



# CHECKLIST FOR INTERNET PROTOCOL TELEPHONY & VOICE OVER INTERNET PROTOCOL STIG

Version 2, Release 2.4

15 August 2008

**Developed by DISA for the DoD**

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

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

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

Final Q/A by: \_\_\_\_\_ Date: \_\_\_\_\_ CAT IV: \_\_\_\_\_

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

UNCLASSIFIED

This page is intentionally left blank.

**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</b>	<b>N</b>	<b>Date of previous SRR</b>		<b>SO1 Available</b>	<b>Y</b>	<b>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 CHANGES

### **15 August 2008 v2r2.4**

Corrected references to outdated versions of the DSN and VoIP STIGs.  
Removed / replaced spurious characters generated by the export from VMS.  
Corrected typographical errors, spelling, and grammar.

### **15 July 2008 v2r2.3**

Generally updated the format and content of each checklist item based on a new VMS VL05 report.

Removed / Deprecated the following STIG IDs due to being superseded by checks in the PC Communications Client STIG and Checklist

VoIP0130; VoIP0135; VoIP0140; VoIP0150; VoIP0160; VoIP0165

This page is intentionally left blank.

## TABLE OF CONTENTS

1.	INTRODUCTION.....	9
1.1	Pre - Requisites .....	9
1.2	RTS 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) .....	11
1.3.3	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.....	12
1.5.1	Computing Asset Creation.....	13
1.6	Creating Assets – Step-by-Step.....	15
1.6.1	Creating the NON-Computing Asset(s).....	15
1.6.2	Creating the Computing Assets .....	17
1.7	Reviewing Assets – Step-by-Step .....	30
1.7.1	First Review of the Asset under VMSv6 .....	30
1.7.2	Procedures for Updating the Vulnerability Status of the Asset .....	32
1.7.3	Verify that all necessary assets were reviewed.....	34
1.7.4	Add Comments to a Visit (Reviewer only).....	34
1.8	Reports – Step-by-Step .....	35
1.8.1	Compliance Monitoring .....	35
1.8.2	Additional Reports .....	36
2.	CHECKLIST ITEMS .....	39

This page is intentionally left blank.

## 1. INTRODUCTION

This document will describe the proper procedure to follow to register and update the IA status of voice and/or video / real time services (RTS) systems and devices in VMSv6. For the purpose of this document, we will use RTS to refer to any voice/video/RTS system or device. This includes all types of telecom switches or video systems, whether they are TDM or IP based, as well as any supporting system or device.

### 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://vmcbt.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://vmcbt.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 RTS 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\_Cisco-VoIP
- Ft.Hood\_MSL100
- LacklandAFB\_MSL100
- Gunter\_CS2100
- Landstuhl\_HiPath4000
- SHAPE\_EWSD
- Pearl\_5ESS

This name represents the Non-Computing Asset for the overall RTS 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\_Cisco-VoIP\_CCM-Registrar\_CCM0001RP
- DISA-SKY7\_Cisco-VoIP\_CCM-Publisher\_CCM0002PP
- DISA-SKY7\_Cisco-VoIP\_CCM-B/URegistrar\_CCM0003RB
- DISA-SKY7\_Cisco-VoIP\_CCM-B/UPublisher\_CCM0004PB
- DISA-SKY7\_Cisco-VoIP\_PSTN-Gateway\_PSTNGW0001
- DISA-SKY7\_Cisco-VoIP\_DSN-Gateway\_DSNGW0001
- DISA-SKY7\_Cisco-VoIP\_LAN-Core\_SKY70001
- DISA-SKY7\_Cisco-VoIP\_ManagementWS\_SKY7MWS0001
- DISA-SKY7\_Cisco-VoIP\_ManagementLS\_SKY7MLS0001

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.

#### **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.

### **1.3.3 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 Asset(s) is(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

‘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 RTS system and/or Adjunct/Auxiliary system NON-Computing Asset.

**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.

#### 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 “RTS Asset Naming Convention” above.
  - o Enter a ‘Description’ of the system.

**Note:** This should reflect a general description of the RTS System and could include the make and version of the LCC 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 ‘Voice/Video/RTS Policy’ (or ‘Telecom Policy’)
- o Check the boxes for appropriate policy/policies as follows:

- Check ‘DRSN Policy’ if the asset is part of, or is connected to, the DRSN.

**Note:** This policy can also apply to other “secure” or classified voice/video/RTS systems.

**OR**

- Check ‘DSN Policy’ if the asset is part of, or is connected to, the DSN.

**Note:** This applies to ALL UN-classified voice/video/RTS systems whether part of the DSN or not. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.

**AND**

- Check ‘VoIP/VoSIP Policy’ if the system being registered provides IP based communications. This includes IP centric systems and IP enabled TDM based systems.

**AND**

- (Conditional) If there is a LAN that only supports the management of the RTS system or an adjunct/auxiliary system to the RTS system AND it is not part of the site LAN/CAN/BAN or the site’s OOB management LAN:

- o Expand ‘Network Policy Requirements’
- o Check ‘Network Infrastructure Policy’

**Note:** If such a LAN is not added here it must be registered separately under both Non-Computing and Computing. Adjunct/auxiliary systems LANs and devices may also be registered separately.

**AND**

- (Conditional) If this LAN has a boundary that touches another LAN, or a local / extended enclave, or a DoD WAN:
  - o Expand ‘Enclave’
  - o Check ‘General Business LAN Enclave’.
- 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-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. (Not available as of 4/7/05 See note below)
    - Click ‘>>’ to move it to the ‘Selected Systems’ window
    - Click ‘Save’ (optional)
  - AND**
    - Find and select ‘ADIMSS’, IF the RTS System is managed or monitored by the ADIMSS (DSN),
  - OR**
    - IF the RTS System is managed or monitored by the ARDIMSS or ESRs (DRSN), Find and select ‘ARDIMSS’ and/or ‘ESRS’
    - Click ‘>>’ to move it to the ‘Selected Systems’ window
    - Click ‘Save’ (optional)
  - 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 ‘Voice/Video/RTS Policy’ postures and program association may be added to an enclave or network non-computing asset instead of creating a separate Voice/Video/RTS 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 register 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 as follows;  
**ELSE** skip to "g)" below
- 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) below:  
**ELSE** skip to i) below:
- 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.
    - 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'
    - Click '>>' to move it to the 'Selected Systems' window
  - 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 to 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.
  - o 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.

## 1.7 Reviewing Assets – Step-by-Step

Note: The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. This will also identify the assets that have been created and can help to eliminate the creation of duplicate assets (i.e., the same asset under different names)

Instructions for generating this report are provided under “Additional Reports” below.

### 1.7.1 First Review of the Asset under VMSv6

When reviewing an asset for the first time under VMSv6 or after initial registration in VMSv6, all asset registration and posture information must be validated. This occurs under the following conditions.

- The asset had been registered in VMSv5.4 and has been brought forward into VMSv6.
  - Additional information as well as the asset postures must be added.
- An SA has initially registered the asset under VMSv6 and a Reviewer will be performing a review on the asset.
  - The reviewer must validate that all information and applicable postures have been properly assigned to the asset. The reviewer must work with the SA to insure proper and complete registration occurs.

#### 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’.**
- vii. *(Reviewer Only)* **Expand ‘Must Review’**  
*SA will not see ‘Must Review’, but will proceed to step viii.*
- viii. **Click the ‘Asset Name’.**
  - Verify data in ‘General’ tab and ‘Asset Identification’.  
For details see Section 1 “Creating the Asset”, steps vii and vii.
- ix. **Click the ‘Asset Posture’ tab** verify the postures/functions assigned to the asset:
  - Expand ‘The Asset Name’ in the ‘Selected ’ window (if it’s there.)
  - Verify that all postures for the asset have been selected and are accurate.
  - IF the asset is not shown in ‘Selected’ box, or the postures are not accurate, see Section 1 “Creating the Asset”, step ix.  
**Note:** Assets registered under VMSv5.4 may have an OS assigned, but the additional postures/functions will have to be assigned.
- x. **Click the ‘Functions’ tab**

- o Verify that all Functions for the asset have been selected and are accurate. See Section 1 “Creating the Asset”, step x. (As of 4/7/06 there are no RTS specific functions. This step may be skipped at this time.)
- xi. **Click the ‘Systems / Enclaves’ tab.**
  - o Verify that the asset has been associated with the appropriate or all applicable program(s), enclave(s), and site(s). See Section 1 “Creating the Asset”, step xi.
- xii. **Click the ‘Additional Details’ tab**
  - o Verify that the information on this tab is accurate. See Section 1 “Creating the Asset”, step xii.
- xiii. If any of the information found is inaccurate, See Section 1 “Creating the Asset” for instructions on making additions or changes.
- xiv. Continue with the following section ‘Procedures for Review of the Asset’ step vii ‘Must Review’

## 1.7.2 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 then work 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 his/her vulnerability statuses, he/she must notify the team lead, 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 then 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, he/she becomes the SA or “owner” for the asset. “Ownership” of assets created by a reviewer must be transferred to the actual SA for the asset.

- 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.*  
**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(s), 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.

### 1.7.3 Verify that all necessary assets were reviewed

*e. 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.

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

*f. 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’**

## 1.8 Reports – Step-by-Step

### 1.8.1 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.
  - g. *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's 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. Has 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'

## 1.8.2 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'

This page is intentionally left blank.

## 2. CHECKLIST ITEMS

**Vulnerability Key:** V0007999  
**STIG ID:** DSN18.14  
**Release Number:** 5  
**Status:** Active  
**Short Name:** Serial Mgmt. Ports do not drop interrupted session  
**Long Name:** Serial management/maintenance ports are not configured to force out or drop any interrupted user session.  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 14.1 Network Management Services (NMS)

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that serial management ports immediately drop any connection that is interrupted for any reason. Reasons include modem power failure, link disconnection, loss of carrier, time-out, etc. Serial ports that are interrupted due to link disconnection, power failure or other reasons will force out the user (i.e., end the session using the port). This will prevent a remote user from ending a session without logging off and leaving the remote maintenance port available with an active session that might allow unauthorized use by someone other than the authenticated user.

**Default Finding Details:** Serial management/maintenance ports are not configured to force out or drop any interrupted user session.

**Potential Impacts:** Denial of Service, degradation of service, loss of confidentiality, system compromise, and/or unauthorized access to network or system resources or services and the information they contain.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-in-Depth:

Information Assurance C-F-2, Para 5, Sec e  
DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

**Checks:**

Interview IAO/ SA - Gen (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable  
Demonstrate Compliance (Manual)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.  
DSN18.14 - Nortel (Manual)  
LOGINCONTROL ALL QUERY. (SET TO DISABLE ON OPEN COND)

**Fixes:**

Ensure session ends on inter (Manual)  
Configure the DSN component to force out users when the session is interrupted.  
Comply with Policy - General (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008222

**STIG ID:** VoIP 0020

**Release Number:** 2

**Status:** Active

**Short Name:** LAN Not Enclave and Network STIG compliant

**Long Name:** The VoIP system is not compliant with overall network security architecture and appropriate enclave security requirements.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE Note: in future this should be a cat1 if stigs not applied, reduced to Cat 2 if applied but there are significant numbers of findings, Cat3 if there are a minimal number of findings.

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is configured to comply with the Network Infrastructure and Enclave STIGs. Network security to include filtering and monitoring are essential elements of a modern VoIP network architecture. This is especially important for voice with the transition from the data network to the VoIP network environment. The two most important forms of protection against unauthorized use of common user communications networks are packet filtering and monitoring. If these do not exist, this would present exposure to new threats, such as communications traffic interception, modification, insertion and denial of service. It is imperative that all measures be taken at the network architectural level to ensure the security of telephony traffic in the IP environment. Guidance for this should be obtained from the Network Infrastructure and Enclave Security STIGs in addition to this STIG.

**Default Finding Details:** The VoIP system is not compliant with overall network security architecture and appropriate enclave security requirements in accordance with the Enclave and Network Infrastructure STIGs.

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Para. 1.0

**Checks:** Review Network & Enclave SRR (Manual)  
Review the results of the most recent Enclave and Network Reviews. If there are a significant number of findings reported or if these STIGs were not applied, this is a finding.

**Fixes:** Perform Enclave and Network Re (Manual)  
Review the VoIP environment using the Network Infrastructure and Enclave STIGs / Checklists. Ensure firewall filtering and intrusion detection monitoring is in place according to guidance.  
Upgrade/configure the LAN (Manual)  
Upgrade the LAN infrastructure as necessary to comply with policy.

---

**Vulnerability Key:** V0008302

**STIG ID:** VoIP 0025

**Release Number:** 1

**Status:** Active

**Short Name:** IPT / VoIP LAN cannot support C2 assured service

**Long Name:** The LAN supporting IPT / VoIP is not designed or implemented as a DOD C2VG LAN in accordance with the DOD GSCR, Appendix 3 and therefore cannot support assured service in support of C2 reliability requirements.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the network supporting IPT implementations (i.e., the underlying data network) is designed and implemented as a DOD C2VG LAN or ASCLAN and will possess bandwidth, reliability, survivability, and prioritization capabilities in accordance with the DOD GSCR, Appendix 3 and/or ASCLAN GSR. Voice services in support of C2 and Special C2 users are required to meet certain minimum requirements relating to reliability and survivability of the supporting infrastructure. Design requirements for networks supporting DOD IPT/VoIP implementations can be found in the DOD Generic Switching Center Requirements (GSCR) document in Appendix 3. This Appendix contains the specifications for a Command and Control Voice Grade LAN (C2VG LAN) required to support DOD IPT. These specifications define LAN design requirements for redundancy of equipment and their interconnections as well as minimum requirements for bandwidth and backup power.

**Default Finding Details:** The LAN supporting IPT / VoIP is not designed or implemented as a DOD C2VG LAN in accordance with the DOD GSCR, Appendix 3 and therefore cannot support assured service in support of C2 reliability requirements. Specific deficiencies found should be noted in the areas of: - Equipment redundancy above the access layer - Connection redundancy above the access layer - Equipment robustness and bandwidth capability - Connection bandwidth capability - Access layer switch size / number of phones served is below maximum -Backup power for all equipment. o Support for C2 users requires 2 hours minimum for all supporting equipment. o Support for Special C2 users requires 8 hours minimum for all supporting equipment.

**Potential Impacts:** Denial of service - A high priority command and control call may not be able to be completed in a timely fashion or at all.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of

site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Review Network Diagrams - C2 (Manual)

Interview the IAO and review site network/facilities diagrams and documentation to confirm compliance.

Specific attention should be given in the areas of:

- Equipment redundancy above the access layer
- Connection redundancy above the access layer
- Equipment robustness and bandwidth capability
- Connection bandwidth capability
- Access layer switch size / number of phones served is below maximum
- Backup power for all equipment.
  - o Support for C2 users requires 2 hours minimum for all supporting equipment.
  - o Support for Special C2 users requires 8 hours minimum for all supporting equipment.

**Fixes:**

Comply with Policy - C2 LAN (Manual)

Upgrade the LAN infrastructure as necessary to meet requirements.

**Vulnerability Key:** V0008223

**STIG ID:** VoIP 0030

**Release Number:** 4

**Status:** Active

**Short Name:** The IPT/ VoIP system not in the site's SSAA

**Long Name:** VoIP devices exist that have not been added to site System Security Authorization Agreements (SSAAs).

**IA Controls:** DCHW-1 HW Baseline

**Categories:** 12.2 SSAA Documentation

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that VoIP devices are added to site System Security Authorization Agreements (SSAAs). Documentation of the enclave configuration must include all VoIP systems. If the current configuration cannot be determined then it is difficult to apply security policies effectively. Security is particularly important for VoIP technologies attached to the enclave network because these systems increase the potential for eavesdropping and other unauthorized access to network resources. Accurate network documentation is critical to maintaining the network and understanding its security posture, threats, and vulnerabilities. An SSAA is the vehicle by which the DAA receives security related information on the network for which he/she is personally responsible and accepts the security risk of operating the system.

**Default Finding Details:** The SSAA does not exist or it is not updated to include the following VoIP system(s) / Devices: An SSAA exists but is not updated to include modifications to the following VoIP systems(s):

**Potential Impacts:** The inability to effectively maintain the network or voice service and apply security policy and vulnerability mitigations. The inability for the DAA to understand the voice system's and/or network's security posture, threats, and vulnerabilities. The inability for the DAA to approve or accept the security risk of operating the system

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Para. 1 DOD 8510.1-M; DITSCAP Application Manual

**Checks:** Review the SSAA (Manual)  
Review the SSAA and verify that all installations or modifications are included. Verify there is a procedure for approving changes to configuration.

**Fixes:** Add all VoIP to the SSAA. (Manual)  
Add all VoIP installations and/or modifications to the SSAA. Obtain DAA approval for the updated SSAA. Submit to the SRR team lead for validation and finding closure.

**Vulnerability Key:** V0008285

**STIG ID:** VoIP 0035

**Release Number:** 1

**Status:** Active

**Short Name:** IPT / VoIP LAN NOT DSN STIG compliant

**Long Name:** The IPT / VoIP system is not compliant with the overall DOD voice system requirements contained in the DSN STIG.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	

<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override Guidance:** NONE

**Vulnerability Discussion:** Requirement: The IAO will ensure that VoIP systems are compliant with the DSN STIG. Specific emphasis to be given in the following areas: - System certification, accreditation, and listing on the DSN APL in accordance with the DODI 8100.3 - Site administrative requirements - Requirements for management of voice systems and management interfaces. - This list is not all-inclusive. Many of the requirements that apply to all voice systems are contained in the DSN STIG. AS such any IPT/ VoIP system must be in compliance with the overall DSN / DOD Voice system requirements.

**Default Finding Details:** The IPT / VoIP system is not compliant with the overall DOD voice system requirements contained in the DSN STIG.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality The DOD voice system may not be protected as required and may be vulnerable to attack.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** DOD Telecommunications and Defense Switched Network (DSN) STIG Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3

**Checks:** Review DSN SRR results (Manual)  
Review the results of the most recent DSN SRR or Self Assessment. If there are a significant number of findings reported or if the DSN STIG was not applied, this is a finding.

**Fixes:** Perform a DSN review (Manual)  
Review the VoIP environment using the DSN STIG / Checklist for compliance. Ensure firewall filtering and intrusion detection monitoring is in place according to guidance. Upgrade the LAN as necessary to meet requirements.

---

**Vulnerability Key:** V0008224

**STIG ID:** VoIP 0040  
**Release Number:** 2  
**Status:** Active  
**Short Name:** MGCP is being used without IPSEC  
**Long Name:** MGCP is being used without IPSEC enabled on each the MGCs to provide authentication and encryption.  
**IA Controls:** ECCT-1 Encryption for Confidentiality (Data in Transit)  
 ECNK-1 Encryption for Need-To-Know  
 ECSC-1 Security Configuration Compliance  
**Categories:** 8.1 Encrypted Data in Transit

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: If MGCP is used, the IAO will ensure that IPSEC is enabled on each of the MGCs to provide authentication and encryption. Media Gateway Control Protocol (MGCP) is a protocol that is used between Media Gateways to exchange sensitive gateway status and zone information. MGCP is a clear text protocol. This information is critical in the setup and completion of voice calls from VoIP zone to VoIP zone. If this information is poisoned or if collected and used by an unauthorized unscrupulous individual, the effects to the VoIP environment could be detrimental. In addition, (RFC) 2705 (MGCP) outlines and recommends the use of IPSEC for encryption and authentication between gateways. Since this feature is inherent to the protocol, good security practice dictates its use.

**Default Finding Details:** The Media Gateway Control Protocol (MGCP) is being used between Media Gateways without IPSEC enabled on the following gateways:

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.12

**Checks:** IAO/SA demonstrate IPSEC on M (Manual)  
Inspect, or have site personnel demonstrate compliance on, a sampling of effected devices to confirm compliance. Request the SA demonstrate that IPSEC is enabled for MGCP signaling on Media Gateways, Media Gateway Controllers, and other devices such as end instruments if they use MGCP, by providing configuration details.

**Fixes:** Enable IPSEC for MGCP (Manual)  
Enable IPSEC for MGCP signaling on Media Gateways, Media Gateway Controllers, and other devices such as end instruments that use the Media Gateway Control Protocol.

**Vulnerability Key:** V0008225

**STIG ID:** VoIP 0050

**Release Number:** 2

**Status:** Active

**Short Name:** Improper Physical security - System access

**Long Name:** Critical VoIP network and server components are NOT located in secured areas.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 5.9 Device Locations

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure all critical VoIP network and server components are located in a secured area. This does not apply to end instruments. Controlling physical access to the VoIP network and server components is critical to assuring the reliability of the voice network and service delivery. Documenting or logging physical access to the VoIP network and server components is critical to determine

accountability for auditing purposes.

**Default Finding Details:** The following VoIP components are installed in an area that does not have adequate physical security controls applied: List components and locations that are not physically secure (except end instruments): VoIP system servers and/or network components are installed in a locked room, closet, or cabinet, but the distribution of keys to access the equipment is NOT limited, controlled, or documented. A physical access log is not maintained.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Physical access to systems by unauthorized personnel leaves the system components vulnerable to a multitude of attack vectors and/or accidental de-activation or disconnection.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.2

**Checks:** Confirm physical security (Manual)  
During a walk through inspection, visually confirm that VoIP network and server components are installed in secured areas to include locked rooms, closets, and/or cabinets. Interview the IAO to determine how the distribution of keys to access the equipment is limited, controlled, and documented. Additionally determine if access control procedures/documentation are/is being used and review the access logs for compliance.

**Fixes:** Establish Physical Security (Manual)  
The IAO must ensure that all equipment is installed in a locked room, closet, or cabinet. Additionally the IAO must insure that the distribution of keys to access the equipment is limited, controlled, and documented. Additionally, access control procedures should be implemented to insure that physical access is documented so that an audit trail can be established if necessary.

---

**Vulnerability Key:** V0008226

**STIG ID:** VoIP 0060

**Release Number:** 2

**Status:** Active

**Short Name:** Network configuration is displayed on IP phones

**Long Name:** IP phones are configured to display network IP configuration information without the use of a password.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that IPT terminals (VoIP phones or instruments) cannot be configured at the terminal and do not display network/terminal configuration information on their display without the use of a password. Some IP phones display VoIP network information making it easy to collect VoIP network information that could be used by would be hackers / attackers. Therefore these devices should be considered a target to be defended against such individuals that would collect voice network information for illicit purposes. To help prevent against information gathering by the unscrupulous, measures must be taken to protect this information. Programming IP Phones not to display Network information (i.e. IP address, subnet mask, gateway, LCC addresses or URLs, etc.), without entering a password or PIN code, should be considered another layer of security in protecting the VoIP environment.

**Default Finding Details:** IP phones display VoIP network information (i.e. IP address, subnet mask, gateway, LCC addresses or URLs, etc.) without the entry of a password or PIN code.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. System or server attack based on information gathered from end instruments.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.3

**Checks:** Demonstrate Compliance (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Fixes:** Properly configure IP Phones (Manual)  
Configure IP Phones to NOT display voice network information without the entry of a password or a PIN code.

**Vulnerability Key:** V0008287

**STIG ID:** VoIP 0061

**Release Number:** 1

**Status:** Active  
**Short Name:** Phone passwords/PINs do not remote authenticate  
**Long Name:** The IPT terminal's configuration/configuration-display passwords/PINs DO NOT authenticate remotely to the IPT system controller (Local Call Controller (LCC)).  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the IPT terminal's configuration/configuration-display passwords authenticate remotely to the IPT system controller (Local Call Controller (LCC)). Passwords or PIN codes used to access an IPT / VoIP terminals or end instruments configuration menu or display should not be stored on the terminal or end instrument. They should be stored on the system controller. The terminal or end instrument should query the system controller for password or PIN code authentication. In this way, passwords and PIN codes can be managed and changed as necessary to comply with password management policy.

**Default Finding Details:** The IPT terminal's configuration/configuration-display passwords DO NOT authenticate remotely to the IPT system controller(Local Call Controller (LCC)).

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Password or PIN code compromise. As compromise is easier or more likely if they are not centrally managed since Password or PIN codes stored on the terminals or end instruments will most likely never be changed.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.3

**Checks:** Demonstrate Compliance (Interview)  
 Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Fixes:** Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.  
Configure the system for comp (Manual)  
Configure the system for compliance if the feature is available. Vendors should provide this capability in their systems

**Vulnerability Key:** V0008288  
**STIG ID:** VoIP 0062  
**Release Number:** 1  
**Status:** Active  
**Short Name:** There is NO IPT / VoIP terminal PIN policy  
**Long Name:** There is NO IPT / VoIP terminal password/PIN management policy.  
**IA Controls:** ECSC-1 Security Configuration Compliance  
IAIA-1 Individual Identification and Authentication  
IAIA-2 Individual Identification and Authentication  
**Categories:** 1.1 Passwords

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that a policy is in place to ensure that the IPT terminal (VoIP phone or instrument) configuration and display password is managed IAW DOD password policies (e.g., password complexity, expiration, reuse, protection and storage). PINs that are not managed or required to be changed are most likely never changed, therefore they are easily compromised or guessed.

**Default Finding Details:** A policy is NOT in place to ensure that the IPT terminal (VoIP phone or instrument) configuration and display password is managed IAW DOD password policies (e.g.,

password complexity, expiration, reuse, protection and storage).

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Password or PIN code compromise. As compromise is easier or more likely if PINs are not managed.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.3

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008289

**STIG ID:** VoIP 0065

**Release Number:** 2

**Status:** Active

**Short Name:** Auto-reg. of VoIP terminals NOT disabled

**Long Name:** Auto-registration of VoIP terminals is NOT disabled.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 2.1 Object Permissions

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity:** NONE

**Override**

**Guidance:**

**Vulnerability**

**Discussion:**

Requirement: The IAO will ensure that auto-registration of VoIP terminals is disabled within 5 days following initial system setup and/or following any subsequent large redeployments or additions. The Auto-registration feature provided in some IPT / VoIP systems presents various issues. In general this feature allows any end instrument to function using a default configuration as soon as it is plugged into the network without prior authorization and configuration by an SA. In general this feature should never be used even in the limited situations mentioned in the requirement since the SA loses control of the system. In this situation the SA may not know what phones are on the system or where they are and since phone numbers are usually assigned out of a pool, there is no SA control over number assignments. Additionally since end instruments can work as soon as plugged in, they could be used to abuse the phone system.

**Default Finding Details:**

Auto-registration of IPT / VoIP terminals is NOT disabled during normal system operation.

**Potential Impacts:**

Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Loss of management control of the system and potential system abuse.

**Responsibility:**

Information Assurance Officer

**Mitigations:**

**References:**

Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.4

**Checks:**

Demonstrate Compliance (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:**

Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008290

**STIG ID:** VoIP 0066

**Release Number:** 1

**Status:** Active

**Short Name:** NO Inventory of authorized instruments

**Long Name:** An inventory of authorized instruments is NOT documented or maintained.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 2.1 Object Permissions

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	

<input type="checkbox"/> Not Reviewed	
---------------------------------------	--

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that an inventory of authorized instruments is documented and maintained. It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

**Default Finding Details:** An inventory of authorized instruments is NOT documented or maintained.

**Potential Impacts:** Unauthorized use or abuse of the system

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.4

**Checks:** Inspect/Review Documents (Interview)  
Inspect or review the required documents on file that are necessary for compliance with the requirement.  
Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008291

**STIG ID:** VoIP 0067

**Release Number:** 1

**Status:** Active

**Short Name:** UN-authorized terminals are registered  
**Long Name:** UN-authorized VoIP terminals are registered With the LCC and are operational  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 2.1 Object Permissions

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the VoIP system only registers authorized terminals. This can be through an automated authorization process during auto-registration or by comparing the registration logs to the documented authorized inventory following any usage of auto-registration. It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

**Default Finding Details:** Unauthorized IPT / VoIP terminals or end instruments are registered with the LCC and in use on the IPT / VoIP system.

**Potential Impacts:** Unauthorized use or abuse of the system

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.4

**Checks:** Demonstrate Compliance (Interview)  
 Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.  
 Review current configuration (Manual)  
 Review current configuration files of effected devices to confirm compliance.  
 Perform a walk-through (Manual)

Perform a walk through of the facility to confirm compliance via inspection of the effected devices or items

**Fixes:**

- Comply with Policy (Manual)
- Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.
- Remove unauthorized phones (Manual)
- Remove unauthorized terminals, phones, endpoints etc from the VoIP network.

**Vulnerability Key:** V0008293

**STIG ID:** VoIP 0068

**Release Number:** 2

**Status:** Active

**Short Name:** Manual registration of VoIP terminals NOT used

**Long Name:** Manual registration of VoIP terminals is not being used for normal operations

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 2.1 Object Permissions

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that manual registration of VoIP terminals is used for normal, day-to-day, troubleshooting and repairs, or moves, adds, and changes. It is critical to the security of the system that all IPT /VoIP end instruments be authorized to connect to and use the system. Only authorized instruments should be configured in the system controller and therefore allowed to operate. Unauthorized instruments could lead to system abuse.

**Default Finding** Manual registration of VoIP terminals is NOT being used for normal, day-to-day,

**Details:** troubleshooting and repairs, or moves, adds, and changes.

**Potential Impacts:** Unauthorized use or abuse of the system

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.4

**Checks:**  
 Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Demonstrate Compliance (Interview)  
 Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Fixes:**  
 Comply with Policy (Manual)  
 Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
 Configure for manual registration (Manual)  
 Configure the LCC for manual registration.

**Vulnerability Key:** V0008227

**STIG ID:** VoIP 0070

**Release Number:** 2

**Status:** Active

**Short Name:** VoIP system is not addressed differently than data

**Long Name:** VoIP systems and components are not deployed on a logically segregated Subnet with different IP addressing from the data network.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.5 Physical Layer Security

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality**

	<b>I - Mission Critical</b>	<b>II - Mission Support</b>	<b>III - Administrative</b>
--	-----------------------------	-----------------------------	-----------------------------

<b>Grid:</b>	<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all VoIP systems and components are deployed on their own dedicated IP network(s) or sub-network(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs. The combination of logical data and voice segmentation via addressing and VLANs coupled with a switched and routed infrastructure strongly mitigates call eavesdropping and other attacks. In addition, limiting logical access to VoIP components is necessary for protecting telephony applications running across the infrastructure. Segregating data from telephony by placing VoIP servers and subscriber terminals on logically separate IP networks while controlling access to these VoIP components through IP filters will help to ensure security and aid in protecting the VoIP environment.

**Default Finding Details:** VoIP systems and components are not deployed on a logically segregated and dedicated telephony network.

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Demonstrate Compliance (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Fixes:** Segregate VoIP systems (Manual)  
Implement VoIP systems and components on a logically segregated and dedicated telephony (VoIP) network.

**Vulnerability Key:** V0008228

**STIG ID:** VoIP 0080

**Release Number:** 3

**Status:** Active

**Short Name:** VoIP system does not use RFC 1918 addressing

**Long Name:** VoIP systems are not deployed on a "private" (non WAN routed) network in accordance with Request for Comments (RFC) 1918.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override Guidance:** This check does not apply to VoIP systems residing on the SIPRNet; therefore this is not a finding under the specified condition.

**Vulnerability Discussion:** Requirement: The IAO will ensure that all local VoIP systems and components are deployed using "private" (non WAN routed) IP address space IAW RFC 1918. Note: This check does not apply to VoIP systems residing on the SIPRNet (i.e., VoSIP) and other closed globally addressed networks where it is the policy of the Program Manager to require individual "public" addresses to be individually assigned to each device connected to the network for the purpose of traceability and accountability. Therefore this is not a finding under these specific conditions. The use of the term "private" (non WAN routed) IP addresses in this sense means that the addresses are not routed or advertised across the internet by international agreement. NIPRNet also follows this policy. RFC 1918 addresses are routable within the LAN enclave. Deploying VoIP Systems on such an address space enhances security of the VoIP environment by denying access from outside routable addresses, thus effectively hiding the voice network. If VoIP systems are not deployed on "private" address space and if the address space is not properly configured, managed, and controlled, the VoIP network could be accessed by unauthorized personnel resulting in security compromise of site information and resources.

**Default Finding Details:** VoIP systems are not deployed on non-routable (RFC 1918) network address space. VoIP systems are not deployed on "private" (non WAN routed) IP address space IAW RFC 1918. This finding is NA if the VoIP system resides on the SIPRNet (i.e., VoSIP) and/or other closed globally addressed networks where it is the policy of the Program Manager to require individual "public" addresses to be individually assigned to each device connected to the network for the purpose of traceability and accountability.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. The IPT / VoIP infrastructure would not be hidden and therefore would be easier to attack

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.1

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Demonstrate Compliance (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Implement RFC 1918 addressing (Manual)  
Use RFC 1918 addressing for all voice components. Monitor and control the use of this address space.

**Vulnerability Key:** V0008294

**STIG ID:** VoIP 0082

**Release Number:** 2

**Status:** Active

**Short Name:** VoIP DHCP server NOT Dedicated

**Long Name:** A DHCP server used for IPT / VoIP terminal IP address assignment, is not dedicated to the IPT / VoIP system

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity:** NONE

**Override**

**Guidance:**

**Vulnerability**

**Discussion:**

Requirement: The IAO will ensure that when using DHCP for address assignment, different servers are used for voice components and data components. Additionally, the IAO will ensure that these servers will reside in their respective voice or data address space. When using Dynamic Host Configuration Protocol (DHCP) for address assignment, different servers will be used for voice components and data components. That is to say that a DHCP server serving VoIP devices needs to be in the VoIP domain i.e., same address space. This alleviates the need to route DHCP requests into the data environment on the LAN. The best practice is to manually assign addresses when authorizing the instrument by generating its configuration file.

**Default Finding Details:**

The IPT / VoIP system uses a DHCP server that is not dedicated to the IPT / VoIP system.

**Potential Impacts:**

Loss of reliability; Possible assignment of IP addresses that are not dedicated to the IPT / VoIP system; Degradation of the data and VoIP network segregation.

**Responsibility:**

Information Assurance Officer

**Mitigations:**

**References:**

Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.1

**Checks:**

Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:**

Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
Dedicate a VoIP DHCP Server (Manual)  
If DHCP is used to initialize VoIP phones, Implement a dedicated DHCP server or manually assign addresses when authorizing the instrument by generating its configuration file.

---

**Vulnerability Key:** V0008295

**STIG ID:** VoIP 0085

**Release Number:** 1

**Status:** Active

**Short Name:** VoSIP on SIPRNet NOT properly addressed

**Long Name:** VoSIP systems and components residing on the SIPRNet ARE NOT utilizing address blocks assigned by the DRSN VoSIP PMO.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open	Comments:
-------------------------------	-----------

<input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	
--	--

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all VoSIP systems and components residing on the SIPRNet utilize address blocks assigned by the DRSN VoSIP PMO. IP addresses that are used by IPT / VoIP systems that are part of the VoSIP system using the SIPRNet as the VoSIP WAN, must be assigned from the pool of SIPRNet addresses that is maintained by the DRSN VoSIP PMO. This is to maintain the segregation of the Voice and data environments on the SIPRNet as required by this STIG. This also facilitates proper routing and flow control over the traffic between VoSIP addresses.

**Default Finding Details:** VoSIP systems and components residing on the SIPRNet ARE NOT utilizing address blocks assigned by the DRSN VoSIP PMO.

**Potential Impacts:** Denial of service; Lack of interoperability with other VoSIP enclaves.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.1

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Review current configuration (Manual)  
   Review current configuration files of effected devices to confirm compliance.  
 Review VoSIP address assignment (Manual)  
   Review address assignment documentation provided by the DRSN PMO- VoSIP department

**Fixes:** Comply with Policy (Manual)  
 Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
 Obtain & use VoSIP addresses (Manual)  
 Obtain and assign IP addresses as provided by the DRSN PMO- VoSIP department

**Vulnerability Key:** V0008350  
**STIG ID:** VoIP 0090  
**Release Number:** 1  
**Status:** Active  
**Short Name:** NO firewall between voice and data VLANs & LCC  
**Long Name:** A stateful inspection firewall is not used between the voice and data VLANs and between the voice VLANs and the VoIP core control equipment on the network to protect VoIP system and communications.  
**IA Controls:** DCPA-1 Partitioning the Application  
 ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that voice or data traffic between the data and voice VLANs and between the voice VLANs and the VoIP core control equipment is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned and approved traffic between authorized devices using approved ports, protocols, and services. Firewalls, routers, and switches must be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control (i.e., block) access from the data network to the IP telephony network. Such traffic must be blocked if there is no compelling need for it. Systems or devices that must be accessed from both the data and voice VLANs must be placed in a VLAN separate from both so that traffic to and from this VLAN is controlled

and that there is no direct traffic between the voice and data VLANs. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. This firewall must control all traffic between the various VLANS discussed here.. This will mitigate possible malicious attacks that may originate from within the data network. At minimum IP filtering must be implemented between the IP telephony network and the IP data network.

**Default Finding Details:** A stateful inspection firewall is not used between the voice and data VLANs and between the voice VLANs and the VoIP core control equipment on the network to protect VoIP system and communications.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Locate/inspect the VoIP firewall (Manual)  
Locate the firewall used to protect the VoIP system / portion of the network. Review current configuration files to confirm compliance.

**Fixes:** Implement proper VoIP firewall (Manual)  
Implement a stateful inspection firewall between the IP telephony (VoIP) network and the IP data network. Additionally control traffic to and from the voip phone VLANs and the VoIP core equipment. (i.e., LCC, media gateways, messaging systems, etc).

**Vulnerability Key:** V0008328

**STIG ID:** VoIP 0095

**Release Number:** 2

**Status:** Active

**Short Name:** The Data Enclave Perimeter does not block VoIP

**Long Name:** The data network perimeter protection is NOT configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and VLANs

**IA Controls:** EBBD-1 Boundary Defense  
EBBD-2 Boundary Defense  
EBBD-3 Boundary Defense  
ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	Comments:
--	-----------

<input type="checkbox"/> Not Reviewed	
---------------------------------------	--

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the Data network perimeter protection (i.e., Data premise router, Data perimeter firewall) is configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and/or fulfill one or more of the traffic control requirements noted above under VLAN traffic control. Enclave boundary Firewalls and premise routers should be implemented in a manner that will protect the VoIP servers, VLANs, and communications from unauthorized access. This is necessary to limit and control access from the data network and from influences from outside the enclave to the IP telephony network. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. At minimum IP filtering should be implemented between the IP telephony network and the WAN as well as the IP data network. This will mitigate possible malicious attacks that may originate from within the data network. Additionally, this will force any approved WAN VoIP traffic to go through the VoIP firewall structure.

**Default Finding Details:** The data network perimeter protection is NOT configured to block all traffic destined to or sourced from the Voice VLAN IP Address space and VLANs

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Block VoIP at data firewall (Manual)  
Configure the enclave perimeter premise router and data firewall to block all traffic to and from the Voice VLANs and IP Address space. Additionally configure the Premise router to route approved VoIP traffic from the WAN to the VoIP firewall.

**Vulnerability Key:** V0008230  
**STIG ID:** VoIP 0100  
**Release Number:** 2  
**Status:** Active  
**Short Name:** VoIP system is not in its own VLAN(s)  
**Long Name:** VoIP systems do not reside on dedicated and separate VLAN(s) from the data network.  
**IA Controls:** DCPA-1 Partitioning the Application  
 ECSC-1 Security Configuration Compliance  
**Categories:** 14.5 Physical Layer Security

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override Guidance:**

This may not be a finding under certain circumstances such as in the case of a small footprint tactical system where there is a limited number of VoIP instruments (i.e., 20). This package system must have been accredited via the appropriate test exercises and configured in accordance with the accreditation. This override is partially driven by the difficulty in supporting a complex configuration for these small systems in deployed environments. This Severity Override does not apply to strategic systems. (i.e., systems implemented on a base or fixed DOD facility)

**Vulnerability Discussion:**

Requirement: The IAO will ensure that the local network supporting IPT implementations (i.e., the underlying data network) is configured using VLANs, and that at a minimum, one voice VLAN has been configured to segregate voice traffic from data traffic. The implementation of VLAN technology serves to mitigate the risk that a DoS attack or packet sniffing, sourced from the data network. Will affect the voice network and vice versa. In addition, placing voice and data traffic into separate VLANs will reduce competition for the network and thus reduce latency (queue/wait time) for transmission services, which will reduce the possibility of denial of voice services. This also reduces the Ethernet broadcast domain thereby reducing network overhead. Since VoIP is very latency sensitive this segmentation approach is the most economical way to improve performance in an existing network infrastructure.

**Default Finding Details:**

VoIP systems and devices do not reside on at least one dedicated, VLAN that is separate from the data network.

**Potential**

Denial of Service, loss of confidentiality, and/or unauthorized access to network or

**Impacts:** voice system resources or services and the information they contain. The IPT / VoIP infrastructure would not be hidden and therefore would be easier to attack from the data network. Voice performance may also be degraded.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:**  
 Interview the IAO or SA (Interview)  
 Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
 Demonstrate Compliance (Interview)  
 Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.  
 Review current configuration (Manual)  
 Review current configuration files of effected devices to confirm compliance.

**Fixes:**  
 Segregate VoIP systems (Manual)  
 Deploy VoIP systems and components on a dedicated VLAN structure that is separate from the data network VLAN structure. A minimum of one VLAN is required. More than one is highly recommended.

**Vulnerability Key:** V0008296

**STIG ID:** VoIP 0101

**Release Number:** 1

**Status:** Active

**Short Name:** Multiple IPT / VoIP VLANs not implemented

**Long Name:** Multiple IPT / VoIP VLANs are not implemented

**IA Controls:** DCPA-1 Partitioning the Application  
 ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓

<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the voice network is subdivided into multiple VLANs to segregate VoIP devices by type and function. At a minimum, this shall include five VLANs containing the following as might be applicable: call control servers, message servers (voice-mail, e-mail, unified), gateways, VoIP phones, and workstations with soft phones. Suggested VLANs - Call processing and voice DHCP servers - Directory servers - Message servers and/or servers that might be accessed from both the data network and the VoIP network. - Gateways possibly multiple VLANs for multiple types of gateways - WAN Access firewalls

**Default Finding Details:** Multiple IPT / VoIP VLANs have not been implemented to further segregate and protect the IPT / VoIP system from the data environment.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Critical IPT / VoIP support infrastructure would not be sufficiently hidden and protected therefore making it easier to attack.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
Implement multiple VoIP VLANs (Manual)  
Implement a multiple VLAN IPT / VoIP environment. Upgrade the network to support this if necessary.

---

**Vulnerability Key:** V0008335  
**STIG ID:** VoIP 0102  
**Release Number:** 1  
**Status:** Active  
**Short Name:** NO VLANs for Mutually accessible systems  
**Long Name:** Message servers or workstations with soft phones have not been placed in their own VLAN(s)  
**IA Controls:** DCPA-1 Partitioning the Application

ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that servers or devices that are to be accessed from both the voice and data networks (i.e., message servers or workstations with soft phones) reside in their own protected VLANs. Mutually accessible servers may be placed in the DMZ of a dedicated stateful firewall placed between the voice and data networks per voice/data network protection requirements. This practice enhances the segregation between the IPT / VoIP and data portions of the LAN by requiring that the traffic into and out of this VLAN be controlled by a layer 3 device that would not allow direct traffic across this VLAN between the IPT / VoIP and data portions of the LAN.

**Default Finding Details:** The following message servers or workstations with soft phones have not been placed in their own VLAN(s)

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation and associated problems

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Review current configuration (Manual)  
 Review current configuration files of effected devices to confirm compliance.

**Fixes:** Comply with Policy (Manual)  
 Implement processes / procedures, generate documents, and/or adjust

configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008304  
**STIG ID:** VoIP 0103  
**Release Number:** 1  
**Status:** Active  
**Short Name:** VLANs not Network STIG compliant  
**Long Name:** The IPT / VoIP VLANs are NOT configured according to the Network Infrastructure STIG.  
**IA Controls:** DCPA-1 Partitioning the Application  
 ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the local network's VLANs are implemented in accordance with the VLAN section of the Network Infrastructure STIG. See the Network Infrastructure STIG & Checklist for a discussion of the associated vulnerabilities.

**Default Finding Details:** The IPT / VoIP VLANs are NOT configured according to the Network Infrastructure STIG.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Degradation of the data and VoIP network segregation and associated problems. Additionally, see the Network Infrastructure STIG & Checklist for a discussion of the associated vulnerabilities.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG SECTION 3.5.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review DSN SRR results (Manual)  
Review the results of the most recent DSN SRR or Self Assessment. If there are a significant number of findings reported or if the DSN STIG was not applied, this is a finding.  
Review current configurations (Manual)  
Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

**Fixes:** Upgrade/configure the LAN (Manual)  
Upgrade the LAN infrastructure as necessary to comply with policy.  
Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008305

**STIG ID:** VoIP 0105

**Release Number:** 1

**Status:** Active

**Short Name:** Devices NOT connected to proper VLAN

**Long Name:** IPT / VoIP instruments and/or data workstations are NOT connected to the VLANs that are designated for their use.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality**

	I - Mission Critical	II - Mission Support	III - Administrative
--	----------------------	----------------------	----------------------

<b>Grid:</b>	<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that IP phones (that do not contain a multi-port switch), and servers providing voice services are connected to switch-ports with membership only to the voice VLAN(s). Additionally, the IAO will ensure that data workstations (without approved Soft Phones) are connected to switch-ports with membership only to the data VLAN(s). These devices are to be connected to the VLANs that have been configured for their proper traffic control and protection of the Voice network.

**Default Finding Details:** IPT / VoIP instruments and/or data workstations are NOT connected to the VLANs that are designated for their use.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Degradation of the data and VoIP network segregation and associated problems.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.  
Inspect effected devices (Manual)  
Inspect a sampling of effected devices to confirm compliance. Review device connections and port connections to determine if they are properly connected.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
Comply with Policy - VLAN ass (Manual)  
Connect data devices such as workstations to the data VLANs only. Connect voice devices such as IPT/VoIP phones, media gateways, and LCCs to the appropriate Voice VLANs only.

**Vulnerability Key:** V0008306

**STIG ID:** VoIP 0110

**Release Number:** 1  
**Status:** Active  
**Short Name:** IP Phone switches NOT disabled or NOT using 802.1Q  
**Long Name:** IP phones containing a multi-port switch do NOT utilize 802.1Q VLAN tagging and/or the PC port is not disabled.  
**IA Controls:** DCPA-1 Partitioning the Application  
 ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all IP phones containing a multi-port switch for connecting external devices such as a workstation, utilize 802.1Q trunking to separate voice and data traffic or have the data port(s) disabled. Some IPT/VoIP instruments contain a multi-port switch for connecting external devices such as a workstation (i.e., PC port). These multi-port switches must be capable of supporting 802.1Q tagging for VLAN separation. If they do not, this will mix the voice and data networks if used. Requirement: The IAO will ensure that all IP Phones and Soft Phones are: - VLAN capable and that this function is enabled - Assigned to the VoIP VLAN segment. Many IP hardware phones provide a separate data port for the connection of a PC to the phone so that only a single cable is required to provide data and voice connectivity to the end users desktop. Additionally, some IP hardware phones are only capable of providing basic layer 2 connectivity, acting like a hub and combining the data and voice network segments. While other IP phones offer enhanced Layer 2 connectivity providing the option to use VLAN technology, to place the phone and the data traffic on two different VLANs. To ensure logical separation of voice and data in order to maintain the security of the VoIP environment, only layer 2 enhanced or VLAN capable phones should be considered for use.

**Default Finding Details:** The following IP phones that contain a multi-port switch do NOT utilize 802.1Q VLAN tagging and/or the PC port is not disabled: The following IP Phones that contain a multi-port switch are being used that are not VLAN capable and/or VoIP traffic is not assigned to a VoIP VLAN segment and/or the PC port is not assigned to a data VLAN:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Degradation of the data and VoIP network segregation and associated problems.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:**  
Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:**  
Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008307

**STIG ID:** VoIP 0111

**Release Number:** 1

**Status:** Active

**Short Name:** Access switches do not separate voice and data.

**Long Name:** Access layer switch ports do not separate voice and data onto the appropriate voice and data VLANs that arrives from IP phones that contain a multi-port switch

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	-------------------------------------	-------------------------------------	-------------------------------------

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all access switch ports supporting IP phones that contain a multi-port switch route voice and data traffic to their respective VLANs. Some IPT/VoIP instruments contain a multi-port switch for connecting external devices such as a workstation (i.e., PC port). These multi-port switches must be capable of supporting 802.1Q tagging for VLAN separation and the voice and data traffic must be tagged appropriately. If this feature is not supported, the access layer switch must detect the traffic types and rout the packets to the proper VLAN.

**Default Finding Details:** Voice and data traffic from IP phones that contain a multi-port switch is NOT routed to the proper voice and data VLAN by access layer switches. The following network access layer switches do not maintain voice and data VLAN separation:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Degradation of the data and VoIP network segregation and associated problems.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008323

**STIG ID:** VoIP 0115

**Release Number:** 2

**Status:** Active

**Short Name:** IP filters between Voice and Data VLANs NOT used

**Long Name:** IP filters have NOT been implemented between Voice and Data VLANs to control traffic such that it is restricted to planned traffic between authorized devices using approved ports, protocols, and services.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that traffic between all voice VLANs is filtered and controlled by a layer-3 switch/router ACL or a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services. Firewalls, routers, and switches must be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control (i.e., block) access from the data network to the IP telephony network. Such traffic must be blocked if there is no compelling need for it. Systems or devices that must be accessed from both the data and voice VLANs must be placed in a VLAN separate from both so that traffic to and from this VLAN is controlled and that there is no direct traffic between the voice and data VLANs. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. This firewall must control all traffic between the various VLANS discussed here.. This will mitigate possible malicious attacks that may originate from within the data network. At minimum IP filtering must be implemented between the IP telephony network and the IP data network

**Default Finding Details:** P filters have NOT been implemented between Voice and Data VLANs to control traffic such that it is restricted to planned traffic between authorized devices using approved ports, protocols, and services.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Possible degradation of the data and VoIP network segregation.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.1

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Review current configuration (Manual)

Review current configuration files of effected devices to confirm compliance.

**Fixes:** Implement Data-VoIP VLAN IP f (Manual)  
Implement a stateful inspection firewall or router ACLs between the IP telephony (VoIP) network and the IP data network. Additionally control traffic to and from the VoIP phone VLANs and the VoIP core equipment. (i.e., LCC, media gateways, messaging systems, etc).

**Vulnerability Key:** V0008325

**STIG ID:** VoIP 0116

**Release Number:** 1

**Status:** Active

**Short Name:** Mutually accessible VLANs are not IP filtered

**Long Name:** Traffic between the VLAN containing mutually accessible servers or devices (such as softphones) to and from the voice VLAN(s) or the data VLAN(s) is NOT filtered and controlled by a stateful inspection firewall.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that traffic between the VLAN containing mutually accessible servers or devices (such as softphones) to and from the voice VLAN(s) or the data VLAN(s) is filtered and controlled by a stateful inspection firewall, such that traffic is restricted to planned traffic between authorized devices using approved ports, protocols, and services. This firewall will block traffic between the voice and data VLANs or fulfill one or more of the traffic control requirements noted above.

Firewalls, routers, and switches should be implemented in a manner that will compartmentalize VoIP servers and communications from unauthorized access. This is necessary to limit and control access from the data network to the IP telephony network. Firewall controls are to be placed in front of all networks and components supporting VoIP servers. At minimum IP filtering should be implemented between the IP telephony network and the IP data network. This will mitigate possible malicious attacks that may originate from within the data network.

**Default Finding Details:** Traffic between the VLAN containing mutually accessible servers or devices (such as softphones) to and from the voice VLAN(s) or the data VLAN(s) is NOT filtered and controlled by a stateful inspection firewall.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Possibly degradation of the data and VoIP network segregation.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.1

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configurations (Manual)  
Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

**Fixes:** Implement IP filtering (Manual)  
Implement IP filtering between the IP telephony (VoIP) network and the IP data network as well as to and from a VLAN housing mutually accessible systems or devices.

**Vulnerability Key:** V0008351

**STIG ID:** VoIP 0120

**Release Number:** 1

**Status:** Active

**Short Name:** Unused voice VLAN ports are not disabled.

**Long Name:** Unused physical ports assigned to the voice VLAN are not disabled in access layer network switches.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.5 Physical Layer Security

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override**

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all unused ports are disabled and are placed in an unused VLAN. Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that any unused physical access layer switch ports that could be assigned to the voice VLAN are disabled. If unauthorized personnel gains access to a VLAN through an unsecured physical switch port, they could cause disruptions, denial of service conditions, or access sensitive information. Disabling inactive or unused ports and assigning them to an unused VLAN prevents this type of unauthorized and unwanted activity.

**Default Finding Details:** The following unused voice VLAN ports are not disabled:

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Numerous potential impacts are made available by vulnerabilities associated with unauthorized access to the network.

**Responsibility:** System Administrator

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.2

**Checks:**  
 Review switch configuration (Manual)  
 Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing switch/router configuration files, that unused ports are disabled. Site personnel provide these files.  
 Inspect effected devices (Manual)  
 Inspect a sampling of effected devices to confirm compliance. Plug a laptop or other Ethernet device into unused switch ports and see if link lights on both devices light indicating an active port.

**Fixes:**  
 Disable unused VoIP ports (Manual)  
 Disable all unused physical network access ports or interfaces and assign them to an unused VLAN.

**Vulnerability Key:** V0008232

**STIG ID:** VoIP 0122

**Release Number:** 3

**Status:** Active  
**Short Name:** Unused data ports on IP phones are not disabled  
**Long Name:** Data ports on IP phones are not being disabled or controlled as required.  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all IP phones with a multi-port switch have the data port disabled if a PC is not normally attached. Many IP hardware phones provide a separate data port for the connection of a PC to the phone so that only a single cable is required to provide data and voice connectivity to the end users desktop. Additionally, some IP hardware phones are only capable of providing basic layer 2 connectivity, acting like a hub and combining the data and voice network segments. While other IP phones offer enhanced Layer 2 connectivity providing the option to use VLAN technology, to place the phone and the data traffic on two different VLANs. To ensure logical separation of voice and data in order to maintain the security of the VoIP environment, only layer 2 enhanced or VLAN capable phones should be considered for use. Many attacks on DOD computer systems are launched from within the network by dissatisfied or disgruntled employees, therefore, it is imperative that any active IP Phone data ports be disabled. just as with unused physical ports on a network switch. If unauthorized personnel gain access to the VoIP or data environment through an unsecured data port, they could cause disruptions, denial of service conditions, or access sensitive information. Disabling data ports on IP Phones prevents this type of unauthorized and unwanted activity.

**Default Finding Details:** The following IP Phones data ports are not disabled: List the phone locations and phone numbers.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Numerous potential impacts are made available by vulnerabilities associated with unauthorized access to the network.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.2

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Inspect effected devices (Manual)  
Inspect a sampling of effected devices to confirm compliance. Review device connections and port connections to determine if they are properly connected.  
Review phone configurations (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Fixes:** Properly configure IP Phones (Manual)  
Configure IP Phones to NOT display voice network information without the entry of a password or a PIN code.  
Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008308

**STIG ID:** VoIP 0125

**Release Number:** 1

**Status:** Active

**Short Name:** Port security on voice VLAN NOT implemented

**Long Name:** Port security is NOT configured on all switch-ports with voice VLAN membership.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓

<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	-------------------------------------	-------------------------------------	-------------------------------------

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that port security is configured on all switch-ports with voice VLAN membership. Many attacks on DOD computer systems are launched from within the network by dissatisfied or disgruntled employees, therefore, it is imperative that any active switch-ports with voice VLAN membership provide port security. If unauthorized personnel gain access to the VoIP VLAN through an unsecured switch port, they could cause disruptions, denial of service conditions, or access sensitive information. Port security on switch-ports with voice VLAN membership prevents this type of unauthorized and unwanted activity.

**Default Finding Details:** Port security is NOT configured on the following network access layer switches and/or on the following switch-ports with voice VLAN membership:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Numerous potential impacts are made available by vulnerabilities associated with unauthorized access to the network.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.2

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.  
Apply port security (Manual)  
Apply port security to switch-ports with voice VLAN membership.

**Vulnerability Key:** V0008309

**STIG ID:** VoIP 0127

**Release Number:** 1

**Status:** Active

**Short Name:** MAC addresses NOT limited on switch-ports

**Long Name:** The maximum number of MAC addresses that can be dynamically configured on a given switch port is NOT limited to that which is required to support authorized attached equipment (i.e., 1, 2, 3 or in some special cases 4).

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that the maximum number of MAC addresses that can be dynamically configured on a given switch port is limited to that which is required to support authorized attached equipment (i.e., 1, 3, or in some special cases 4). Allowing too many MAC addresses on a switch port could allow a mini-hub or switch to be added to the voice VLAN port or PC/data port on a IP phone to which additional unauthorized devices or workstations to be connected. In the event that only a phone is to be attached with no PC connected to it, 1 or 2 MAC addresses would be appropriate. If a PC is to be attached, then 3 is appropriate. In the special case where a security device is also attached to the phone along with a PC, then 4 would be appropriate.

**Default Finding Details:** The maximum number of MAC addresses that can be dynamically configured on a given switch port is NOT limited to that which is required on the following network access layer switches or switch-ports:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality. Numerous potential impacts are made available by vulnerabilities associated with unauthorized access to the network.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.5.2.2

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Inspect effected devices (Manual)  
 Inspect a sampling of effected devices to confirm compliance. Review device connections and port connections to determine if they are properly connected.

Review current configurations (Manual)

Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

**Fixes:**

Comply with Policy (Manual)

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Limit MAC Addresses (Manual)

Limit the maximum number of MAC addresses that can be dynamically configured on a given switch to that which is required (i.e., 1 - 3). IP phones with a multi-port switch (data/PC port) would require 3 MAC addresses if a PC is attached while only 2 if no PC is to be attached, IP phones without a multi-port switch (data/PC port) would only require 1 MAC address. In the special case where a security device is also attached to the phone along with a PC, then 4 would be appropriate.

**Vulnerability Key:** V0008318

**STIG ID:** VoIP 0130

**Release Number:** 3

**Status:** Active

**Short Name:** Soft-phone are installed without DAA approval

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override Guidance:** NONE

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document..

**Default Finding Details:**

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008235

**STIG ID:** VoIP 0135

**Release Number:** 2

**Status:** Active

**Short Name:** A local Soft Phone policy does not exist

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**IA Controls:** DCSD-1 IA Documentation  
ECSC-1 Security Configuration Compliance

**Categories:** 12.1 INFOCON Policy & Procedures

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
Classified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
---------------	-------------------------------------	-------------------------------------	-------------------------------------

**Severity:** Category III

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Default Finding Details:**

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008319

**STIG ID:** VoIP 0140

**Release Number:** 1

**Status:** Active

**Short Name:** Workstations with softphones NOT compliant

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	<b>I - Mission Critical</b>	<b>II - Mission Support</b>	<b>III - Administrative</b>
--	-----------------------------	-----------------------------	-----------------------------

<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Default Finding Details:**

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008233

**STIG ID:** VoIP 0150

**Release Number:** 3

**Status:** Active

**Short Name:** PC-based soft-phones not properly implemented.

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**IA Controls:** DCPA-1 Partitioning the Application  
ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category III

**Severity Override Guidance:** None

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Default Finding Details:**

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008236

**STIG ID:** VoIP 0160

**Release Number:** 3

**Status:** Active

**Short Name:** Remote softphones are not properly implemented

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document..

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable	<b>Comments:</b>  
--	--------------------------

<input type="checkbox"/> Not Reviewed	
---------------------------------------	--

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override Guidance:** None

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Default Finding Details:**

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008321

**STIG ID:** VoIP 0165

**Release Number:** 3

**Status:** Active

**Short Name:** Call center not configured as an enclave

**Long Name:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open	Comments:
-------------------------------	-----------

<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override Guidance:** NONE

**Vulnerability Discussion:** This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Default Finding Details:**

**Potential Impacts:** .

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.6

**Checks:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Fixes:** Deferred to PCCC Checklist (Manual)  
This requirement is superseded by the PC Communications Client STIG & Checklist. Refer to the appropriate document.

**Vulnerability Key:** V0008238

**STIG ID:** VoIP 0180

**Release Number:** 2

**Status:** Active

**Short Name:** Stateful firewalls not used at VoIP/WAN boundary

**Long Name:** A Stateful inspection firewall has not been deployed at the VoIP LAN-to-WAN connection.

**IA Controls:** EBBD-2 Boundary Defense  
EBBD-3 Boundary Defense  
ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that VoIP aware firewalls are deployed at all approved VoIP enclave to WAN connections providing VoIP call connectivity. Such firewalls must employ stateful packet inspection and dynamic port mapping. LAN-to-WAN VoIP connections may have application filtering issues when using the H.323 protocol. This problem is encountered when return TCP connections on higher range ports attempt to establish. There are similar issues when using SIP signaling. Therefore, VoIP aware stateful firewalls must be used at LAN-to-WAN VoIP call connection network points to protect the internal VoIP environment.

**Default Finding Details:** Stateful firewalls have not been deployed at VoIP WAN-to-WAN connection points.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the enclave's boundary defense

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Locate/inspect the VoIP firewall (Manual)  
Review network diagrams and confirm firewall type and deployment location within the VoIP environment. Review firewall configuration for H.323 and SIP rule settings.

**Fixes:** Implement stateful firewall (Manual)  
Implement stateful inspection firewalls at VoIP WAN-to-WAN connection points.

**Vulnerability Key:** V0008331  
**STIG ID:** VoIP 0190  
**Release Number:** 1  
**Status:** Active  
**Short Name:** NAT is NOT used on VoIP WAN connections.  
**Long Name:** NAT is NOT used on VoIP WAN connections.  
**IA Controls:** EBBD-1 Boundary Defense  
 EBBD-2 Boundary Defense  
 EBBD-3 Boundary Defense  
 ECSC-1 Security Configuration Compliance  
**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that NAT is implemented on approved VoIP enclave to WAN connections. To maintain the private addressing scheme (RFC 1918) on in the VoIP LAN enclave, Network Address Translation (NAT) must be implemented at the VoIP enclave WAN connection point. This provides additional protection in that hackers outside the VoIP network segment will not be able to scan the VoIP segment for vulnerabilities.

**Default Finding Details:** NAT is NOT used on VoIP WAN connections.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Implement VoIP NAT (Manual)  
Implement NAT on the VoIP enclave firewall.

**Vulnerability Key:** V0008240

**STIG ID:** VoIP 0200

**Release Number:** 2

**Status:** Active

**Short Name:** Voice Perimeter firewalls are not dedicated

**Long Name:** Voice enclave Perimeter firewalls are not dedicated to VoIP connections.

**IA Controls:** EBBD-1 Boundary Defense  
EBBD-3 Boundary Defense  
ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure all voice enclave security perimeter firewalls are dedicated to VoIP The IAO will ensure all VoIP security perimeter firewalls are

dedicated to VoIP traffic to reduce transmission latency caused by access control list (ACL) processing. Firewalls, routers, and switches should be implemented in a manner that will compartmentalize the VoIP servers and phones from unauthorized access. This is necessary to limit and control access from the data network and WAN to the IP telephony network, firewall controls are to be placed in front of all networks and components supporting VoIP servers. VoIP systems require many ports to be opened in firewalls to avoid a noticeable delivery delay. The protocol used for carrying VoIP traffic through the network uses a wide range of ports (10024 to 65535) to transport packets. The filtering of VoIP packets is difficult to perform to avoid noticeable delivery delay. It is for this reason that firewalls are to be dedicated to the VoIP environment to adequately handle telephony traffic. This will also help to mitigate the risk of possible malicious attacks that may originate from within the data network.

**Default Finding Details:** Voice enclave Perimeter firewalls are not dedicated to VoIP connections.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the enclave's boundary defense and unauthorized management access to VoIP systems from outside the enclave.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:** Review Network Diagrams- Fire (Manual)  
Review network diagrams and confirm firewall type and deployment location within the VoIP environment. Ensure firewalls are dedicated to processing VoIP traffic.

**Fixes:** Dedicate IP filters/firewall t (Manual)  
Review the VoIP environment and dedicate firewall and filtering device to the environment.

---

**Vulnerability Key:** V0008241  
**STIG ID:** VoIP 0210  
**Release Number:** 2  
**Status:** Active  
**Short Name:** VoIP firewall management traffic is not controlled  
**Long Name:** VoIP firewall administrative/management traffic (i.e. ports 69,161,162, 389) is not being controlled or encrypted at the VoIP network perimeter.  
**IA Controls:** EBBD-1 Boundary Defense  
EBBD-2 Boundary Defense  
EBBD-3 Boundary Defense  
EBRP-1 Remote Access for Privileged Functions  
EBRU-1 Remote Access for User Functions  
ECCT-1 Encryption for Confidentiality (Data in Transit)  
ECNK-1 Encryption for Need-To-Know  
ECSC-1 Security Configuration Compliance  
**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure VoIP perimeter firewall administrative/management traffic is blocked at the perimeter or tunneled/encrypted using VPN technology at the security perimeter (ports 69, 161, 162, 389). Administrative and management access to firewalls supporting the VoIP environment for configuration management must be protected. To securely protect the telephony network, firewall access must be controlled to guard against unauthorized intrusion, which could result in system or network compromise. Administering or managing firewalls from the same network used for public use increases the risk of compromising data that will allow unauthorized people access to critical areas of the VoIP network. At a minimum, these types of sessions must be controlled by port and IP or encrypted at the enclave perimeter.

**Default Finding Details:** VoIP firewall administrative/management traffic (i.e. ports 69,161,162, 389) is not being controlled or encrypted at the VoIP network perimeter. For example:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the enclave's boundary defense and unauthorized management access to VoIP systems from outside the enclave

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.9.2

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Control firewall admin access (Manual)  
Control all VoIP firewall administrative/management traffic by port and IP if internal

to the enclave. If remote connections are required from outside the enclave use encryption to secure the connections in addition to filtering by IP port and IP address.

**Vulnerability Key:** V0008242  
**STIG ID:** VoIP 0220  
**Release Number:** 2  
**Status:** Active  
**Short Name:** MS-SQL port 1433 not controlled at VoIP boundary  
**Long Name:** MS-SQL port 1433 is not being controlled at the VoIP security perimeter.  
**IA Controls:** EBBD-1 Boundary Defense  
 EBBD-2 Boundary Defense  
 EBBD-3 Boundary Defense  
 ECSC-1 Security Configuration Compliance  
**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure MS-SQL (port 1433) is blocked at the VoIP security perimeter. Microsoft SQL Server (MS-SQL) is used by some VoIP solutions and MS-SQL Server traffic uses port 1433. There are several serious vulnerabilities associated with MS-SQL Server that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts. MS-SQL vulnerabilities are well publicized and actively under attack. In order to ensure the security of VoIP environment this port must be controlled if not blocked at the enclave perimeter.

**Default Finding Details:** MS-SQL port 1433 is not being controlled at the VoIP security perimeter.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the enclave's boundary defense

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:**  
 Interview the IAO or SA (Interview)  
 Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
 Review current configurations (Manual)  
 Review current configuration files of effected devices to confirm compliance. The reviewer must physically verify, by reviewing firewall configuration files, that unused ports are disabled. Site personnel provide these files.

**Fixes:**  
 Block MS-SQL port 1433 (Manual)  
 Block MS-SQL port 1433 at the VoIP security perimeter.

**Vulnerability Key:** V0008243

**STIG ID:** VoIP 0230

**Release Number:** 2

**Status:** Active

**Short Name:** NTP port 123 not controlled at VoIP boundary

**Long Name:** The network time protocol (NTP) port 123 is not blocked at the VoIP security perimeter and clock is not being derived from a local global position system (GPS).

**IA Controls:**  
 EBBD-1 Boundary Defense  
 EBBD-2 Boundary Defense  
 EBBD-3 Boundary Defense  
 ECSC-1 Security Configuration Compliance

**Categories:** 4.7 Routers

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

<b>Severity:</b>	Category III
<b>Severity Override:</b>	None
<b>Guidance:</b>	
<b>Vulnerability Discussion:</b>	Updated Requirement: The IAO will ensure the network time protocol (NTP port 123) is blocked at the VoIP-WAN security perimeter. The IAO will ensure the internal VoIP network device time is derived from the premise router of the LAN on which the VoIP system resides. The premise router is synchronized with two up-stream NTP servers and acts as the NTP server for the LAN. This is in accordance with the Network Infrastructure STIG and is for the purpose of logging and audit time stamp coordination with other devices and systems on the LAN. This includes the IP network side of media gateways (and other TDM-IP devices) but not the TDM side of the device. VoIP network administrative/audit time should be derived from the local network premise router. The Premise router should synchronize its time from 2 of the Naval Observatory Tier1 NTP servers. Timing and synchronization is critical to the telephony network since VoIP packets cannot be re-transmitted to compensate for unstable or intermittent timing. Network Time Protocol (NTP) is used administratively to automatically synchronize computer clock times among systems on a network. Critical VoIP servers depend on an NTP server by which to synchronize their own clocks. In order to ensure proper synchronization with other VoIP components NTP must be derived from GPS system. This is especially important when making VoIP calls across domains in order to ensure global synchronization.
<b>Default Finding Details:</b>	The network time protocol (NTP) port 123 is not blocked at the VoIP security perimeter and clock is not being derived from the local network.
<b>Potential Impacts:</b>	Degradation of the enclave's boundary defense.
<b>Responsibility:</b>	
<b>Mitigations:</b>	
<b>References:</b>	Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2
<b>Checks:</b>	Interview the IAO or SA (Interview) Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable. Review current configuration (Manual) Review current configuration files of effected devices to confirm compliance.
<b>Fixes:</b>	Block (NTP) port 123 (Manual) Block (NTP) port 123 at the VoIP-WAN security perimeter. Derive time locally (Manual) Derive VoIP network administrative/audit time from the local network premise router. Synchronize Premise router time (Manual) Synchronize Premise router time to 2 of the Naval Observatory NTP servers in accordance with the Network Infrastructure STIG

---

**Vulnerability Key:** V0008244  
**STIG ID:** VoIP 0240

**Release Number:** 2  
**Status:** Active  
**Short Name:** Terminal services (port 3389) is not being blocked  
**Long Name:** Terminal services (port 3389) is not being blocked, or if used, encrypted at the VoIP security perimeter.  
**IA Controls:** EBBD-1 Boundary Defense  
 EBBD-2 Boundary Defense  
 EBBD-3 Boundary Defense  
 EBRU-1 Remote Access for User Functions  
 ECCT-1 Encryption for Confidentiality (Data in Transit)  
 ECNK-1 Encryption for Need-To-Know  
 ECSC-1 Security Configuration Compliance  
**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure Terminal Services or remote desktop protocol (port 3389) is blocked at the security perimeter or that these connections are encrypted. Terminal Services enables users to log on to a remote system as if they were logging on locally. The Terminal Services client program, which runs on any version of Windows, redirects the local keyboard and mouse and emulates the remote video display. Some VoIP vendors use terminal services to remotely manage their VoIP systems. If Terminal Services access is compromised the whole VoIP environment would be in jeopardy and at risk of compromise or even denial of service. It is imperative that all Terminal Services connections be blocked at the enclave boundary and if used all connections are to be encrypted.

**Default Finding Details:** Terminal Services are not being used and are not blocked at the security enclave boundary. and/or Terminal Services are used and are not being controlled or encrypted at the security enclave boundary.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Unauthorized management access to VoIP systems from outside the enclave. Degradation of the enclave's boundary defense

**Responsibility:**

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Block all Terminal Services (Manual)  
If not used, block all Terminal Services access (port 3389) at the security enclave boundary. If Terminal Services is required, encrypt all connections at the security enclave boundary.

**Vulnerability Key:** V0008245

**STIG ID:** VoIP 0245

**Release Number:** 2

**Status:** Active

**Short Name:** Remote firewall Web connections are not proxied

**Long Name:** Remote firewall Web connections for firewall administration are not proxied at the site perimeter.

**IA Controls:** EBBD-1 Boundary Defense  
EBBD-2 Boundary Defense  
EBBD-3 Boundary Defense  
ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all remote HTTP access to the VoIP enclave perimeter firewalls is proxied. HTTP access from the VoIP enclave, if required, should route through the data enclave. Additionally HTTPS should be used in place of this if possible. This includes ports 80, 8080, 443, 8002, and 8003. In order to ensure the security of VoIP perimeter firewalls it is imperative that administrative/management connections and access to the devices be controlled. Some VoIP systems support web-based remote administration using the HTTP protocol. Web access is a viable mechanism for monitoring, configuring, and attacking critical devices such as firewalls. It is imperative that remote Web access for administrative purposes be proxied at the enclave perimeter.

**Default Finding Details:** Remote firewall administrative connections are not being proxied at the enclave perimeter.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Unauthorized management access to VoIP systems from outside the enclave. Degradation of the enclave's boundary defense

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.2

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:** Proxy "Web based" Management (Manual)  
Proxy all remote firewall and VoIP system "web based" administrative connections at the enclave perimeter.

---

**Vulnerability Key:** V0008247

**STIG ID:** VoIP 0270

**Release Number:** 2

**Status:** Active

**Short Name:** Critical servers supporting VoIP are not dedicated

**Long Name:** Critical servers supporting the VoIP telephony environment are not dedicated to VoIP telephony applications.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open	Comments:
-------------------------------	-----------

<input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	
--	--

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that VoIP servers are dedicated to only applications required for VoIP operations. VoIP servers represent mission critical equipment that contain potentially sensitive information that needs to be secured and treated with the same precautions as any other servers containing sensitive information. Dedicating critical VoIP servers to only VoIP required applications is key to securing the IP telephony environment. To minimize possible risk these servers are to be dedicated to the IP Telephony applications required for VoIP operations minimizing the chance of infection or attack through an unused, unnecessary application residing on the system.

**Default Finding Details:** The following critical servers supporting the telephony environment are not dedicated to telephony VoIP applications: The following critical servers supporting the VoIP telephony environment are not dedicated to VoIP telephony applications: (List the servers.) The following applications were found on critical VoIP servers that are not directly related to the operation of the VoIP server or system or its management: (List the applications):

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. The DOD voice system may not be protected as required and may be vulnerable to attack or loss of availability due to non-VoIP related applications.

**Responsibility:**

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.1

**Checks:**  
 Interview the IAO or SA (Interview)  
 Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
 Review Server applications (Manual)  
 Review the server for additional applications required for operational support.

**Fixes:**  
 Dedicate VoIP Servers (Manual)  
 Dedicate critical servers supporting the VoIP telephony environment to running VoIP

telephony applications only. Additionally, remove all unnecessary portions of the Operating System such as sub-applications or files and routines that are not required to support the VoIP telephony system.

**Vulnerability Key:** V0008248

**STIG ID:** VoIP 0280

**Release Number:** 2

**Status:** Active

**Short Name:** Servers supporting VoIP are not STIG compliant

**Long Name:** Critical servers supporting the telephony environment have not been secured in compliance with applicable STIG guidelines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that critical VoIP servers have been secured in compliance with all applicable STIGs (i.e., UNIX, Microsoft NT/Win2K, database, web, etc.). VoIP servers represent mission critical equipment that contain potentially sensitive information that needs to be secured and treated with the same precautions as any other server containing sensitive information. Securing critical VoIP servers is key in securing the IP Telephony environment. Some vendors provide IP Telephony services on their own proprietary systems while others provided these services on standard UNIX and Microsoft Windows based systems. Most known vulnerabilities exist on UNIX and Windows based operating systems. They may also use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Additionally, application security guidance may be applicable for the vendor's application that makes the server or device perform the

functions, or the management, of the system. Therefore, the securing of these voice processing and signaling platforms, to include their installed applications, is vital in protecting the VoIP environment from malicious attack. The specific VoIP system server or device determines the applicability of any given STIG.

**Default Finding Details:** The following critical servers supporting the telephony environment have not been secured in compliance with the following applicable STIG guidelines: (List the servers and the STIGs that have not been applied)

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. The DOD voice system may not be protected as required and may be vulnerable to attack or loss of availability due to a multitude of OS and application vulnerabilities.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.1

**Checks:** Review SRR documentation (Interview)  
Interview the IAO. Obtain a copy of the applicable SRR results and review for compliance. If SRR results are not available, then SRR a representative number of devices.

**Fixes:** Secure critical servers (Manual)  
Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e., UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

---

**Vulnerability Key:** V0008349

**STIG ID:** VoIP 0281

**Release Number:** 1

**Status:** Active

**Short Name:** Not using Vendor originated Patches

**Long Name:** Software patches for critical VoIP servers and other IPT devices DO NOT originate from the system manufacturer and are NOT applied in accordance with manufacturer's instructions.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 3.1 Security Patches

<input type="checkbox"/> Open	Comments:
<input type="checkbox"/> Not a Finding	
<input type="checkbox"/> Not Applicable	
<input type="checkbox"/> Not Reviewed	

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override Guidance:**

**Vulnerability Discussion:**

Requirement: The IAO will ensure that software patches for critical VoIP servers and other IPT devices originate from the system manufacturer and are applied in accordance with manufacturer's instructions. Many IPT / VoIP systems are based on general-purpose operating systems and applications such as databases and web servers (i.e., Windows XX, MS-SQL, IIS, Unix, LINUX, etc). The original vendors of these general-purpose software packages provide patches for their individual packages. A vendor of a IPT / VoIP system must test and approve these patches for use on their system before they are applied in the event that the OEM patch might break a portion of the IPT / VoIP system or degrade it's security. The IPT / VoIP vendor may have to modify the OEM patch before releasing it to their customers.

**Default Finding Details:**

Software patches for critical VoIP servers and other IPT devices DO NOT originate from the system manufacturer and are NOT applied in accordance with manufacturer's instructions.

**Potential Impacts:**

Denial of Service. Patches that have not been approved and provided by a vendor and/or applied in conflict with vendor's instructions can break features or disable the system.

**Responsibility:**

Information Assurance Officer

**Mitigations:**

**References:**

Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.1.1

**Checks:**

Only Apply vendor approved pat (Manual)  
Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

**Fixes:**

Only Apply vendor approved pat (Manual)  
Only Apply vendor-approved or vendor supplied patches. Correct site policy to require only vendor provided and approved patches are applied.

**Vulnerability Key:** V0008286

**STIG ID:** VoIP 0282

**Release Number:** 1

**Status:** Active

**Short Name:** Not applying Vendor approved IAVA Patches

**Long Name:** IAVAs are NOT being referred to IPT / VoIP vendors for approval and patch distribution

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 3.1 Security Patches

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all IAVAs applicable to the general-purpose systems and applications used in VoIP systems are referred to the system manufacturer for approval and patch distribution in order to maintain timely IAVA compliance. IPT / VoIP vendors must be immediately advised of IAVAs that apply to their systems so that they can test the required patch / mitigation and subsequently distribute an approved patch for their system (in accordance with VoIP0281) so that the site can maintain IAVA compliance.

**Default Finding Details:** IAVAs are NOT being referred to IPT / VoIP vendors for approval and patch distribution

**Potential Impacts:** Systems may be left vulnerable to the issue detailed in the IAVA.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.1.1

**Checks:** Determine IAVA response (Interview)  
Interview the IAO and/or SA to determine their response to IAVAs affecting the platforms supporting IPT / VoIP systems. Review patching records.

**Fixes:** Comply with IAVA policy (Manual)  
Comply with policy. Contact the VoIP system vendor upon receipt of a IAVA to determine if the vendor can provide the required approved patch or refer the IAVA to the vendor for testing and approval

---

**Vulnerability Key:** V0008249

**STIG ID:** VoIP 0290  
**Release Number:** 2  
**Status:** Active  
**Short Name:** Remote admin of VoIP servers is not encrypted  
**Long Name:** Remote administrative connections to critical VoIP servers are not encrypted.  
**IA Controls:** EBRU-1 Remote Access for User Functions  
 ECCT-1 Encryption for Confidentiality (Data in Transit)  
 ECNK-1 Encryption for Need-To-Know  
 ECSC-1 Security Configuration Compliance  
**Categories:** 8.1 Encrypted Data in Transit

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The system administrator will ensure all remote administrative connections to critical VoIP servers are encrypted. In order to ensure the security of critical VoIP servers it is necessary that administrative connections be encrypted. Remote access connections are a viable mechanism for monitoring, configuring, and attacking these critical systems. It is imperative, that at a minimum, remote access connections to critical VoIP servers be encrypted at the enclave perimeter.

**Default Finding Details:** Remote administrative connections to the following critical VoIP servers are not encrypted.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Unauthorized management access to VoIP systems from outside the enclave

**Responsibility:** System Administrator

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.9.1

**Checks:** Interview the IAO or SA (Interview)  
 Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

**Demonstrate Compliance (Interview)**

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Review Network Diagrams (Manual)**

Review network diagrams and confirm network perimeter device configuration rule settings for specific port and proxy control.

**Fixes:**

**Encrypt all administrative ac (Manual)**

Encrypt all administrative access connections to critical VoIP servers. At a minimum these remote connections are to be encrypted at the enclave perimeter.

**Vulnerability Key:** V0008332

**STIG ID:** VoIP 0295

**Release Number:** 1

**Status:** Active

**Short Name:** VoIP system management is not per DSN STIG

**Long Name:** The VoIP system management is not performed in accordance with the requirements in the DSN STIG

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all VoIP systems are managed in accordance with all requirements in the DSN STIG. VoIP system management is not detained in the IPT/VoIP STIG. This version of the STIG refers to the DSN STIG for system management requirements.

**Default Finding Details:** he VoIP system management is not performed in accordance with the requirements in the DSN STIG

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation. Unauthorized management access to VoIP systems from outside the enclave

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.9

**Checks:** Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.  
Review network diagrams (Manual)  
Review network diagrams and confirm VoIP system Management connections are encrypted.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

---

**Vulnerability Key:** V0008250  
**STIG ID:** VoIP 0300  
**Release Number:** 2  
**Status:** Active  
**Short Name:** VoIP is not encrypted over a "public" IP WAN  
**Long Name:** VoIP traffic is being sent over a public IP network (i.e. internet, NIPRNet) without being encrypted.  
**IA Controls:** EBRU-1 Remote Access for User Functions  
ECCT-1 Encryption for Confidentiality (Data in Transit)  
ECNK-1 Encryption for Need-To-Know  
ECSC-1 Security Configuration Compliance  
**Categories:** 8.1 Encrypted Data in Transit

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that all VoIP traffic that is sent over approved VoIP enclave-to-WAN connections via an IP WAN network (i.e., Internet, NIPRNet,) is encrypted, at a minimum, between enclaves across the WAN. NOTE: The inherent site-to-site encryption employed in classified networks, such as the SIPRNet, meets this requirement. When WAN VoIP connections are established, all call privacy can be lost. Just as all DSN trunks are encrypted ensuring the privacy of subscriber calls any Wan-to-Wan VoIP call connection must be encrypted in order to maintain the same level of security. If Wan-to-Wan VoIP traffic is passed in the clear it is open to sniffing attacks. Encryption can be accomplished at the link-level through the incorporation of VPN technology. Gateway devices are normally designed to handle heavier processing loads and are also capable of providing link encryption. If implemented, either method would be transparent to the subscriber community but provide the same level of security and privacy that is provided to long distance voice calls processed by the DSN.

**Default Finding Details:** VoIP Wan calls are being processed in the clear.

**Potential Impacts:** Loss of confidentiality

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.8

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Review network diagrams - Wan (Manual)  
Review network diagrams and device configurations as appropriate, to confirm VoIP LAN-to-Wan connections are encrypted.  
Review current configuration: Review current configuration files of effected devices and confirm compliance

**Fixes:** Encrypt all VoIP/ Wan calls (Manual)  
Secure all VoIP Wan-to-Wan call connections via encryption.

**Vulnerability Key:** V0008251  
**STIG ID:** VoIP 0310  
**Release Number:** 3  
**Status:** Active  
**Short Name:** Legacy Unified mail, text to speech is enabled  
**Long Name:** The unified mail, text to speech feature is enabled using an existing email system.  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure text-to-speech is disabled if the voice mail platform is configured to interact with a legacy corporate email system and both systems are not collocated in the same or adjoining VLANs as required under the VLAN section above. Voice mail services in a VoIP environment are available in several different configurations. A legacy voice mail platform can connect to a VoIP environment to provide voice mail services for VoIP users. In the same respect, a VoIP voice mail platform can provide voice mail services to the legacy voice users and the VoIP users. Some VoIP voice mail systems are also capable of providing unified mail, by interacting with existing email messaging systems. If the legacy corporate email system is accessible to the VoIP system not placed in a VLAN that is separate from the data network VLANs, the text to speech feature will degrade the separation of the voice and data environments and VLANs. See VLAN requirements above.

**Default Finding Details:** The unified mail, text to speech feature is enabled using an existing email system.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Additionally the corruption of data and/or unauthorized use of the supporting server.

**Responsibility:** System Administrator  
Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.10

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Demonstrate Compliance (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

**Fixes:** Disable unified mail text to s (Manual)  
Disable the text to speech of unified mail if using an existing email system for voice mail.

**Vulnerability Key:** V0008253

**STIG ID:** VoIP 0330

**Release Number:** 3

**Status:** Active

**Short Name:** Voice mail system VoIP is not STIG compliant

**Long Name:** The Voice mail system supporting VoIP is not secured to applicable STIG guidance.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability:** Requirement: The IAO will ensure the server hosting the Voice Mail Service is

**Discussion:** properly secured in accordance with all applicable STIGs (i.e., Windows, Unix, Database, and Web). Various VoIP solutions provide voice mail services support in different ways to include integrating these services with existing email services. When voice mail is leveraged off of an existing email server it leaves the telephony environment open to all vulnerabilities that exist on the data network. Many of these voice mail services can provide access to the VoIP environment via unsecured channels if servers are not secured. This can happen through the abuse and use of enabled but unused services or through known un-patched vulnerabilities that exist on common mail servers. To protect against this, all unused services are to be disabled and all voice mail application servers are to be secured using the applicable STIG guidance.

**Default Finding Details:** The following Voice mail system supporting VoIP is not secured to applicable STIG standards:

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Additionally the corruption of data and/or unauthorized use of the supporting server.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Para 3.10

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Review server SRR results (Manual)  
Obtain a copy of all applicable SRR or Self Assessment results and review for compliance. If there are a significant number of findings reported or if the an applicable STIG was not applied, this is a finding. If SRR results are not available, then perform all applicable SRRs on a representative number of VoIP system servers and devices. Note: The specific VoIP system server or device determines the applicability of any given STIG. Many VoIP system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.

**Fixes:** Secure critical servers (Manual)  
Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e., UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

---

**Vulnerability Key:** V0008254

**STIG ID:** VoIP 0340

**Release Number:** 3

**Status:** Active

**Short Name:** Supporting application services not STIG Compliant

**Long Name:** Application services (i.e. SQL, IIS, Apache, Oracle, etc.) supporting the VoIP environment

have not been secured to applicable STIG guidance.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure the application services (SQL, IIS, Apache, Oracle, etc.) supporting the voice mail service are properly secured according to the appropriate STIGs. Various VoIP solutions use various application services to provide Voice and voice mail support. Many of these applications can provide access to the VoIP environment via unsecured channels. This can happen through the abuse and use of enabled but unused services or through known un-patched vulnerabilities that exist on common application servers. All unused services are to be disabled and all application servers are to be secured using the applicable STIG guidance.

**Default Finding Details:** The following application services supporting the VoIP environment have not been secured to applicable STIG standards.

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Additionally the corruption of data and/or unauthorized use of the supporting server.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.10

**Checks:** Review server SRR results (Manual)  
Obtain a copy of all applicable SRR or Self Assessment results and review for compliance. If there are a significant number of findings reported or if the an applicable STIG was not applied, this is a finding. If SRR results are not available, then perform all applicable SRRs on a representative number of VoIP system servers and devices. Note: The specific VoIP system server or device determines the applicability of any given STIG. Many VoIP system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or

Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.

**Fixes:**

Secure critical servers (Manual)

Secure critical servers supporting the telephony environment. Apply all applicable STIGs (i.e., UNIX, Microsoft Windows, database, web, etc. UNIX, Win2k/NT, DSN, etc.) and ensure compliance with applicable STIG guidelines.

**Vulnerability Key:** V0008255

**STIG ID:** VoIP 0350

**Release Number:** 2

**Status:** Active

**Short Name:** Voice mail settings can be changed - unsecured

**Long Name:** Voice mail settings can be changed by the subscriber via a unsecured/unencrypted connection.

**IA Controls:** EBRU-1 Remote Access for User Functions  
ECCT-1 Encryption for Confidentiality (Data in Transit)  
ECNK-1 Encryption for Need-To-Know  
ECSC-1 Security Configuration Compliance

**Categories:** 8.1 Encrypted Data in Transit

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure the subscriber can only change their voice mail settings via the phone interface or through an SSL connection. HTTP and Telnet services will be disabled on the voice mail platform. Access to voice mail services via

an encrypted IP connection is inherently dangerous because anyone with a sniffer and access to the right LAN segment can acquire the subscriber's account and password information. With this intercepted information a hacker could gain access to the subscribers voice mail, intercept sensitive information, and/or perform other destructive actions. It is for this reason that all subscriber connections to voice mail settings are to be encrypted using SSL, SSH, or other encryption if natively provided by the voice mail/VoIP system.

**Default Finding Details:** Voice mail settings can be changed by the subscriber via an unsecured/unencrypted "Web" connection (i.e., in the clear).

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Application of features and potential call redirection by unauthorized users.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.10

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.  
Demonstrate Voice mail Config (Interview)  
Have the IAO or SA demonstrate compliance with the requirement; Have the SA demonstrate from an IP Phone. If settings can also be changed via a web connection, ensure this connection utilizes SSL.

**Fixes:** Secure voice mail user config (Manual)  
Secure all subscriber access to voice mail settings with SSL, SSH or available encryption.

**Vulnerability Key:** V0008256

**STIG ID:** VoIP 0360

**Release Number:** 3

**Status:** Active

**Short Name:** Wireless VoIP is being used without Wireless STIG

**Long Name:** Wireless VoIP is being used without Wireless STIG security guidance applied.

**IA Controls:** ECSC-1 Security Configuration Compliance  
ECWN-1 Wireless Computing and Networking

**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	✓	✓	✓
<b>Sensitive</b>	✓	✓	✓
<b>Public</b>	✓	✓	✓

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that if wireless VoIP is used, the requirements contained in the Wireless STIG have been applied to the wireless VoIP environment. The Incorporation of Wireless technology elevates many existing VoIP concerns such as quality of service (QoS), network capacity, provisioning, architecture and not the least important, security. Many government entities are exploring mobile communication solutions that include wireless VoIP that can meet critical needs for interoperability and flexibility. If this technology is deployed all the requirements in the VoIP STIG as well as those contained in the Wireless STIG are to be applied to the wireless VoIP environment.

**Default Finding Details:** Wireless VoIP is being used without Wireless STIG security guidance applied.

**Potential Impacts:**

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.11

**Checks:**  
Interview the IAO (Interview)  
Review the SSAA (Manual) - Review the SSAA and verify that all VoIP installations or modifications are included. Verify there is a procedure for approving changes to configuration.  
Review Wireless SRR results (Manual)  
Review the results of the most recent Wireless Reviews and/or wireless discovery. If Wireless VoIP is used, and there are a significant number of findings reported against the WLAN or if the STIG was not applied, this is a finding.

**Fixes:**  
Comply with Wireless Policy (Manual)  
Apply requirements contained in both the VoIP STIG and the Wireless STIG wherever VoIP over Wireless is used.

**Vulnerability Key:** V0008333

**STIG ID:** VoIP 0361

**Release Number:** 1

**Status:** Active

**Short Name:** NO DAA approval for Wireless VoIP  
**Long Name:** Wireless VoIP is being used without DAA approval  
**IA Controls:** ECSC-1 Security Configuration Compliance  
**Categories:** 14.3 Network Device Configuration

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that written DAA approval is obtained prior to the implementation of VoIP over WLAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors. The Incorporation of Wireless technology elevates many existing VoIP concerns such as quality of service (QoS), network capacity, provisioning, architecture and not the least important, security. Many government entities are exploring mobile communication solutions that include wireless VoIP that can meet critical needs for interoperability and flexibility. If this technology is deployed the DAA must be aware and accept the risk.

**Default Finding Details:** Wireless VoIP is being used without DAA approval

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.11

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

**Fixes:** Comply with Policy (Manual)  
 Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008257  
**STIG ID:** VoIP 0370  
**Release Number:** 2  
**Status:** Active  
**Short Name:** The VoIP system is not DSN APL certified  
**Long Name:** VoIP systems or networks are connected to the DSN or PSTN switching system without being certified and placed on the DSN APL.  
**IA Controls:** EBCR-1 Connection Rules  
 ECSC-1 Security Configuration Compliance  
**Categories:** 12.6 CAP

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** Gold

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity Override:** None

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that no VoIP systems or networks are connected to the DSN switching system without being certified, accredited, and placed on the DSN Approved Products List per DODI 8100.3. Any VoIP network connected to any DSN switch poses a potential security risk to the network and should not be connected until interoperability certification by the DISA Joint Interoperability Test Command (JITC) and Information Assurance Certification and Accreditation by the DISN Security accreditation Working Group (DSAWG) is completed.

**Default Finding Details:** VoIP systems that are not DSN APL certified are connected to the DSN..

**Potential Impacts:** Denial of Service and/or unauthorized access to network or voice system resources or services and the information they contain. Loss of confidentiality Non-compliance with public law and DOD policy resulting in the possible disconnection of the VoIP system from the DSN and other legal action.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** DOD Telecommunications and Defense Switched Network (DSN) STIG Section 6.0 Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.13  
DODI 8100.3; Department of Defense (DoD) Voice Networks DoD Voice Networks, 16 January, 2004

**Checks:** Interview the IAO or SA (Interview)  
Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

**Fixes:** Comply with Policy (Manual)  
Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

**Vulnerability Key:** V0008329

**STIG ID:** VoIP 0900

**Release Number:** 1

**Status:** Active

**Short Name:** External VoIP calls NOT routed via Media Gateway

**Long Name:** Calls to and from the enclave system to external networks are NOT routed via Media Gateway

**IA Controls:** EBBD-1 Boundary Defense  
EBBD-2 Boundary Defense  
EBBD-3 Boundary Defense  
ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

MAC / Confidentiality Grid:	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category II

**Severity:** NONE

**Override**

**Guidance:**

**Vulnerability**

**Discussion:**

Requirement: The IAO will ensure that all calls into and out of the VoIP network enclave are routed via a media gateway to the traditional TDM networks i.e., DSN and/or PSTN. An exception is made for DAA approved remote VoIP instruments and Soft Phones that connect to the VoIP network enclave via a VPN and are therefore part of the VoIP network. As of the writing of the IPT/VoIP STIG V2R1, off-site VoIP Trunking is not approved for use in unclassified DOD telecommunications systems. The DOD DSN PMO is only certifying VoIP systems at the PBX-1, PBX-2, and SMEO level, as specified in the GSCR, for inclusion on the DSN APL. These systems are specified for use at the BPCS level. No systems are being certified to use VoIP Trunking for off-premise connections. Due to the fact that DOD policy requires that only DSN APL certified systems be deployed, IP trunking is not approved. All trunking connections to DOD VoIP networks must be through media gateways to the TDM DSN/PSTN. This requirement is intended to assure proper access the DSN/PSTN as well as interoperability between VoIP systems in other enclaves that may be from different vendors. The Standard VoIP signaling protocols (SIP and H.323) were developed to provide signaling methods for the transport of voice and video across the Internet as well as some other types of Internet communications. As such, they were not developed to support the many features that we have come to rely on in today's TDM based enterprise phone systems. To overcome this lack of standardized features, each vendor of a VoIP system has developed their systems to provide these features in different ways. Some use modifications or extensions of the standard protocols, while others use proprietary protocols. Typically, these systems do not interoperate. Additionally, this supports current data firewall policy.

**Default Finding Details:**

Calls to and from the enclave system to external networks are NOT routed via Media Gateway

**Potential Impacts:**

Inability to communicate outside the enclave.

**Responsibility:**

Information Assurance Officer

**Mitigations:**

**References:**

Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.1

**Checks:**

Interview the IAO and/or SA (Interview)  
Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
Review current configuration (Manual)  
Review current configuration files of effected devices to confirm compliance.

**Fixes:**

Implement Media Gateway (Manual)  
Block all VoIP traffic at the enclave boundary and implement a media gateway to handle calls into and out of the enclave.

---

**Vulnerability Key:** V0008330

**STIG ID:** VoIP 0901

**Release Number:** 1

**Status:** Active

**Short Name:** VoIP trunking is used without DAA approval.  
**Long Name:** VoIP trunking is used without DAA approval.  
**IA Controls:** EBBD-1 Boundary Defense  
 EBBD-2 Boundary Defense  
 EBBD-3 Boundary Defense  
 ECSC-1 Security Configuration Compliance

**Categories:** 4.3 Firewall

<input type="checkbox"/> Open <input type="checkbox"/> Not a Finding <input type="checkbox"/> Not Applicable <input type="checkbox"/> Not Reviewed	Comments:
---	-----------

**Condition:** VoIP/VoSIP Policy (Target: VoIP/VoSIP Policy)

**Policy:** All Policies

**MAC / Confidentiality Grid:**

	I - Mission Critical	II - Mission Support	III - Administrative
<b>Classified</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Sensitive</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Public</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Severity:** Category III

**Severity Override:** NONE

**Guidance:**

**Vulnerability Discussion:** Requirement: The IAO will ensure that written DAA approval is obtained prior to the implementation of IP Trunking connections from the VoIP enclave to the WAN. The IAO will maintain documentation pertaining to such approval for inspection by auditors. The use of VoIP Trunking can subject the enclave to threats from the WAN if the enclave boundary is not properly protected. VoIP communications requires that there be up to 4 ports opened in the boundary firewall for each call in progress. This can leave gaping holes in a enclave's boundary.

**Default Finding Details:** VoIP trunking is used without DAA approval.

**Potential Impacts:** Denial of Service, loss of confidentiality, and/or unauthorized access to network or voice system resources or services and the information they contain. Degradation of the data and VoIP network segregation.

**Responsibility:** Information Assurance Officer

**Mitigations:**

**References:** Internet Protocol Telephony (IPT) / Voice over Internet Protocol (VoIP) STIG Section 3.7.2.1

**Checks:** Interview the IAO and/or SA (Interview)  
 Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.  
 Review current configuration (Manual)

**Fixes:**

Review current configuration files of effected devices to confirm compliance.

Implement Media Gateway (Manual)

Block all VoIP traffic at the enclave boundary and implement a media gateway to handle calls into and out of the enclave.

Obtain DAA approval (Manual)

Obtain DAA approval for VoIP Trunking and use. Be sure the DAA is informed regarding the IA issues with using VoIP Trunking. Maintain DAA approval documentation. Otherwise discontinue use of VoIP Trunking.

---

**Vulnerability Count - 63**

