "Assured Service" capabilities.
- Users, administrators, and helpdesk representatives are trained in all aspects of VTC system and endpoint vulnerability/risk mitigation and operating procedures. This training may be tailored to the specific VTC system or devices the user is receiving, will receive, (e.g., office VTU, desktop VTU, or PC soft-VTU) or is authorized to use (e.g., a conference room system).
- Administrators and helpdesk representatives are trained in all aspects of VTC system and endpoint configuration and implementation to include approved connections.

Furthermore ensure such training includes the requirements in this STIG and other DoD policies that address acceptable use and secure/proper operation and configuration of the various VTC endpoint types and their associated systems. Topics to be covered in such training are, but are not limited to, the following:

-The details contained in the SOPs intended to mitigate the vulnerabilities and risks associated with the configuration and operation of the specific VTC system or devices to include:

> Protection of the information discussed or presented in the meeting such as the technical measures to prevent disclosure as well as the inadvertent disclosure of sensitive or classified information to individuals within view or earshot of the VTU.

>The inadvertent disclosure of non-meeting related information to other conference attendees while sharing a presentation or other information from a PC workstation.

>The inadvertent capture and dissemination of non-meeting related information from the area around the VTC endpoint to the other conference attendees.

>The ability of the specific VTC system and network to provide or not to provide "Assured Service".

- Other training topics mentioned elsewhere in this document, are not listed here.

Provide training to users, administrators, and helpdesk representatives initially and on an annually recurring basis. Maintain documentation on who received training and when.

**Responsibility:** IAM, IAO, SA, User

**Mitigations:**

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 3720.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017711</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3720.00 [IP][ISDN]; VTC Endpoint User's Agreement and Training Acknowledgment**

**Vul. Name:** VTC system user agreements are not signed or used when a user receives an endpoint or approval to use an endpoint.

**Discussion:** DoDI 8500.2 IA control PRRB-1 regarding "Security Rules of Behavior or Acceptable Use Policy" states "A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access."

This IA control requires, or at minimum supports, the generation and use of a "user agreement" that contains site policy regarding acceptable use of various IS assets. Requiring the user to read and sign the user agreement before receiving their government furnished hardware and/or software, or before gaining access to an additional IS or add on application or an additional privilege, provides the required acknowledgement.

The Secure Remote Computing STIG requires a user agreement be used and signed for a user to be permitted to remotely access a DoD network or system. The Wireless STIG adds policy items to this user agreement regarding the use of wireless capabilities in conjunction with remote access. While the first two STIGs mentioned require a user agreement prior to remote access privileges being granted, there should also be a user agreement signed when the user receives any government furnished hardware that covers all acceptable use policies to include such things as acceptable web browsing, remote access, all wireless usage, as well as the usage of certain applications and personal hardware and software.

This STIG defines most but not necessarily all of the rules of use and operational procedures for VTC endpoints of all types. Each endpoint type will or may require different rules and procedures. Users must be informed of the vulnerabilities and risks of VTC endpoint use and trained in the procedures required to mitigate them as described in the training requirement. Furthermore, users must acknowledge their awareness of the IA issues and mitigating requirements and their agreement to abide by the rules of operation of the VTC endpoint or system. This is accomplished by the user signing a "user agreement". This user agreement should restate the high points of the required training and might serve as an acknowledgement that the training was received. This user agreement can also include a statement of the penalties for non-compliance with the rules of operation.

**Default Details:** VTC system user agreements are not signed or used when a user receives an endpoint or approval to use an endpoint.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** PRRB-1 Personnel/Security Rules of Behavior or Acceptable Use Policy

**Mgmt Category:** 6.4 - Personnel – Training

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 4.5

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3720.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:

- Ensure VTC endpoint and/or system user's agreements are signed when a user receives an endpoint or approval to use an endpoint. The user agreement will provide, but is not limited to, the following:
  - Acknowledgement of their awareness of the vulnerabilities and risks associated with the use of the specific VTC system or devices the user is receiving, will receive, or use.
  - Acknowledgement of their awareness of the methods contained in the SOP and training materials intended to mitigate the vulnerabilities and risks
  - Agreement to operate the system in a secure manner and employ the methods contained in the SOP and training materials intended to mitigate the vulnerabilities and risks
  - Acknowledgement of the penalties for non-compliance with the rules of operation if stated in the agreement.
  - Acknowledgement of their awareness of the capability (or lack thereof) of the system to provide "assured service" for C2 communications

**Note:** The site may modify these items in accordance with local site policy however these items must be addressed in a user agreement.

Inspect signed user agreements for content and to validate that they are being used and signed.

**Fixes:**

RTS-VTC 3720.00 (Manual); [IP][ISDN]; Perform the following tasks:

Develop a user agreement. The user agreement will provide, but is not limited to, the following:

- Acknowledgement of their awareness of the vulnerabilities and risks associated with the use of the specific VTC system or devices the user is receiving, will receive, or use.
- Acknowledgement of their awareness of the methods contained in the SOP and training materials intended to mitigate the vulnerabilities and risks
- Agreement to operate the system in a secure manner and employ the methods contained in the SOP and training materials intended to mitigate the vulnerabilities and risks
- Acknowledgement of the penalties for non-compliance with the rules of operation if stated in the agreement.
- Acknowledgement of their awareness of the capability (or lack thereof) of the system to provide "assured service" for C2 communications

**Note:** The site may modify these items in accordance with local site policy however these items must be addressed in a user agreement.

Ensure users sign the user agreement when a user receives an endpoint or approval to use an endpoint. Maintain copies of the signed user agreements and provide a copy to the user for their reference.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 3740.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017712</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 3740.00 [IP][ISDN]; VTC Endpoint User's Guide**

**Vul. Name:** User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.

**Discussion:** User documentation packages should include user agreements, training documentation, and endpoint user guides that reiterate the training information and the agreed upon User Agreement policies. The Endpoint User Guides should also provide additional information to include system or device operations, usage procedures for features, and IA measures as required to address the protection of both meeting related and non-meeting related information  
**Note:** This requirement is supported by DoDI 8500.2 IA control PRRB-1 discussed above.

**Default Details:** User Guides and documentation packages have not been developed and distributed to users that operate and work with VTC endpoints.

**Pot'l Impacts:** The inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** PRTN-1 Personnel / Information Assurance Training - A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery

**Mgmt Category:** 6.4 - Personnel – Training

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 4.6

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 3740.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
 Ensure a user's guide and documentation package is developed and distributed to user's of VTC endpoints to include conference room systems that provides the following information:  
 - Reiterates the policies and restrictions agreed to when the user's agreement was signed upon receiving the VTC endpoint of authorization to use one.  
 - Provides cautions and notice of the non-assured nature of VTC communications so that C2 users are aware and reminded regarding the use of this communications media for C2.  
 - Provides instruction regarding the proper and safe use of a VTC endpoint's or conference room system's audio and video capabilities such that the appropriate confidentiality of meeting related and non-meeting related information is maintained.  
 - Provides instruction regarding the proper and safe use of document and desktop sharing when using a PC connected to a VTC endpoint such that the appropriate confidentiality of meeting related and non-meeting related information is maintained.  
 - Provides instruction regarding the safeguarding of meeting related and non-meeting related sensitive and/or classified information  
 An example of a user's guide brochure is included in Appendix E of the VTC STIG. The specifics relating to the brochure's development and the environment it addresses are noted in the appendix. It may not fully satisfy the requirement. Such a brochure can constitute one part of a larger user's guide or could be modified to fully meet the requirement.  
 Inspect the user's guide and documentation package for content and its existence.  
 Interview a random sampling of users regarding their possession and use of the user's guide  
 This is a finding if the user's guide is not distributed or its content is deficient with regard to the items in the requirement.

**Fixes:** RTS-VTC 3740.00 (Manual); [IP][ISDN]; Perform the following tasks:  
 Ensure a user's guide and documentation package is developed and distributed to user's of VTC endpoints to include conference room systems that provides the following information:  
 - Reiterates the policies and restrictions agreed to when the user's agreement was signed upon receiving the VTC endpoint of authorization to use one.  
 - Provides cautions and notice of the non-assured nature of VTC communications so that C2 users are aware and reminded regarding the use of this communications media for C2.  
 - Provides instruction regarding the proper and safe use of a VTC endpoint's or conference room system's audio and video capabilities such that the appropriate confidentiality of meeting related and non-meeting related information is maintained.

- Provides instruction regarding the proper and safe use of document and desktop sharing when using a PC connected to a VTC endpoint such that the appropriate confidentiality of meeting related and non-meeting related information is maintained.
- Provides instruction regarding the safeguarding of meeting related and non-meeting related sensitive and/or classified information

An example of a user's guide brochure is included in Appendix E of the VTC STIG. The specifics relating to the brochure's development and the environment it addresses are noted in the appendix. It may not fully satisfy the requirement. Such a brochure can constitute one part of a larger user's guide or could be modified to fully meet the requirement.

**Responsibility:** IAO, SA, User

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4120.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017713</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4120.00 [IP]; LAN Service Segregation**

**Vul. Name:** VTC systems are not segregated on the LAN from data systems and other non-integrated voice communication (VoIP) systems.

**Discussion:** A common and widely used practice in traditional LAN design is the use and implementation of VLANs (at layer 2) and IP subnets (at layer 3) to segregate services and organizational workgroups or departments including their traffic as it traverses the LAN. This has the effect of providing confidentiality for the workgroup traffic by limiting the ability of users in other workgroups to see and access the traffic during normal operations. It also enhances the ability to control traffic flows for, and access to, LAN services. Another benefit of using VLANs is that it can improve network performance if they are properly pruned. Typically, when a VLAN is configured on one LAN switch, the other switches in the network will "learn" that VLAN, thus it will propagate throughout the network. This property is not what enhances network performance since it allows broadcast traffic in the VLAN to traverse the entire network. Also if the number of allowable VLANs that a switch has configured or learns is exceeded, the LAN can become unstable. VLAN pruning eliminates this problem and is actually what can enhance network performance by limiting the traffic that devices in the LAN must process.

This practice is very useful in protecting a communications service running on the LAN. The use of a separate IP address space and separate VLANs for VoIP telephone systems (different than those assigned to data services) is required by the VoIP STIG. This requirement helps protect the voice communication service from compromise and will provide the same protection for VTC services running on the LAN.

The use of a separate IP address space and properly pruned separate VLANs for VTC systems will have the following effects:

- Enhance the confidentiality of unencrypted VTC traffic
- Enhance the confidentiality of the VTC device management traffic particularly if secure protocols are not available for use.
- Limit the ability of the average LAN user (in the data VLAN(s)) to "see" the VTC device(s) on the LAN (in the VTC VLAN(s)) thereby limiting the possibility of compromise from user or machine induced malicious activity (in data VLAN(s)).

**Note:** This separation is intended to protect the VTC devices and the information conveyed by them from compromise. It is not intended to prevent a PC soft VTC client (in the data VLAN(s)) from participating in a conference or from viewing a streamed conference. This can be implemented through appropriate routing and gateways. PC based soft-VTUs and their segregation is covered in a related document covering softphones and soft-VTUs.

Different VTC systems should be protected using different VLAN structures as follows:

- Primary conference room systems should have their own closely pruned VLAN and IP subnet. This could be a single conference room or several conference rooms if they are required to communicate with each other or are part of an overall managed VTC network within the enclave. This will provide the maximum protection from compromise for the conference room systems.
- Hardware based desktop and office VTUs should be grouped into their own VLAN and IP subnet. This could be the same VLAN and subnet as the one used for conference rooms if these devices are to communicate with them or if they are part of an overall managed VTC network within the enclave.
- Hardware based desktop and office VTUs that integrate and signal with the site's VoIP telephone system may be grouped separately or utilize the Voice system VLAN structure and IP subnet.
- PC based soft-VTU are to be implemented or segregated/controlled as described in the related document covering softphones and soft-VTUs.
- Local MCUs and VTU management stations must reside in the VTC VLAN and IP subnet with the devices they manage or conference.
- If WAN access is required, the VLAN(s) can be extended to the enclave boundary.

Another concern when implementing VLANs on a LAN is the default functionality of routers to create paths or routes between IP address that they can reach or are aware of. While it requires a routing device (router or a layer three switch) to communicate between VLANs, a router will by default create a route between the IP addresses in the different VLANs it "sees". This behavior works against the separation and protection provided by a segregated VLAN and IP subnet structure. To maintain the integrity of this structure, router ACLs must be configured on routing devices that block this default behavior. VTU Traffic is then only permitted to cross VLAN boundaries where required and at the points in the LAN where required.

**Note:** VLAN Pruning must limit the reach of the VLAN(s) to only those network elements and links required to interconnect the devices in the VLAN.

This requirement is supported by DoDI 8500.2 IA control DCSP-1 regarding Security Design and Configuration/Security Support Structure Partitioning which states "The security support structure is isolated by

means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process.”

**Note:** While separate IP subnets and VLANs closed by ACLs do provide the benefits noted above, they are not in and of themselves a security mechanism. The security benefit is derived from the behavior of VLANs configured in this manner. Additionally, it is known that the separation of VLANs can be overcome by specialized software which sometimes relies on an improperly configured LAN. Such software typically requires the attacker to have physical access to the LAN containing the VLANs. This in no way negates the benefit derived from using separate IP subnets and “closed” VLANs for the protection and benefit of VoIP and VTC systems.

- Default Details:** VTC system(s) have not been segmented to their own closed VLAN structure and IP address space/subnet and kept separate from the VLAN and IP address space/subnet structure(s) assigned to data or management traffic and other non-integrated voice communications (VoIP) systems.
- Pot'l Impacts:** The denial of service for a VTC system/device or the disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.
- 8500.2 IA Cont:** DCSP-1 Security Design and Configuration/Security Support Structure Partitioning  
DCBP-1 Security Design and Configuration/Best Security Practices - system security design incorporates best security practices  
ECND-1 Enclave and Computing Environment/Network Device Controls - A network device control program/policies/SOPs/instructions/restrictions/protections/documentation
- Mgmt Category:** 14.3 - Internal Enclave Network Security - Network Device Configuration
- Severity:** CAT II
- Sev. Override:** NONE
- References:** DoD Video Tele-Conference STIG, Section: Section: 5.1
- Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)
- Checks:** RTS-VTC 4220.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:
- Ensure a pruned and closed VLAN and IP address space/IP subnet structure is configured on the LAN for the VTC system(s) that is separate from the VLAN and IP address space/IP subnet structure(s) assigned to data systems and other non-integrated voice communications (VoIP) systems. VTC systems are segregated on the LAN from themselves and other LAN services as follows:
    - Primary conference room systems
    - Hardware based desktop and office VTUs
      - > Exception 1: If integrated with the VoIP phone system (i.e., signals with the local call controller), these devices may connect to the VoIP system VLAN structure.
      - > Exception 2: If part of an overall managed VTC network within the enclave and/or they must communicate with the conference room systems within the enclave, these devices may connect to the conference room VLAN structure. .
    - Local MCUs and VTU management stations must reside in the VTC VLAN and IP subnet with the devices they manage or conference.
    - If WAN access is required, the VLAN(s) can be extended to the enclave boundary.
- Note:** It is recognized that in some tactical environments or programs this requirement may not be able to be met due to various constraints. In this case, the situation must be documented and the responsible DAA must accept the risk for not meeting the requirement.
- Note:** It is recommended for VTUs that integrate VoIP telephone systems be implemented so that they work with the RTS Assured Service communications infrastructure being developed.
- Review network diagrams and router/switch configurations to verify that VTC endpoints and other systems/devices reside on a separate and dedicated IP space and VLAN, pruned and isolated from the data and management traffic, except in the cases noted in the vulnerability discussion. This is a finding if any of these criteria apply and are not implemented.
- Fixes:** RTS-VTC 4220.00 (Manual); [IP]; Perform the following tasks:
- Establish a dedicated network for VTC system devices that is separate from the site's LAN
- OR
- Establish a dedicated IP address space and/or subnet for the exclusive use of VTC system devices.
  - Establish one or more dedicated VLAN(s) on the LAN for the connection of the VTC system devices.
  - Establish ACLs on each routing device in the LAN to maintain the closed nature of the VTC VLAN structure.
  - Limit traffic that needs to cross between the VTC VLANs and the data or management VLAN to authorized traffic based on the service or authorized IP address.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4220.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017714</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4220.00 [IP]; Wireless STIG Compliance**

**Vul. Name:** VTC endpoint connectivity is established via an unapproved DoD Wireless LAN infrastructure

**Discussion:** In the event wireless LAN connectivity is to be used for VTC endpoints, it must be implemented via an established and approved wireless LAN infrastructure which is configured, along with its connected devices, in compliance with the Wireless STIG. Key requirements include WiFi and WPA2 certification of the VTC wireless LAN Network Interface Card (NIC) and FIPS 140-2 certification of the wireless encryption module.

**Default Details:** Wireless capability exists in a VTC endpoint and is available or actively being used without the proper security implementation per the Wireless STIG.

**Pot'l Impacts:** Unregulated and improperly configured wireless adapters have the potential to provide backdoor connectivity, which ultimately can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment /Security Configuration Compliance - all DoD STIGs (etc.) have been applied. - all DoD STIGs (etc.) have been applied.

**Mgmt Category:** 14.11 - Internal Enclave Network Security - Wireless Access Point

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 5.1.1.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 4220.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

Ensure VTC endpoint connectivity is established via an approved DoD wireless LAN infrastructure. Furthermore, ensure both the LAN and VTC endpoint are configured and operated in compliance with the Wireless STIG.

**Note:** During APL testing, this is a finding in the event the VTU cannot come into compliance with the applicable requirements in the Wireless STIG.

Inspect VTU configuration to verify with that if wireless is not required it is disabled. If wireless connectivity is required verify/inspect that the wireless functionality is configured and operating in accordance with the Wireless STIG.

**Fixes:** RTS-VTC 4220.00 (Manual); [IP]; Perform the following tasks:

If wireless LAN connectivity is required, configure the wireless LAN capabilities of a VTU using the applicable requirements in the Wireless STIG.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4320.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017715</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4320.00 [IP]; Simultaneous Wired and Wireless LAN Connection**

**Vul. Name:** VTC endpoints simultaneously connect to a wired LAN and a wireless LAN.

**Discussion:** A consideration regarding wireless LAN capabilities in VTC endpoints is the possibility that, with some implementations, a VTU could be connected to a wired LAN while also supporting a wireless connection in either ad hoc or infrastructure mode. Activating wireless capabilities on a VTU while it is connected to a wired LAN can provide an attack vector to that LAN. If the VTU connects via infrastructure mode to a non DoD WLAN in the vicinity of the VTU, a bridge could be formed between the 2 LANs compromising the DoD wired LAN as well as any conference sessions in which the VTU is included. If connected via an ad hoc connection, the same vulnerabilities exist for the conference since the other connected device may or may not be connected to another LAN. Either way, this has the potential of creating a back door to the DoD wired LAN, a vulnerability which must be mitigated by preventing this dual connectivity. The Wireless STIG describes security requirements for both ad hoc and infrastructure mode wireless connections. The following requirement parallels the Wireless STIG requirement WIR0161 for Personal Computers (PCs) and Personal Electronic Devices (PEDs).

**Default Details:** A VTU is connected wired LAN and supports an active wireless LAN/connection and permits traffic to pass traffic between the two networks. That is, the VTU provides a bridge between the wired and wireless LAN connections.

**Pot'l Impacts:** Unregulated and improperly configured wireless adapters have the potential to provide backdoor connectivity, which ultimately can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECWN-1 Enclave and Computing Environment/Wireless Computing and Networking - implemented in accordance with DoD wireless policy, as issued. Disable when not needed. Not independently configured by end users.

**Mgmt Category:** 14.11 - Internal Enclave Network Security - Wireless Access Point

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 5.1.1.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 4320.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:  
 Ensure VTC endpoints do not simultaneously connect to a wired LAN and a wireless LAN if traffic can pass between the two LANs (e.g., acts as a LAN bridge or IP router).  
**Note:** This is not a finding if it is proven that the VTU cannot pass network traffic from the wired LAN to the wireless LAN when dual connected and vice versa.  
**Note:** During APL testing, this is a finding in the event the VTU provides a bridge (passes traffic) between the wired and wireless LAN connections.

If the VTU supports an active wireless LAN connection (802.11x), and if it is connected to a wired LAN, determine if the VTU can pass traffic to/from the wireless LAN connection to/from the wired LAN connection.

**Fixes:** RTS-VTC 4320.00 (Manual); [IP]; Perform the following tasks:  
 Purchase and install only those VTUs that do not, or can be configured to not provide a bridge between a wireless and a wired LAN connection, or VTUs that do not support wireless LAN connectivity  
 OR  
 Configure the VTU to not provide a bridge (pass traffic) between its wired and wireless LAN ports.  
 OR  
 Use only one connection method. That is either a wired LAN connection or if absolutely required, a wireless LAN connection which is in compliance with the Wireless STIG.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4360.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017716</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4360.00 [IP]; Disable Wireless Support**

**Vul. Name:** A VTU endpoint does not have the wireless LAN capability disabled.

**Discussion:** The proper mitigation for the vulnerabilities discussed above is to disable the wireless capability available or included in a VTC endpoint. Typically, one would expect a configuration setting that says something like "Disable Wireless" that would disable any onboard wireless capability whether integrated or reliant on a plug-in card. The Wireless STIG in WIR0167 requires all wireless LAN NICs to be turned-off by default after system boot-up or whenever a wireless network connection is not required. Additionally WIR0130 requires that the NIC have the capability to disable ad hoc connectivity. While these requirements are addressed toward PCs and PEDs, they are applicable to VTC endpoints. Support for these requirements does not seem to be available with at least some VTC endpoint's PCMCIA wireless LAN card implementations. It is conceivable that a WLAN card could be inserted into the PCMCIA slot and activated with basic default settings and no security. To prevent this, the VTU's PCMCIA slot must be physically blocked, making it difficult to insert a WLAN card.

**Default Details:** A VTU supports a wireless LAN capability which is enabled, but not required.  
OR  
A VTU supports a wireless LAN capability which is not required and which cannot be positively disabled.

**Pot'l Impacts:** Unregulated and improperly configured wireless adapters have the potential to provide backdoor connectivity, which ultimately can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:** ECWN-1 Enclave and Computing Environment/Wireless Computing and Networking - implemented in accordance with DoD wireless policy, as issued. Disable when not needed. Not independently configured by end users.

**Mgmt Category:** 14.11 - Internal Enclave Network Security - Wireless Access Point

**Severity:** CAT II

**Sev. Override:** In the event a configuration setting is not available for a PCMCIA WLAN card that will disable it when one is plugged in, this finding can be reduced to a CAT III if the PCMCIA slot is fitted with a hard to remove device that prevents the insertion of a card into the slot.

**References:** DoD Video Tele-Conference STIG, Section: Section: 5.1.1.3

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 4360.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

Ensure wireless capability is configured as "disabled".

**Note:** In the event such a setting is not available for a PCMCIA WLAN card. This finding can be reduced to a CAT III if the PCMCIA slot is fitted with a hard to remove device that prevents the insertion of a card into the slot.

If the VTU supports wireless LAN connectivity and it is not needed, verify that it is disabled. In the event the wireless capability is supported by inserting a WLAN card onto a PCMCIA slot, verify that the wireless capability remains disabled when the card is inserted. In the event such a setting is not available for a PCMCIA WLAN card verify that the PCMCIA slot is fitted with a hard to remove device that prevents the insertion of a card into the slot.

**Note:** It is recognized that there is no mitigation for or configuration setting that would prevent the connection of an external wireless LAN adaptor via the wired LAN connection. This however would not permit both the wired and wireless LAN capabilities of the VTU to be active at the same time.

**Fixes:** RTS-VTC 4360.00 (Manual); [IP]; Perform the following tasks:  
Configure the VTU to disable wireless LAN capabilities whether an internal wireless adaptor or a WLAN card plugged into a PCMCIA slot is used.

OR  
Physically prevent the ability to insert a WLAN card into a PCMCIA slot.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4420.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017717</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4420.00 [IP][ISDN]; Wireless Conference Room Implementation**

**Vul. Name:** A VTU or conference room implemented using wireless components is not protected from external control or compromise

**Discussion:** Conference room VTC systems, and particularly large ones, can require multiple microphones, cameras, and displays along with AV control systems. These systems typically require a significant amount of wiring. This can be a problem when retrofitting a well appointed conference room without damaging the room's walls, ceilings, furniture, and finishes. As a result, conference room VTC systems as well as other VTC endpoint systems can utilize various wireless communication technologies to interconnect its microphones, cameras, speakers, desktop audio conferencing units, and displays to the VTC CODEC and control panels to the AV control system and CODEC. The wireless communications technologies used are 802.11, Bluetooth, standard radio (cordless telephone and wireless microphone frequencies/technology) as well as infrared.

The use of wireless technologies to implement a conference room in a DoD facility could pose an eavesdropping vulnerability to VTC conferences and other meetings held in the facility. This could place sensitive or classified DoD information at risk. To mitigate this, all audio, video, white boarding, and data sharing communications within the conference room system must be encrypted. Furthermore, those technologies covered by the Wireless STIG and other DoD wireless policies, must be in compliance with them.

**Default Details:** A VTC system has been assembled using one or more wireless RF based components with one or more of the components having one or more of the following deficiencies:  
 - Information-bearing RF transmissions are not encrypted to prevent eavesdropping.  
 - Control-bearing RF transmissions are not encrypted and/or not authenticated to prevent control hijacking.  
 - Wireless technologies covered by the wireless STIG (primarily 802.11x) and other DoD wireless policies are not implemented and configured in compliance with that STIG and other policies.  
 - The implementation is not approved by the responsible DAA in writing or the IAO has not maintained approval documentation for inspection by IA auditors.

AND/OR

The facility housing the VTC system is not shielded against RF transmissions leaving or entering the facility that could compromise the VTC system or the information communicated.

**Pot'l Impacts:** Unencrypted and unsecured wireless connectivity can allow for wireless sniffing and eavesdropping, which can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance. This can also lead to compromise or denial-of-service for the VTU or its components.

**8500.2 IA Cont:** ECSC-1 Enclave and Computing Environment/Security Configuration Compliance - all DoD STIGs (etc.) have been applied.  
 ECWN-1 Enclave and Computing Environment/Wireless Computing and Networking

**Mgmt Category:** 14.11 - Internal Enclave Network Security - Wireless Access Point

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 5.1.1.4

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 4420.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:

If the audio, video, white boarding, data sharing capabilities or components of a VTC system are implemented using wireless RF technologies, ensure the following:

- All information-bearing RF transmissions are encrypted to prevent eavesdropping.
- All control-bearing RF transmissions are encrypted and/or authenticated to prevent control hijacking.
- Wireless technologies covered by the wireless STIG (primarily 802.11x) and other DoD wireless policies are implemented and configured in compliance with that STIG and other policies.
- Such implementations are approved by the responsible local DAA in writing, and the IAO will maintain approval documentation for inspection by IA auditors.

**Note:** A much more expensive mitigation to this issue would be to enclose the room in RF shielding so that the information or control bearing VTC radio signals cannot escape the facility and external control signals cannot enter the facility. This might not be practical.

**Note:** Wireless AV control systems or "touch panels were discussed and requirements provided earlier in this

document. The earlier mentioned requirements are to be used in conjunction with this one.

**Note:** During APL testing, this is a finding in the event this requirement is not supported by the VTU.

Inspect the configuration of the VTC system and all wireless RF components and their associated documentation to ensure that the wireless traffic is protected as noted in the requirement. Also inspect approval documentation to ensure that the responsible local DAA has approved, in writing, the implementation of VTU based on wireless RF components.

**Fixes:**

RTS-VTC 4420.00 (Manual); [IP][ISDN]; Perform the following tasks:

Purchase and install wireless RF VTC system components that can support the following:

- The encryption of all information-bearing RF transmissions to prevent eavesdropping.
- The encrypted and/or authenticated of all control-bearing RF transmissions to prevent control hijacking.
- The configuration of wireless technologies covered by the wireless STIG (primarily 802.11x) and other DoD wireless policies is supported.

AND

Configure all wireless RF VTC system components to encrypt information-bearing RF transmissions to prevent eavesdropping and to encrypt and/or authenticate all control-bearing RF transmissions to prevent control hijacking.

AND

Obtain written approval from the responsible DAA for the use of wireless RF components to assemble the VTC system.

AND/OR

Enclose the facility housing the VTC system in RF shielding so that the information or control bearing VTC radio signals cannot escape the facility and external control signals cannot enter the facility.

OR

Implement a hardwired VTC system.

**Responsibility:** IAO, SA

**Mitigations:** Enclose the room in RF shielding so that the information or control bearing VTC radio signals cannot escape the facility and external control signals cannot enter the facility.

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 4520.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017718</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 4520.00 [IP]; PPS Registration**

**Vul. Name:** VTC ports and protocols cross DoD/Enclave boundaries without prior registration in the DoD Ports and Protocols Database.

**Discussion:** A portion of the DoDI 8550.1 PPS policy requires registration of those PPS that cross any of the boundaries defined by the policy that are "visible to DoD-managed components". The following PPS registration requirement applies to VTC traffic that crosses the IP based Enclave boundary to the DISN WAN or another enclave.

**Default Details:** VTC ports and protocols cross DoD/Enclave boundaries without prior registration in the DoD Ports and Protocols Database.

**Pot'l Impacts:** Unrestricted and undocumented traffic crossing enclave boundaries can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance as well as denial-of-service and the inability for the operators of the GIG to properly defend it and its interconnected enclaves.

**8500.2 IA Cont:** DCP-1 Security Design and Configuration/Ports, Protocols, and Services (PPS) - comply with DoD PPS guidance/register all active PPS

**Mgmt Category:** 4.1 - Perimeter Enclave Network Security - Unneeded Ports, Protocols, and Services

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 6.5.2

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 4520.00 (Interview); [IP]; Interview the IAO and validate compliance with the following requirement:

Ensure all protocols and services that cross the enclave boundary and/or any of the defined DoD boundaries (along with their associated IP ports) used by VTC systems for which he/she is responsible are registered in the DoD Ports and Protocols Database in accordance with DoDI 8550.1.

Review network diagrams, device documentation, to identify what VTC/VTU/MCU Ports/Protocols/Services are used by the VTC system. Once these Ports/Protocols/Services have been determined and confirmed for use, verify that these same Ports/Protocols/Services are registered and approved for use in the DoD Ports and Protocols Database in accordance with DoDI 8550.1.

**Note:** Reference tables are provided in the STIG

**Fixes:** RTS-VTC 4520.00 (Manual); [IP]; Perform the following tasks:  
- Determine what Ports/Protocols/Services are used by the VTC system within the enclave and which cross the enclave boundary as well as what other boundaries they traverse.  
- Register all Ports/Protocols/Services are used by the VTC system in the PPS database.

**Responsibility:** IAO, SA

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)**

<b>STIG ID:</b> <b>RTS-VTC 5020.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017719</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

## RTS-VTC 5020.00 [IP][ISDN]; Access Control for Multipoint Conferences

**Short Name:**

**Vul. Name:**

**Discussion:**

Access Control Measures are not implemented for all conferences hosted on a centralized MCU appliance.

Access control must be exercised over participants joining multipoint conferences. Attendees and/or endpoints must be pre-authorized or pre-registered. In this way, conference/meeting organizers can control who has access to sensitive or classified information based upon validated clearance and need-to-know. Unrestricted access or the use of a meeting password that is reused and/or well known can lead to a security incident where information is improperly disclosed to unauthorized individuals not having appropriate clearance or need-to-know.

In a previous topic, we discussed the access control required for multipoint conferences hosted by a VTC endpoint with an integrated MCU. Typically access control for such meetings is handled manually by the operator of the hosting VTU calling the participants and joining them to the conference. This is positive access control with the conference host controlling who has access to the session and being responsible, therefore, for the conferees need-to-know or authorization to receive conference information. Additionally, if call-in access is supported and approved, a one time use meeting password is required.

Multipoint conferences hosted on a MCU appliance or network element must also perform access control over who can join a meeting. This includes employing proper practices for distributing conference information as well as for assigning access codes. If access control is not exercised, anyone who knows any phone number or IP address on the MCU can "dial-in" any time and access whatever meeting is being hosted on the MCU at the given time. This cannot be permitted.

MCU Access control can be performed in various ways that may differ from vendor's product to vendor's product. Typically, MCU access is controlled by an H.323 gatekeeper, which uses H.225 gatekeeper RAS messages between itself and its endpoints. A combination of access control lists on the MCU and gatekeeper can also limit access. A full description of this process is beyond the scope of this release of this STIG but a brief description follows along with an issue. Further information can be found in several books and tutorials that are available in both print and on the web.

H.323 gatekeepers provide access control for VTC network infrastructure devices such as MCUs and gateways to VTC endpoints. Using H.225 an endpoint can discover a gatekeeper and register with it. The endpoint is identified by the gatekeeper by a "gatekeeper password" which is essentially the endpoint ID. The gatekeeper provides address translation and bandwidth management. Once registered with the gatekeeper an endpoint must ask permission of the gatekeeper to make a call. If the available VTC bandwidth is used or limited, the gatekeeper can reject the request or negotiate a lower bandwidth. This acts as part of the access control mechanism for the MCU and works in combination with a scheduling application. The rest of the MCU access control equation is pre registration of the endpoint IDs when scheduling a conference. Pre registration of endpoint IDs for specific conferences is required because there are typically no meeting passwords and the phone numbers or IP addresses of the MCU ports don't change between sessions. Additionally (and here's the issue mentioned above) people are not authenticated only endpoints are. The endpoint ID is critical in this access control process. The endpoint ID is entered (pre-configured) in the system for a specific scheduled conference. The system only permits the endpoint to access the MCU during the scheduled time of the conference.

This discussion also applies to ad hoc conferences and "standing" conferences. A standing conference is one where MCU facilities are dedicated to a conference that is operational all of the time or one that is regularly scheduled to be operational for certain time periods. The implementation of a standing conference permits conferees to join the conference at will or as needed to discuss a current topic or mission. Standing conferences are implemented for many reasons. Standing conferences are more vulnerable to compromise than one time scheduled events. Extra care must be exercised regarding access control to these conferences.

**Note:** This general requirement is supported by several DoDI 8500.2 IA controls such as IAIA-1, IAIA-2, and ECPA-1.

**Default Details:**

Access Control Measures are not implemented for all conferences hosted on a centralized MCU appliance.

**Pot'l Impacts:**

Unregulated access by any endpoint to MCU conferences can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance.

**8500.2 IA Cont:**

IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
ECPA-1 Enclave and Computing Environment/Privileged Account Control - use a role-based access scheme, IAM tracks privileged role assignments.

**Mgmt Category:**

1.1 - I&A - Passwords

**Severity:** CAT II  
**Sev. Override:** NONE  
**References:** DoD Video Tele-Conference STIG, Section: Section: 8.1  
**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)  
**Checks:** RTS-VTC 5020.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
Ensure access control measures are implemented for all conferences hosted on a centralized MCU appliance (i.e., not part of an endpoint) as follows:  
- Only authorized endpoints are permitted to access an MCU  
AND/OR  
- Only authorized users are permitted to access/join a conference. Authorization is pre-configured on the MCU access control system and is based on validated need-to-know as well as security clearance if applicable.  
**Note:** this applies to standing, scheduled one-time, and non-scheduled ad hoc conferences.  
Interview IAO and verify with SA and users that only authorized endpoints are permitted to connect to a centralized MCU for conferences. Inspect MCU to verify that there is a mechanism in place that authorization is required prior to accessing/joining conference.  
**Fixes:** RTS-VTC 5020.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Ensure access control measures are implemented for all conferences hosted on a centralized MCU appliance (i.e., not part of an endpoint) as follows:  
- Only authorized endpoints are permitted to access an MCU  
AND/OR  
- Only authorized users are permitted to access/join a conference. Authorization is pre-configured on the MCU access control system and is based on validated need-to-know as well as security clearance if applicable.  
**Note:** this applies to standing, scheduled one-time, and non-scheduled ad hoc conferences.  
**Responsibility:** IAO, SA, User  
**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

Reviewer Notes and Comments: (Not Applicable/Reviewed requires a reason.)

<b>STIG ID:</b> <b>RTS-VTC 5120.00</b>	<b>VMS Vulnerability Key:</b> <b>V0017720</b>	<b>Severity:</b> <b>CAT II</b>	<b>Policy:</b> <b>ALL</b>	<b>MAC:</b>			<b>Confidentiality</b>		
				<b>1</b>	<b>2</b>	<b>3</b>	<b>C</b>	<b>S</b>	<b>P</b>
				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>

**Short Name:** **RTS-VTC 5120.00 [IP][ISDN]; Scheduling System Access Control**

**Vul. Name:** Access Control Measures are not implemented for all conferences hosted on a centralized MCU appliance.

**Discussion:** Access control to the conference scheduling system must be exercised and limited to authorized individuals. This is accomplished in different ways depending upon the access method. Scheduling systems accessed by users or administrators via a web interface must comply with all of the requirements for a web server and/or applications server to include DoD access control (e.g., DoD PKI) and auditing requirements for such devices/systems. Scheduling systems accessed via a collaboration tool must minimally utilize the access control required for accessing the collaboration application. Since an authorized user of a collaboration tool may or may not have the right to schedule VTC conferences, the scheduling application should receive user credentials from the collaboration application to determine authorization or the right must be controlled by the collaboration application. Scheduling systems accessed by administrators using other methods must also employ access control and auditing meeting DoD requirements.

**Note:** The general requirement stated below is supported by several DoDI 8500.2 IA controls such as IAIA-1, IAIA-2, and ECPA-1.

**Default Details:** Access control measures have not been implemented to control access to conference scheduling systems to only limited and authorized individuals.

**Pot'l Impacts:** Unregulated access to conference scheduling by any individual who is not authorized can lead to the inadvertent disclosure of sensitive or classified information to individuals that may not have an appropriate need-to-know or proper security clearance or may lead to a denial-of-service for MCU facilities.

**8500.2 IA Cont:** IAIA-1 Identification and Authentication/Individual Identification and Authentication - Sensitive Systems  
IAIA-2 Identification and Authentication/Individual Identification and Authentication - Classified Systems  
ECPA-1 Enclave and Computing Environment/Privileged Account Control - use a role-based access scheme, IAM tracks privileged role assignments.

**Mgmt Category:** 1.1 - I&A – Passwords

**Severity:** CAT II

**Sev. Override:** NONE

**References:** DoD Video Tele-Conference STIG, Section: Section: 8.2.1

**Conditions:** Non-Computing – Video Policy (Target: Video Tele Conference Policy)

**Checks:** RTS-VTC 5140.00 (Interview); [IP][ISDN]; Interview the IAO and validate compliance with the following requirement:  
Ensure access control measures are implemented to control access to conference scheduling systems such that only authorized individuals can schedule conferences.  
**Note:** General compliance with all applicable STIGs was covered earlier in this document.  
Verify that only authorized individuals are permitted to schedule conferences. Inspect VTC scheduling system to verify that only users that are identified by IAO for accessing and setting up scheduled VTC conferences have access to said scheduling function.

**Fixes:** RTS-VTC 5120.00 (Manual); [IP][ISDN]; Perform the following tasks:  
Ensure access control measures are implemented to control access to conference scheduling systems such that only authorized individuals can schedule conferences.

**Responsibility:** IAO, SA,

**Mitigations:** N/A

<b>Not Reviewed:</b> <input type="checkbox"/>	<b>Not Applicable:</b> <input type="checkbox"/>	<b>Not A Finding:</b> <input type="checkbox"/>	<b>Open Finding:</b> <input type="checkbox"/>	<b>Fixed:</b> <input type="checkbox"/>
---	---	--	---	--

**Reviewer Notes and Comments:** (Not Applicable/Reviewed requires a reason.)