Defense Information Systems Agency

Global Video Services (GVS)
Periods Processing / VTC STIG Use
Policy Document

09 December 2014
Version 1.1

Global Video Services (GVS PMO)
PO Box 549
Ft. Meade, Maryland 20755-0549

DISTRIBUTION

Requests for this document shall be referred to Program Management Office.

From	To

CHANGE LOG

This record shall be maintained throughout the life of the document. Each change and published update shall be recorded.

CHANGE / REVISION RECORD				
Date	**Page/ Paragraph**	**Description of Change**	**Version**	**Made By:**
12/02/2014	All	Initial Release / Revision of 6 August draft document	1.0	E. Georg/G. Saiidifar/J. Geib
12/09/2014	All	Edits/comments by IA personnel	1.1	J. Mutunga/J. Geib

Table of Contents

August 6, 2014

Chief of Video Services
P. O. Box 549
Ft Meade, MD 20755-0549

FOREWORD

As required by Executive Order 12829 and under the following authority:

a. DoD Directive 5220.22M, "National Industrial Security Program (NISP), February 28, 2006, DoD 8500.2.
b. Information Assurance (IA) Implementation Policy.
c. Army Reg 380-19 Information Security.
d. National Security Telecommunications and Information Systems Policy (NSTISSP), No. 11.
e. National Policy Governing the Acquisition Assurance and IA-Enabled Information Assurance and IA-Enabled Information Technology (IT) Products.
f. Video Tele-Conference Security Technical Implementation Guide (STIG), Version 1, Release 3.
g. DISA Circular 300-115-3 Communications Security Classification Guide.

All video teleconferencing suites operating on the Global Video Services (GVS) network will, at a minimum, adhere to the policies and procedures found in this document providing baseline standards for the protection of classified information.

Users of this document are encouraged to submit recommended changes through the Chief of Video Services at the following address:

Defense Information Systems Agency
Chief of Video Services
P. O. Box 549
Ft Meade, MD 20755-0549

PREFACE

Purpose

The Defense Information System Network (DISN) Global Video Services (GVS) Periods Processing / VTC STIG Use Policy Document establish standards of performance required to ensure that Video Teleconferencing (VTC) communications throughout the DISN network are secure. This document and the VTC STIG jointly prescribe the policies, assign responsibilities, and provide procedures required to ensure that necessary security measures are implemented throughout the GVS network.

Applicability

This Security Policy applies to all Department of Defense (DoD) components, other government departments and agencies, and sponsored allied personnel operating Video Teleconferencing Facilities (VTFs) connecting to the GVS network.

Authority

This Policy Document is published in accordance with the authority contained in Executive Order 12829 covering IA security procedures.

References

The following references apply to this Security Policy.

a. DoD Directive 5220.22M, "National Industrial Security Program (NISP)," February 28, 2006, DoD 8500.2.
b. Information Assurance (IA) Implementation Policy.
c. Army Reg 380-19 Information Security.
d. National Security Telecommunications and Information Systems Policy (NSTISSP) No. 11.
e. National Policy Governing the Acquisition Assurance (IA) and IA-Enabled Information Assurance and IA-Enabled Information Technology (IT) Products.
f. Security Technical Implementation Guide.
g. DISA Circular 300-115-3 Communications Security.

1 PERIODS PROCESSING

1.1 Background

Due to the environment that we find ourselves operating in today and will in the future, it is imperative that we develop methods to secure all sensitive data we transmit throughout the GVS network. In the past, the legacy DVS network was limited to Switched Digital Services (H.320) to transmit voice and data (graphics, etc.) for the duration of each session. The inherent nature of the H.320 network limited the exposure to hostile intrusion.

As more Commands used DVS services, the network became saturated, forcing DVS to look at other methods / networks to carry the increased traffic. The obvious choice was a move to Internet Protocol (IP) (H.323) conferencing. The parent organization of DISN and GVS, Defense Information Systems Agency (DISA), owns and operates two IP networks–Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet)– both of which are utilized for IP conferencing.

The upgrade in technology that provided an increase in available bandwidth however, introduced a greater threat to hostile intrusion. To mitigate these threats DISN and GVS have instated two processes—Periods Processing and adherence to Video Teleconferencing (VTC) Security Technical Implementation Guide (STIG) requirements (see Section 2).

Note: Some GVS users – for example, sites that use or have multiple classification capabilities on a single CODEC – will need to adhere to the Periods Processing policies described in this document. Other GVS users, such as those that connect solely to either NIPRNet or SIPRNet via a single CODEC – will not need to adhere to the requirements stipulated by Periods Processing. All GVS users, though, must strictly adhere to the VTC Security Technical Implementation Guide requirements.

1.2 Periods Processing Overview

Periods Processing refers to the sanitization of sensitive information within a single CODEC under the following two conditions:

- When the CODEC is operating with classified and unclassified information at distinctly different times.
- When the CODEC is operated by different users with differing authorizations at distinctly different times.

Sensitive Information (Privacy Act Information to Classified Information) processed through a CODEC utilizing the DISN Network as a means of connectivity requires information sanitization procedures as outlined in Chapter 1 of this document.

1.2.1 Endpoint (CODEC) Operating at Multiple Classification Levels

This refers specifically to any CODEC used to process information of varying classification levels, as well as all associated equipment connected to that CODEC. During the period of processing (conference), all associated equipment will be at the appropriate classification

level prior to connection, and will remain at the appropriate classification level until the end of the conference. Upon conference completion, any equipment or devices that retain files and/or provide logging of information will be sanitized.

1.2.2 Multiple Users of the Same Endpoint

This refers to facilitators or customers who have varying classification levels or need-to-know authorizations operating endpoints at distinctly different periods. When a CODEC, or endpoint, is operated by multiple users with varying classification levels, and the endpoint retains files and/or provides logging of information, it must be sanitized prior to the start of a new period of processing with a new operator.

1.3 GVS Periods Processing Considerations

There are several considerations that should be addressed when operating on multiple networks utilizing a single CODEC. These considerations include type of video teleconferencing equipment, networks, and facilitator abilities, to information security as well as cost.

1.3.1 Equipment Considerations

Although different brands of CODECs are all designed to basically code and decode audio and video for video conferencing, the way in which they function is different in many cases. Some manufacturers use non-volatile memory to store CODEC parameters, while others use volatile memory or a combination of both. These parameters must be sanitized prior to switching between networks. GVS has identified a number of CODEC parameters which, at a minimum, must be sanitized when switching between networks occurs (see paragraph 1.4.4).

The user must understand that, depending on the manufacturer and the firmware version of the CODEC, it may or may not contain all of the parameters identified in this document. Therefore, it is necessary to contact the vendor or manufacturer of the CODEC to identify which parameters exist in order to specify which required sanitization process will be implemented.

1.3.2 Network Considerations

Depending on the types of networks utilized, periods processing may or may not be required.

1.3.2.1. CODECs operating on multiple non-secure dial-up networks are not required to conduct periods processing when switching between networks.

1.3.2.2. CODECs operating on non-secure dial-up and non-secure IP networks are not required to conduct periods processing when switching between networks.

1.3.2.3. CODECs operating on non-secure and secure dial-up networks ***are*** required to sanitize sensitive information when switching between secure and non-secure conferences.

1.3.2.4. CODECs operating on non-secure and secure IP networks ***are*** required to sanitize sensitive information when switching between secure and non-secure conferences.

1-3-2-5. CODECs operating as a hybrid (on non-secure / secure dial-up and non-secure / secure IP networks) ***are*** required to sanitize sensitive information when switching between either of the secure networks, or from either of the secure networks to one of the non-secure networks.

1.3.3 Periods Processing Methodologies

There are two Periods Processing methods. The first is Automatic Periods Processing, accomplished by software and hardware functions and which requires very little facilitator interaction. This option is very desirable, especially if facilitators have limited capabilities. The second option is manual Periods Processing, wherein the facilitator would manually reconfigure the CODEC. The second option, Manual Periods Processing, has several drawbacks, not the least of which is failed conferences.

1.3.3.1. Automatic Periods Processing: An automated process that sanitizes the CODEC without any facilitator involvement other than throwing a switch or pushing a button. Because the system is fully automated, there is a limited possibility of a security breach or a failed conference. This is an ideal option for those sites that don't have a dedicated facilitator or when a facilitator's abilities and time are limited. The drawback is the cost of purchasing and installing the specialized equipment required.

Refer to VTC STIG Vulnerability ID's: V-43015, V-43016, V-43018.

1.3.3.2. Manual Periods Processing: As its name implies, Manual Periods Processing is accomplished through intense interaction between the facilitator and the CODEC. All CODEC parameters listed in paragraph 1.4.4 will be changed manually by the facilitator. While the manual process is not as costly as the automatic option, it has significant drawbacks that offset the cost of the automatic periods processing system. Because success depends solely on the facilitator's ability and accuracy, the CODEC may be subject to security breaches or failed conferences due to inaccurate input from the facilitator.

Refer to VTC STIG Vulnerability ID's: V-43015, V-43016, V-43018.

1.3.4 Security of Information

The primary function of Periods Processing is to ensure the protection of sensitive information. For facilities operating on the GVS network, either a manual or automatic Periods Processing function must be accomplished when switching between classification levels on a single information system, when multiple users with differing security authorizations operate a single information system, or when multiple users with varying need-to-know levels operate a single system.

1.3.4.1. Multiple classification levels on a single system: All GVS facilities operating on multiple levels of classification (classified / unclassified) on a single endpoint (CODEC) that retains information in either volatile or non-volatile memory must ensure that all information retained is sanitized prior to conducting a conference at a different security level.

1.3.4.2. Multiple operators or customers using a single system: All GVS facilities that operate up to and including classified levels, and are operated by several facilitators or customers with varying levels of security clearances, are required to sanitize their CODECs

after each conference to ensure that information contained in either volatile or non-volatile memory is completely purged.

1.3.4.3. Users with varying need-to-know using a single system: Because of the large population using VTC facilities, it is virtually impossible for the facilitator to know who does or does not have the need-to-know information that may be archived within the CODEC from previous conferences. If the need-to-know of each participant can't be determined beyond a reasonable doubt, the CODEC must be sanitized prior to allowing those individuals entry into the VTC suite.

1.4 GVS Periods Processing Requirements and Procedures

Periods Processing requirements and procedures are the responsibility of the owners of the affected networks. In the case of GVS, the affected networks are those networks used by GVS customers to conduct video conferences. The networks used by GVS for video conferencing are a mix of government- and commercially-owned networks.

1.4.1 Government-owned Networks

1.4.1.1. DSN: The Defense System Network (DSN) is an Integrated Services Digital Network (ISDN) which incorporates both government and leased commercial lines. Although the DSN network incorporates both government and commercial lines, it is solely managed by the government.

1.4.1.2. FTS 2001: Federal Technology Service (FTS) provides Government agencies with up-to-date, cost-effective, and easy to utilize telecommunications services. It uses Integrated Services Digital Network (ISDN), which permits the integration of digital services over a single digital transmission path.

1.4.1.3. SIPRNet: The Secure Internet Protocol Router Network (SIPRNet) is a system of interconnected IP (H.323) networks used by the United States Department of Defense and the U.S. Department of State to transmit classified information (up to and including information classified SECRET) via the TCP/IP protocol.

1.4.1.4. NIPRNet: The Unsecure Internet Protocol Router Network (NIPRNet) is used to exchange sensitive but unclassified information between government agencies, as well as to provide users with access to the Internet. NIPRNet is composed of Internet Protocol routers owned by the United States Department of Defense (DOD).

1.4.2 Commercial Networks

Commercial ISDN/ISDN Basic Rate Interface (BRI): A service provided through commercial carriers which supply ISDN service to both civilian and government agencies. The service converts a standard analog copper wire telephone loop into a digital service with three logical channels–two 64k bearer channels for transmitting data and one 16K control channel.

1.4.3 Periods Processing Frequency Requirements

All agencies operating on the GVS network are required to conduct Periods Processing based on the criteria found in the Security of Information paragraph 1.3.4 and in the Video Tele-Conference STIG, Version 1, Release 3.

1.4.4 Periods Processing Data Element Sanitization Requirements

This section contains a list of data elements that require sanitization during Periods Processing.

Every particular manufacturer's various equipment components (including their different models and different firmware versions) may or may not contain each of these data elements. Each agency, then, must contact their vendor or CODEC manufacturer to determine which of the data elements are contained within their equipment components and the procedures to sanitize those differing elements. This descriptive list of data elements indicates the minimum of data elements that GVS requires to be sanitized during Periods Processing. Agencies may increase these minimum requirements, but must not lessen them.

1.4.4.1 - Static IP Address: A static IP address is one that is manually assigned to your CODEC by a network or network administrator. The result of this manual assignment is that your CODEC IP address always stays the same until you manually change it to something else.

1.4.4.2 - DHCP IP Address: Dynamic Host Configuration Protocol (DHCP) is a networking protocol used by devices (DHCP clients) which dynamically distributes the IP address to the destination host. DHCP automates network IP assignment to network devices from one or more DHCP servers.

1.4.4.3 - Corporate Address Book Addresses: The corporate address book is a listing of phone numbers and IP addresses of each CODEC within your organization.

1.4.4.4 - Global Address Book Addresses: The global address book is a listing of all phone numbers and IP addresses of each CODEC operating on the associated network.

1.4.4.5 - Gateway IP Address: A set of four grouped numbers separated by periods (e.g., 198.168.12.100) that uniquely identifies a Gateway on a given network.

1.4.4.6 - Gatekeeper Address: A set of four grouped numbers separated by periods (e.g., 198.168.12.100) that uniquely identifies a Gatekeeper on a given network.

1.4.4.7 - Endpoint IP Address: A set of four grouped numbers separated by periods (e.g., 198.168.12.100) that uniquely identifies an endpoint (CODEC) on a given network.

1.4.4.8 - SNMP Information: Simple Network Management Protocol (SNMP) consists of a set of standards for network management data which describe the system configuration.

1.4.4.9 - Subnet Mask Address: The process of subnetting is the division of a network into groups of endpoints. These groups are identified by four sets of numbers separated by periods (e.g., 255.255.255.0) that uniquely identify the group.

1.44.10 - DNS Information: The Domain Name System (DNS) makes it possible to assign domain names to groups of endpoints in a meaningful way, independent of each site's physical location. Domain names are easier to remember and can identify a site by name (e.g., forteustisroom1) rather than by an IP addresses.

1-4-4-11 - NAT Information: A Network Address Table (NAT) is used in the process of modifying network address information for the purpose of remapping a given address into another.

1.4.4.12 - SIP Address: Session Initiation Protocol (SIP) Address is a signaling protocol, widely used for controlling multimedia communication sessions over Internet Protocol (IP) and consists of a user domain name and port designations.

1.4.4.13 - SIP User Information: SIP User Information contains site address information including, but not limited to, a user name, domain name, IP routing, and port information.

1.4.4.14 - SIP Password: A SIP user password is used to authenticate an organization's SIP proxy server over the GVS IP network.

1.4.4.15 - CODEC Profiles (Alternate Configurations): CODEC profiles are a collection of characteristics that govern how an individual CODEC connects to a given network, as well as how voice, video, and encryption data is processed during a conference.

1.4.4.16 - Authorization Codes: Authorization Codes are a group of alpha or numeric characters that authorize a video conferencing site's entry into a conference which has controlled entry.

1.4.4.17 - H.323 Extensions: H.323 Extensions usually consist of several numbers much like an area code and phone number associated with an IP address. It is possible to use either the H.323 Alias (see "H.323 Alias ID" below) or the H.323 extension for dialing into a conference.

1.4.4.18 - H.323 Alias IDs: An H.323 Alias ID is either a descriptive identifier or a group of alphanumeric characters that are associated with an IP address. The Alias ID is used during the dialing sequence to keep the actual IP address from being displayed for security reasons.

1.4.4.19 - Alias Password: An Alias Password allows you to define a secondary password that provides another level of security. The alias password is especially useful when you may not want to reveal the 'real world' password to third parties.

1.4.4.20 - Call Manager IP Address: The Call Manager IP Address is the IP address used to communicate with an IP network's call processing component used to pass signaling to associated network endpoints and gateways.

1.4.5 Periods Processing Procedures

Periods Processing physical procedures will vary depending on whether the command has opted for an automatic process or a manual process. As stated in paragraphs 1.3.3.1 and 1.3.3.2, the automatic process has a very high degree of successful conference completion, while the manual process has more possibility of conference-related error based on facilitator abilities.

1.4.5.1. Automatic Periods Processing Procedures

To conduct automatic periods processing, one of several automated systems will have to be purchased and installed. Contact your account manager for a list of contractors that provide GVS-approved hardware for Periods Processing.

a. Based on the manufacturer and module selected, the Periods Processing sequence will be initiated by the facilitator or other responsible individual by a remote switch or button on a touch panel.

b. For the most part, the actual automatic process is transparent to the operator but, depending on the hardware selected, may give visual prompts providing general progress information.

c. During the automatic process, the CODEC will be disconnected from any available networks. Once the CODEC is isolated from any attached networks, the required data elements discussed earlier in this document will be automatically cleared and new data elements (for the new network) will be inserted.

d. The CODEC will be forced into a reboot to ensure that any residual data elements are cleared. Depending on the hardware installed, the CODEC may be rebooted several times during the automatic process.

e. Once the old network information has been purged, the new network data written and the reboot sequence(s) completed, the network will be reconnected. At this point, the system has been reconfigured and is ready for the new conference.

1.4.5.2. Manual Periods Processing Procedures: Manual Periods Processing is as its name implies; it is accomplished by direct facilitator interface with the CODEC, fiber optic switch, and media converters. Due to security concerns of classified information being retained after a manual process has been completed, one of the following processes must be utilized. The processes described below discuss the physical actions of the facilitator when switching between networks. It doesn't contain the vendor-specific actions of sanitizing the actual CODEC (see paragraph 1.3.1).

1.4 5 3. Manual Periods Processing using a Laptop Computer: When using a laptop computer (authorized to process classified information) to perform Manual Periods Processing, follow the sequence outlined below. The sequence outlined is limited to the physical process of sanitization and doesn't contain the vendor-specific CODEC sanitization process, nor do the data elements (please review paragraph 1-4-4 for a listing of the data elements requiring sanitization).

a. Disable local room controller from the CODEC (AMX / Crestron, etc) if applicable.

b. Power off all Fiber Optic Modems (FOM):
   - Power off FOM to dial-up network, if applicable.
   - Power off FOM to NIPRNet network, if applicable.
   - Power off FOM to SIPRNet network, if applicable.
   - Power off FOM between fiber optic switch and CODEC.

c. Set the fiber optic switch to the unused port (normally the B port if installed correctly).

d. Set the CODEC network setting to “No Network” and verify that the change was saved.

e. Ensure that, if there are direct ISDN lines connected to the CODEC, they are removed or that an approved switch has been installed and is switched to the off position (Red to Black Issue).

f. Set Red and Black switches (RS-530 switches) to the secure mode.

g. Connect the laptop computer to the RS-232 port on the back of the CODEC.

h. Enable the HTTP setting in the CODEC. The HTTP setting would be normally set to disable if the CODEC is compliant to the VTC STIG (see chapter 2).

i. Based on the information received from the vendor concerning what data elements are retained in your CODEC and the procedures to clear those data elements, clear and add ‘bogus’ (fictitious) entries for each of the following as applicable. This is because most CODECs retain the last set of data elements in the user profiles located in the non-volatile memory.

- Endpoint IP
- DHCP IP
- Gateway IP
- Gatekeeper IP
- Far end IP
- Subnet mask IP
- DNS data
- NAT data
- SIP address
- H.323 extensions
- Call manager IP
- All passwords (SIP, Alias)
- Clear all address book entries if address books are not already disabled.

j. Reboot the CODEC.

k. Based on the information received from the vendor concerning what data elements are retained in your CODEC and the procedures to clear those data elements, clear and add the correct entries for the network to be used.

l. Reboot the CODEC.

m. Verify that the new entries within the CODEC.

n. Disconnect the laptop computer.

o. Reestablish room control connection with the CODEC.

p. Disable HTTP setting within the CODEC.

q. Set Red and Black switches to proper setting based on the network you are going to connect to.

r. Reset the CODEC network setting to the selected network.

s. Power on the FOM from the fiber optic switch to the CODEC.

t. Power on the FOM for the selected network.

u. Ensure that FOMs for the unselected networks are powered off.

v. Connect to the conference.

1.4.5.4. Periods Processing using the Remote Control (touch panel not in system):
The sequence outline is limited to the physical process and doesn't contain the vendor specific CODEC sanitization nor data elements that require sanitization (review paragraph 1.4.4).

a. Power off all Fiber Optic Modems (FOM)

- Power off FOM to dial-up network, if applicable.
- Power off FOM to NIPRNet network, if applicable.
- Power off FOM to SIPRNet network, if applicable.
- Power off FOM between fiber optic switch and CODEC.

b. Set the fiber optic switch to the unused port (normally the B port if installed correctly).

c. Set the CODEC network setting to "No Network" and verify that the change was saved.

d. Ensure that, if there are direct ISDN lines connected to the CODEC, they are removed, or that an approved switch has been installed and is switched to the off position (Red Black Issue).

e. Set Red and Black switches (RS-530 switches) to the secure mode.

f. Based on the information received from the vendor concerning what data elements are retained in your CODEC, and the procedures to clear those data elements, clear and add 'bogus' (fictitious) entries for each of the following as applicable. This is because most CODECs retain the last set of data elements in the user profiles located in the nonvolatile memory.

- Endpoint IP
- DHCP IP
- Gateway IP
- Gatekeeper IP
- Far end IP
- Subnet mask IP
- DNS data

- NAT data
- SIP address
- H.323 extensions
- Call manager IP
- All passwords (SIP, Alias)
- Clear all address book entries if address books are not already disabled.

g. Reboot the CODEC.

h. Based on the information received from the vendor concerning what data elements are retained in your CODEC and the procedures to clear those data elements, clear and add the correct entries for the network to be used.

i. Reboot the CODEC.

j. Verify the new entries within the CODEC.

k. Set Red and Black switches to the proper setting based on the network you are going to connect to.

l. Reset the CODEC network setting to the selected network.

m. Power on the FOM from the fiber optic switch to the CODEC.

n. Power on the FOM for the selected network.

o. Ensure that FOMs for the unselected networks are powered off.

p. Connect to the conference.

1.4.5.5. Manual Periods Processing using a Touch Panel (AMX, Crestron, etc.): GVS doesn't authorize the use of a touch panel for Manual Periods Processing, as the integrated controller used by the various manufacturers of touch panels retain information concerning CODEC configurations that are accessible from outside sources. To preclude loss of sensitive information, sites utilizing Manual Periods processing will use either of the two options listed above (laptop computer or vendor-supplied remote control).

1.5 Questions and Comments Concerning Periods Processing

Questions and/or comments concerning requirements discussed in this policy document concerning Periods Processing should be addressed to your GVS Account Manager.

2 VTC SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)

2.1 Background

The Video Teleconferencing (VTC) Security Technical Implementation Guide (STIG) provides the architectural and technical security policies, requirements, and implementation details for applying security concepts to video teleconferencing systems.

All GVS users and sites must strictly adhere to all of the requirements specified in the VTC STIG.

2.2 Access to VTC STIG

The current VTC STIG is Version 1, Release 4, dated 24 October 2014. It can be downloaded from the following URL:

http://iase.disa.mil/stigs/Pages/index.aspx