

cyber**protection**

PROGRAM From
Tyco Security Products

VideoEdge

DISA Security Requirements

General Purpose Operating System

VideoEdge v4.8



Defense Information Systems Agency
Department of Defense

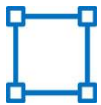
Proactively Monitoring and Managing Cybersecurity Risks

Not all security manufacturers' cyber security programs are equal because not all engineering teams are equal. Our autonomous Cyber Protection Team, an independent branch of Tyco Security Products development group, has deep process control knowledge and specialized expertise in cyber concerns with physical security systems. With the authority and responsibility of managing the Cyber Protection Program, the team uses best practices to monitor compliance:



Secure Product Development Practices

With secure coding and testing backgrounds, our highly trained engineers minimize the possibility of inadvertently introducing vulnerabilities during product development.



Inclusive Protection of Components and Systems

Our holistic approach includes the ability to secure systems with a range of capabilities to complement diverse security needs. For example, a C·CURE 9000 and iSTAR access control system can be configured to support some of the most stringent controls necessary for secure network communication.



Configuration Guidelines for Compliance

We provide comprehensive guidelines on how to configure C·CURE 9000, VideoEdge and victor systems to assist customers in complying with their identified regulatory requirements.



Testing Procedures

The Cyber Protection Team employs rigorous, continuous testing, both internally and with an independent test house, to minimize the risk of introducing new vulnerabilities to software updates and new configurations of our cyber program-compliant products..



Rapid Response to Vulnerabilities

When a vulnerability is announced, the team quickly assesses the situation, distributes an advisory bulletin, and follows up with fully qualified patches.



Education and Advocacy

In addition to maintaining critical training and development certifications, our Cyber Protection Team travels the world, speaking and advocating for the rigorous protection of all security systems.

Overview

To assist installations within the Department of Defense in meeting the security hardening requirements of the Defense Information Systems Agency (DISA), Tyco Security Products has developed this System Security Requirements guide based on the DISA General Purpose operating Systems STG, Version 1, Release 3 published 22 January 2016, for the sole purposes of meeting said requirements for the VideoEdge Network Video Recorder (NVR) appliance. We have provided the 250 technical control requirements of the General Purpose Operating System Security Requirements Guide (SRG) as well as a description of how a VideoEdge device meets the technical controls or if it does not meet the controls, guidance has been provided so the customer can configure VideoEdge to meet the requirements.

This document covers all VideoEdge devices with version 4.6 and higher.

If you have any questions or comments, please reach out to the contact information below.

William L Brown Jr. / Sr. Engineering Manager /
/ Regulatory and Product Security /
/ willbrown@tycoint.com /

DISCLAIMER

This document is being provided for informational purposes only, and is not intended as, and shall not constitute, legal advice. Compliance with any law or regulation is solely the responsibility of the user, and Tyco strongly cautions users to seek the advice of qualified legal counsel on such matters. The inclusion of information herein shall not be considered a determination that any portion of any law or regulation is applicable to any specific user or that the implementation of any of the system configuration settings discussed herein will bring a user or their system into full compliance with any law or regulation. This document is current as of its date of issuance, and Tyco does not undertake any obligation to update or supplement the information contained herein due to any changes in law, regulation or otherwise.

THIS DOCUMENT IS BEING PROVIDED “AS IS”, WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TYCO EXPRESSLY DISCLAIMS ANY AND ALL SUCH WARRANTIES (INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY), FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL TYCO BE LIABLE FOR ANY DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF FUTURE SALES, LOSS OF PROFITS OR GOODWILL, LOSS OF DATA OR LOSS OF USE. The foregoing disclaimers and limitations shall apply to the maximum extent permitted by applicable law.

Rule Version (STIG-ID): SRG-OS-000001-GPOS-00001

Rule Title: The operating system must provide automated mechanisms for supporting

Account management functions include: assigning group or role membership; identifying account type; specifying user access authorizations (i.e., privileges); account removal, update, or termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000002-GPOS-00002

Rule Title: The operating system must automatically remove or disable temporary user accounts after 72 hours.

VideoEdge: Compliant

Accounts may also be set to automatically lock if not used within a set period of time, e.g., to ensure ex-employee accounts are disabled. When login is attempted after this time period, the account is locked and may only be unlocked by an administrator.

Rule Version (STIG-ID): SRG-OS-000004-GPOS-00004

Rule Title: The operating system must audit all account creations.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create an account. Auditing account creation actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems may be integrated with enterprise level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

VideoEdge has enhanced security logging, audit trail and email alerts which track things such as the creation of user accounts.

Rule Version (STIG-ID): SRG-OS-000021-GPOS-00005

Rule Title: The operating system must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

VideoEdge: Compliant

User accounts for VideoEdge Administrator Interface and VideoEdge Client may be set to permanently or temporarily lock after a configurable number of invalid login attempts.

Rule Version (STIG-ID): SRG-OS-000023-GPOS-00006

Rule Title: The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system.

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters.

VideoEdge: Compliant

The System Use Banner can be configured to display an approved system use notification message or banner before the user logs on to the system either locally or remotely. It also can be used to provide privacy and security notices consistent with applicable federal laws, executive orders, directives, polices, regulations, standards, and guidance.

Rule Version (STIG-ID): SRG-OS-000024-GPOS-00007

Rule Title: The operating system must display the Standard Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions and take explicit actions to log on for further access.

VideoEdge: Compliant

The System Use Banner can be configured to display an approved system use notification message or banner before the user logs on to the system either locally or remotely. It also can be used to provide privacy and security notices consistent with applicable federal laws, executive orders, directives, polices, regulations, standards, and guidance.

Rule Version (STIG-ID): SRG-OS-000027-GPOS-00008

Rule Title: The operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.

Vulnerability Discussion: Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

VideoEdge: Partial Compliance

Currently VideoEdge does not have a session lock feature, but can be easily implemented with a third party software such as Userlock.

Rule Version (STIG-ID): SRG-OS-000028-GPOS-00009

Rule Title: The operating system must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

VideoEdge: Partial Compliance

Currently VideoEdge does not have a session lock feature, but can be easily implemented with a third party software such as Userlock.

Rule Version (STIG-ID): SRG-OS-000029-GPOS-00010

Rule Title: The operating system must initiate a session lock after a 15-minute period of inactivity for all connection types.

Vulnerability Discussion: A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to

vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

VideoEdge: Compliant

VideoEdge Administrator Interface user accounts can be configured to automatically log out the user after a configurable period of inactivity (between 5 and 60 minutes).

Rule Version (STIG-ID): SRG-OS-000030-GPOS-00011

Rule Title: The operating system must provide the capability for users to directly initiate a session lock for all connection types.

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, operating systems need to provide users with the ability to manually invoke a session lock so users may secure their session should the need arise for them to temporarily vacate the immediate physical vicinity.

VideoEdge: Compliant

VideoEdge Administrator Interface user accounts can be configured to automatically log out the user after a configurable period of inactivity (between 5 and 60 minutes). The client machine that users will access the VideoEdge webpage with, such as a windows pc or server has the ability to lock the session.

Rule Version (STIG-ID): SRG-OS-000031-GPOS-00012

Rule Title: The operating system must conceal, via the session lock, information previously visible on the display with a publicly viewable image.

Vulnerability Discussion: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. The operating system session lock event must include an obfuscation of the display screen so as to prevent other users from reading what was previously displayed.

Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

VideoEdge: Partial Compliance

VideoEdge does not offer this feature, but Windows operating system, which User's will utilize to access the VideoEdge webpage meets SRG-OS-000031-GPOS-00012.

Rule Version (STIG-ID): SRG-OS-000032-GPOS-00013

Rule Title: The operating system must monitor remote access methods.

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system. VideoEdge supports remote access from authorized system components. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge.

Rule Version (STIG-ID): SRG-OS-000033-GPOS-00014

Rule Title: The operating system must implement DoD-approved encryption to protect the confidentiality of remote access sessions.

Vulnerability Discussion: Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Encryption provides a means to secure the remote connection to prevent unauthorized access to the data traversing the remote access connection (e.g., RDP), thereby providing a degree of confidentiality. The encryption strength of a mechanism is selected based on the security categorization of the information.

VideoEdge: Compliant

When HTTPS is enabled, web GUI commands are transferred using TLS (Transport Layer Security) with AES 256 bit encryption. Data is transferred using SSL (Secure Socket Layer) with AES 256 bit encryption

Rule Version (STIG-ID): SRG-OS-000037-GPOS-00015

Rule Title: The operating system must produce audit records containing information to establish what type of events occurred.

Vulnerability Discussion: Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

VideoEdge: Compliant

Logs track general system operation and are useful for troubleshooting and incident investigation. The VideoEdge system generates a number of different log files to track areas such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation. These logs are useful in monitoring the general operation of the Linux system. The VideoEdge system also generates a number of application-specific log files to aid in diagnosing areas such as camera communication and video playback events. Log backup to an external server is supported.

Rule Version (STIG-ID): SRG-OS-000038-GPOS-00016

Rule Title: The operating system must produce audit records containing information to establish when (date and time) the events occurred.

Vulnerability Discussion: Without establishing when events occurred, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

In order to compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know when events occurred (date and time).

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

VideoEdge: Compliant

Category	Log
info	Dec 2 14:51:23 info [SECURITY CONFIG] Successfully changed password for user operator. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed the enhanced password validation settings for role operator to 0. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed inactivity lockout interval for role operator to 30. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed auto logout for role operator to 0. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed login retry limit for role operator to 3. Remote user=admin, ip=192.168.200.80
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed lockout policy for role operator to 1. Remote user=admin, ip=192.168.200.80
info	Dec 2 12:37:14 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:37:01 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:35:27 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:35:24 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:32:55 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80
info	Dec 2 12:32:38 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80

Rule Version (STIG-ID): SRG-OS-000039-GPOS-00017

Rule Title: The operating system must produce audit records containing information to establish where the events occurred.

Vulnerability Discussion: Without establishing where events occurred, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

In order to compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know where events occurred, such as operating system components, modules, device identifiers, node names, file names, and functionality.

Associating information about where the event occurred within the operating system provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

VideoEdge: Compliant

Logs track general system operation and are useful for troubleshooting and incident investigation. The VideoEdge system generates a number of different log files to track areas such as general system operation, web server operation, web server errors, and Network time Protocol (NTP) operation.

Rule Version (STIG-ID): SRG-OS-000040-GPOS-00018

Rule Title: The operating system must produce audit records containing information to establish the source of the events.

Vulnerability Discussion: Without establishing the source of the event, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack.

In addition to logging where events occur within the operating system, the operating system must also generate audit records that identify sources of events. Sources of operating system events include, but are not limited to, processes and services.

In order to compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know the source of the event.

VideoEdge: Compliant

Category	Log
notice	Jan 25 03:29:58 notice sudo: wwwrun : TTY=unknown ; PWD=/var/lib/wwwrun ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/dump_logs.py --audit
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
notice	Jan 25 03:29:51 notice sudo: wwwrun : TTY=unknown ; PWD=/var/lib/wwwrun ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/dump_logs.py --audit
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth3
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth2
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth1
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth0
err	Jan 25 03:29:42 err sshd[14417]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:42 err sshd[14417]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10

Rule Version (STIG-ID): SRG-OS-000041-GPOS-00019

Rule Title: The operating system must produce audit records containing information to establish the outcome of the events.

Vulnerability Discussion: Without information about the outcome of events, security personnel cannot make an accurate assessment as to whether an attack was successful or if changes were made to the security state of the system.

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). As such, they also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response.

VideoEdge: Compliant

Category	Log
notice	Jan 25 03:29:58 notice sudo: wwwrun : TTY=unknown ; PWD=/var/lib/wwrun ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/dump_logs.py --audit
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:57 err sshd[15229]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:52 err sshd[15150]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
notice	Jan 25 03:29:51 notice sudo: wwwrun : TTY=unknown ; PWD=/var/lib/wwrun ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/dump_logs.py --audit
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:47 err sshd[15033]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth3
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth2
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth1
notice	Jan 25 03:29:46 notice sudo: root : TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/opt/americandynamics/venvr/django/rootaccess/scripts/system_file_read.py /etc/sysconfig/network/ifcfg-eth0
err	Jan 25 03:29:42 err sshd[14417]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10
err	Jan 25 03:29:42 err sshd[14417]: error: PAM: Authentication failure for VideoEdge from 10.38.180.10

Rule Version (STIG-ID): SRG-OS-000042-GPOS-00020

Rule Title: The operating system must generate audit records containing the full-text recording of privileged commands.

Vulnerability Discussion: Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

VideoEdge: Compliant

VideoEdge provides audit records that contain the full-text recordings of privileged commands in the logs under Event Logs and Audit trail tabs.

Rule Version (STIG-ID): SRG-OS-000042-GPOS-00021

Rule Title: The operating system must produce audit records containing the individual identities of group account users.

Vulnerability Discussion: Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the individual identities of group users. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the actual account involved in the activity.

VideoEdge: Compliant

VideoEdge provides audit records containing the individual identities of a group account user in the logs under Event Logs and Audit trail tabs.

Rule Version (STIG-ID): SRG-OS-000046-GPOS-00022

Rule Title: The operating system must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.

Vulnerability Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to

assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000047-GPOS-00023

Rule Title: The operating system must shut down by default upon audit failure (unless availability is an overriding concern).

Vulnerability Discussion: It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include: software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

- 1) If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.
- 2) If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

VideoEdge: Non-Compliant, but mitigated

VideoEdge may be configured to only allow administrative access. The victor application contains the user functionality needed for guard and surveillance responsibilities removing the need for user accounts to the VideoEdge appliance itself.

Rule Version (STIG-ID): SRG-OS-000051-GPOS-00024

Rule Title: The operating system must provide the capability to centrally review and analyze audit records from multiple components within the system.

Vulnerability Discussion: Successful incident response and auditing relies on timely, accurate system information and analysis in order to allow the organization to identify and respond to potential incidents in a proficient manner. If the operating system does not provide the ability to centrally review the operating system logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and log event alarming difficult to implement and manage, particularly when the system has multiple logging components writing to different locations or systems.

To support the centralized capability, the operating system must be able to provide the information in a format that can be extracted and used, allowing the application performing the centralization of the log records to meet this requirement.

VideoEdge: Compliant

Audit trails keep track of system configuration operations including the configuration of information security controls. This aspect of the VideoEdge system is being continually improved. An audit log interrogation tool is provided as part of the VideoEdge Administrator Interface. This allows audit events to be queried by severity and searched using a text filter.

Rule Version (STIG-ID): SRG-OS-000054-GPOS-00025

Rule Title: The operating system must provide the capability to filter audit records for events of interest based upon all audit fields within audit records.

Vulnerability Discussion: The ability to specify the event criteria that are of interest provides the individuals reviewing the logs with the ability to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

Events of interest can be identified by the content of specific audit record fields, including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component.

This requires operating systems to provide the capability to customize audit record reports based on all available criteria.

VideoEdge: Compliant

Retrieve Logs	Log Management	Event Logs	Connection	Device Logs	Audit Trail
Log Filters					
Error <input checked="" type="checkbox"/>	Alert <input checked="" type="checkbox"/>	Notice <input type="checkbox"/>	Info <input checked="" type="checkbox"/>	Filter Text SECURITY	<input type="button" value="Apply"/>
Category	Log				
info	Dec 2 14:51:23 info [SECURITY CONFIG] Successfully changed password for user operator. Remote user=admin, ip=192.168.200.80				
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed the enhanced password validation settings for role operator to 0. Remote user=admin, ip=192.168.200.80				
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed inactivity lockout interval for role operator to 30. Remote user=admin, ip=192.168.200.80				
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed auto logout for role operator to 0. Remote user=admin, ip=192.168.200.80				
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed login retry limit for role operator to 3. Remote user=admin, ip=192.168.200.80				
info	Dec 2 14:50:05 info [SECURITY CONFIG] Successfully changed lockout policy for role operator to 1. Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:37:14 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:37:01 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:35:27 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: enabled Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:35:24 info [SECURITY CONFIG] Re-configuring service: VNC, Action: disabled, New status: disabled Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:32:55 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80				
info	Dec 2 12:32:38 info [SECURITY CONFIG] Re-configuring service: VNC, Action: enabled, New status: disabled Remote user=admin, ip=192.168.200.80				

Rule Version (STIG-ID): SRG-OS-000055-GPOS-00026

Rule Title: The operating system must use internal system clocks to generate time stamps for audit records.

Vulnerability Discussion: Without an internal clock used as the reference for the time stored on each event to provide a trusted common reference for the time, forensic analysis would be impeded. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

If the internal clock is not used, the system may not be able to provide time stamps for log messages. Additionally, externally generated time stamps may not be accurate.

VideoEdge: Compliant

VideoEdge uses the internal clock on the SUSE Linux Enterprise Server (SLES) the local operating system to generate time stamps for audit logs.

Rule Version (STIG-ID): SRG-OS-000057-GPOS-00027

Rule Title: The operating system must protect audit information from unauthorized read access.

Vulnerability Discussion: Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit operating system activity.

VideoEdge: Compliant

An audit log interrogation tool is provided as part of the VideoEdge Administrator Interface. Restriction of ports, protocols, and services to only those required to support VideoEdge functionality.

Rule Version (STIG-ID): SRG-OS-000058-GPOS-00028

Rule Title: The operating system must protect audit information from unauthorized modification.

Vulnerability Discussion: If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized modification.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

VideoEdge: Compliant

The VideoEdge audit record databases are write-only databases. Access is restricted to authorized accounts.

Rule Version (STIG-ID): SRG-OS-000059-GPOS-00029

Rule Title: The operating system must protect audit information from unauthorized deletion.

Vulnerability Discussion: If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized deletion. This requirement can be achieved through multiple methods, which will depend upon system architecture and design.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

VideoEdge: Compliant

The VideoEdge audit record databases are write-only databases. Access is restricted to authorized accounts.

Rule Version (STIG-ID): SRG-OS-000062-GPOS-00031

Rule Title: The operating system must provide audit record generation capability for DoD-defined auditable events for all operating system components.

Vulnerability Discussion: Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

- 1) Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);

- 2) Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;

- 3) All account creations, modifications, disabling, and terminations; and
- 4) All kernel module load, unload, and restart actions.

VideoEdge: Compliant

VideoEdge audits user session events including log in and log out. VideoEdge audits system administrative actions and correlates the actions to the user that performed them. VideoEdge audits operational events of the system. VideoEdge audits client actions performed or attempted as part of the system's usage. VideoEdge audits server actions.

Rule Version (STIG-ID): SRG-OS-000063-GPOS-00032

Rule Title: The operating system must allow only the ISSM (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.

Vulnerability Discussion: Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

VideoEdge: Compliant

The VideoEdge server separates roles based on responsibilities such as admin access, operator access, general system configuration, software installation, access to PTZ and clip export features.

Rule Version (STIG-ID): SRG-OS-000064-GPOS-00033

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to access privileges occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

In support of this control, VideoEdge generates auditable events for security configuration changes, user login and logout events, account lockout events, system administrative actions, server events, client actions and system operational events.

Rule Version (STIG-ID): SRG-OS-000066-GPOS-00034

Rule Title: The operating system, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Vulnerability Discussion: Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

VideoEdge: Compliant

VideoEdge NVRs allow you to create a certificate that is tailored to the individual NVR so that its identity can be verified by your web browser or victor Client. The certificate can be self-signed, or for more security-conscious customers, it can be signed by a trusted certificate authority such as Thawte or Verisign. VideoEdge certificates use 2048-bit keys.

Rule Version (STIG-ID): SRG-OS-000067-GPOS-00035

Rule Title: The operating system, for PKI-based authentication, must enforce authorized access to the corresponding private key.

Vulnerability Discussion: If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and non-repudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

VideoEdge: Not Applicable

This control is the responsibility of the organization. In support of this control, the VideoEdge platform may provide mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000068-GPOS-00036

Rule Title: The operating system must map the authenticated identity to the user or group account for PKI-based authentication.

Vulnerability Discussion: Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

VideoEdge: Not Applicable

This control is the responsibility of the organization. In support of this control, the VideoEdge platform may provide mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000069-GPOS-00037

Rule Title: The operating system must enforce password complexity by requiring that at least one upper-case character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

VideoEdge: Compliant

VideoEdge NVRs ship with preset passwords on all accounts. When activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords
- Passwords must differ from the previous password by a minimum of three characters
- Passwords must be a minimum of seven characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

Rule Version (STIG-ID): SRG-OS-000070-GPOS-00038

Rule Title: The operating system must enforce password complexity by requiring that at least one lower-case character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

VideoEdge: Compliant

VideoEdge NVRs ship with preset passwords on all accounts. When activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords
- Passwords must differ from the previous password by a minimum of three characters
- Passwords must be a minimum of seven characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

Rule Version (STIG-ID): SRG-OS-000071-GPOS-00039

Rule Title: The operating system must enforce password complexity by requiring that at least one numeric character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

VideoEdge: Compliant

VideoEdge NVRs ship with preset passwords on all accounts. When activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords
- Passwords must differ from the previous password by a minimum of three characters

- Passwords must be a minimum of seven characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

Rule Version (STIG-ID): SRG-OS-000072-GPOS-00040

Rule Title: The operating system must require the change of at least 50% of the total number of characters when passwords are changed.

Vulnerability Discussion: If the operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

If the password length is an odd number then number of changed characters must be rounded up. For example, a password length of 15 characters must require the change of at least 8 characters.

VideoEdge: Compliant

VideoEdge NVRs ship with preset passwords on all accounts. When activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords

- Passwords must differ from the previous password by a minimum of three characters

Passwords must be a minimum of seven characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

Rule Version (STIG-ID): SRG-OS-000073-GPOS-00041

Rule Title: The operating system must store only encrypted representations of passwords.

Vulnerability Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

VideoEdge: Not Applicable

This control is the responsibility of the organization. In support of this control, VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000074-GPOS-00042

Rule Title: The operating system must transmit only encrypted representations of passwords.

Vulnerability Discussion: Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

VideoEdge: Not Applicable

This control is the responsibility of the organization. In support of this control, VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000075-GPOS-00043

Rule Title: Operating systems must enforce 24 hours/1 day as the minimum password lifetime.

Vulnerability Discussion: Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

VideoEdge: Not Applicable

This control is the responsibility of the organization. This can be implemented using a GPO and will be enforced for users authenticating to the domain. In support of this control, VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000076-GPOS-00044

Rule Title: Operating systems must enforce a 60-day maximum password lifetime restriction.

Vulnerability Discussion: Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

VideoEdge: Not Applicable

This control is the responsibility of the organization. This can be implemented using a GPO and will be enforced for users authenticating to the domain. VideoEdge can be joined to an Active Directory domain, with LDAP, which supports automated account management and authentication. VideoEdge Linux accounts are also capable of being joined to an Active Directory domain. VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000077-GPOS-00045

Rule Title: The operating system must prohibit password reuse for a minimum of five generations.

Vulnerability Discussion: Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed as per policy requirements.

VideoEdge: Not Applicable

This control is the responsibility of the organization. This can be implemented using a GPO and will be enforced for users authenticating to the domain. VideoEdge can be joined to an Active Directory domain, with LDAP, which supports automated account management and authentication. VideoEdge Linux accounts are also capable of being joined to an Active Directory domain. VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000078-GPOS-00046

Rule Title: The operating system must enforce a minimum 15-character password length.

Vulnerability Discussion: The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

VideoEdge: Not Applicable

This control is the responsibility of the organization. This can be implemented using a GPO and will be enforced for users authenticating to the domain. VideoEdge can be joined to an Active Directory domain, with LDAP, which supports automated account management and authentication. VideoEdge Linux accounts are also capable of being joined to an Active Directory domain. VideoEdge provides mechanisms to support this control.

Rule Version (STIG-ID): SRG-OS-000079-GPOS-00047

Rule Title: The operating system must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Vulnerability Discussion: To prevent the compromise of authentication information, such as passwords during the authentication process, the feedback from the operating system shall not provide any information allowing an unauthorized user to compromise the authentication mechanism.

Obfuscation of user-provided information that is typed into the system is a method used when addressing this risk.

For example, displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

VideoEdge: Compliant

Passwords are not showing in plain text. VideoEdge obscures user passwords when they are being input for authentication.

Rule Version (STIG-ID): SRG-OS-000080-GPOS-00048

Rule Title: The operating system must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Vulnerability Discussion: To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DoD-approved PKIs, all DoD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Access control policies include: identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include: access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

VideoEdge: Compliant

The organization is responsible for determining the access control policy and procedures. VideoEdge functionality supports access control policies.

Rule Version (STIG-ID): SRG-OS-000095-GPOS-00049

Rule Title: The operating system must be configured to disable non-essential capabilities.

Vulnerability Discussion: It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software, not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

VideoEdge: Compliant

VideoEdge NVR appliance comes with only essential software to operate.

Rule Version (STIG-ID): SRG-OS-000096-GPOS-00050

Rule Title: The operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

Vulnerability Discussion: In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

VideoEdge: Compliant

The principle of least functionality is implemented, only ports and services to run the NVR appliance are enabled. An administrator can turn off any other port or service to further lock down the system and once disabled only an admin can enable the port or service.

Rule Version (STIG-ID): SRG-OS-000104-GPOS-00051

Rule Title: The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users).

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

- 1) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and
- 2) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000105-GPOS-00052

Rule Title: The operating system must use multifactor authentication for network access to privileged accounts.

Vulnerability Discussion: Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include:

- 1) something a user knows (e.g., password/PIN);
- 2) something a user has (e.g., cryptographic identification device, token); and
- 3) something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the Internet).

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000106-GPOS-00053

Rule Title: The operating system must use multifactor authentication for network access to non-privileged accounts.

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, non-privileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include:

- 1) Something you know (e.g., password/PIN);
- 2) Something you have (e.g., cryptographic identification device, token); and
- 3) Something you are (e.g., biometric).

A non-privileged account is any information system account with authorizations of a non-privileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where said access is obtained through a network connection.

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000107-GPOS-00054

Rule Title: The operating system must use multifactor authentication for local access to privileged accounts.

Vulnerability Discussion: To assure accountability and prevent unauthenticated access, privileged users must utilize multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication is defined as using two or more factors to achieve authentication.

Factors include:

- 1) Something you know (e.g., password/PIN);
- 2) Something you have (e.g., cryptographic identification device, token); and
- 3) Something you are (e.g., biometric).

A privileged account is defined as an operating system account with authorizations of a privileged user.

Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000108-GPOS-00055

Rule Title: The operating system must use multifactor authentication for local access to non-privileged accounts.

Vulnerability Discussion: To assure accountability, prevent unauthenticated access, and prevent misuse of the system, non-privileged users must utilize multifactor authentication for local access.

Multifactor authentication is defined as using two or more factors to achieve authentication.

Factors include:

- 1) Something you know (e.g., password/PIN);
- 2) Something you have (e.g., cryptographic identification device or token); and
- 3) Something you are (e.g., biometric).

A non-privileged account is defined as an operating system account with authorizations of a regular or non-privileged user.

Local access is defined as access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

The DoD CAC with DoD-approved PKI is an example of multifactor authentication.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000109-GPOS-00056

Rule Title: The operating system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator.

Vulnerability Discussion: To assure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows operating systems offer a 'switch user' capability allowing users to authenticate with their individual credentials and, when needed, 'switch' to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge provides accounts at the application and operating system level. Application accounts are grouped into role-based access permissions. Access to the information system requires authentication prior to granting access. Guest accounts are disabled.

Rule Version (STIG-ID): SRG-OS-000112-GPOS-00057

Rule Title: The operating system must implement replay-resistant authentication mechanisms for network access to privileged accounts.

Vulnerability Discussion: A replay attack may enable an unauthorized user to gain access to the operating system. Authentication sessions between the authenticator and the operating system validating the user credentials must not be vulnerable to a replay attack.

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

A privileged account is any information system account with authorizations of a privileged user.

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000113-GPOS-00058

Rule Title: The operating system must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.

Vulnerability Discussion: A replay attack may enable an unauthorized user to gain access to the operating system. Authentication sessions between the authenticator and the operating system validating the user credentials must not be vulnerable to a replay attack.

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

A non-privileged account is any operating system account with authorizations of a non-privileged user.

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000114-GPOS-00059

Rule Title: The operating system must uniquely identify peripherals before establishing a connection.

Vulnerability Discussion: Without identifying devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000118-GPOS-00060

Rule Title: The operating system must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

Vulnerability Discussion: Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

VideoEdge: Compliant

Accounts may also be set to automatically lock if not used within a set period of time, e.g., to ensure ex-employee accounts are disabled. When login is attempted after this time period, the account is locked and may only be unlocked by an administrator.

Rule Version (STIG-ID): SRG-OS-000120-GPOS-00061

Rule Title: The operating system must use mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Vulnerability Discussion: Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000121-GPOS-00062

Rule Title: The operating system must uniquely identify and must authenticate non-organizational users (or processes acting on behalf of non-organizational users).

Vulnerability Discussion: Lack of authentication and identification enables non-organizational users to gain access to the application or possibly other information systems and provides an opportunity for intruders to compromise resources within the application or information system.

Non-organizational users include all information system users other than organizational users, which include organizational employees or individuals the organization deems to have equivalent status of an employee (e.g., contractors and guest researchers).

Non-organizational users shall be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization when related to the use of anonymous access.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system. VideoEdge is capable of providing unique identification for non-organizational users. It is the responsibility of the organization to configure the systems to support this requirement.

Rule Version (STIG-ID): SRG-OS-000122-GPOS-00063

Rule Title: The operating system must provide an audit reduction capability that supports on-demand reporting requirements.

Vulnerability Discussion: The ability to generate on-demand reports, including after the audit data has been subjected to audit reduction, greatly facilitates the organization's ability to generate incident reports as needed to better handle larger-scale or more complex security incidents.

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. The report generation capability provided by the application must support on-demand (i.e., customizable, ad hoc, and as-needed) reports.

VideoEdge: Compliant

VideoEdge's audit functionality supports this control.

Rule Version (STIG-ID): SRG-OS-000123-GPOS-00064

Rule Title: The information system must automatically remove or disable emergency accounts after the crisis is resolved or 72 hours.

Vulnerability Discussion: Emergency accounts are privileged accounts that are established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

VideoEdge: Not Applicable

VideoEdge does not support temporary or emergency accounts.

Rule Version (STIG-ID): SRG-OS-000125-GPOS-00065

Rule Title: The operating system must employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions.

Vulnerability Discussion: If maintenance tools are used by unauthorized personnel, they may accidentally or intentionally damage or compromise the system. The act of managing systems and applications includes the ability to access sensitive application information, such as system configuration details, diagnostic information, user information, and potentially sensitive application data.

Some maintenance and test tools are either standalone devices with their own operating systems or are applications bundled with an operating system.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Remote access to VideoEdge can be accomplished through a VPN. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge.

Rule Version (STIG-ID): SRG-OS-000126-GPOS-00066

Rule Title: The operating system must terminate all sessions and network connections related to nonlocal maintenance when nonlocal maintenance is completed.

Vulnerability Discussion: If a maintenance session or connection remains open after maintenance is completed, it may be hijacked by an attacker and used to compromise or damage the system.

Some maintenance and test tools are either standalone devices with their own operating systems or are applications bundled with an operating system.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Remote access to VideoEdge can be accomplished through a VPN. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge.

Rule Version (STIG-ID): SRG-OS-000132-GPOS-00067

Rule Title: The operating system must separate user functionality (including user interface services) from operating system management functionality.

Vulnerability Discussion: Operating system management functionality includes functions necessary for administration and requires privileged user access. Allowing non-privileged users to access operating system management functionality capabilities increases the risk that non-privileged users may obtain elevated privileges.

Operating system management functionality includes functions necessary to administer console, network components, workstations, or servers and typically requires privileged user access.

The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, different TCP/UDP ports, virtualization techniques, combinations of these methods, or other methods, as appropriate.

An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different security domain and with additional access controls.

VideoEdge: Compliant

VideoEdge provides the following user account types as defined by the assigned role – Administrator, Operator, Viewer. These roles provide separation of user functionality.

Rule Version (STIG-ID): SRG-OS-000134-GPOS-00068

Rule Title: The operating system must isolate security functions from nonsecurity functions.

Vulnerability Discussion: An isolation boundary provides access control and protects the integrity of the hardware, software, and firmware that perform security functions.

Security functions are the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Operating systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved

through file system protections that serve to protect the code on disk and address space protections that protect executing code.

Developers and implementers can increase the assurance in security functions by employing well-defined security policy models; structured, disciplined, and rigorous hardware and software development techniques; and sound system/security engineering principles. Implementation may include isolation of memory space and libraries. Operating systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000138-GPOS-00069

Rule Title: Operating systems must prevent unauthorized and unintended information transfer via shared system resources.

Vulnerability Discussion: Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge supports access by authenticated users that provide valid credentials assigned by the organization when accessing the system.

Rule Version (STIG-ID): SRG-OS-000142-GPOS-00071

Rule Title: The operating system must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of Denial of Service (DoS) attacks.

Vulnerability Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

DoS attacks on video systems are generally managed through network segmentation and firewall implementations.

Rule Version (STIG-ID): SRG-OS-000163-GPOS-00072

Rule Title: The operating system must terminate all network connections associated with a communications session at the end of the session, or as follows: for in-band management sessions (privileged sessions), the session must be terminated after 10 minutes of inactivity; and for user sessions (non-privileged session), the session must be terminated after 15 minutes of inactivity, except to fulfill documented and validated mission requirements.

Vulnerability Discussion: Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000184-GPOS-00078

Rule Title: The operating system must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.

Vulnerability Discussion: Failure to a known safe state helps prevent systems from failing to a state that may cause loss of data or unauthorized access to system resources. Operating systems that fail suddenly and with no incorporated failure state planning may leave the system available but with a reduced security protection capability. Preserving operating system state information also facilitates system restart and return to the operational mode of the organization with less disruption to mission-essential processes.

Abort refers to stopping a program or function before it has finished naturally. The term abort refers to both requested and unexpected terminations.

VideoEdge: Compliant

In support of this control, VideoEdge provides functionality to backup and restore system-level information and/or revert to a previous configuration baseline.

Rule Version (STIG-ID): SRG-OS-000185-GPOS-00079

Rule Title: The operating system must protect the confidentiality and integrity of all information at rest.

Vulnerability Discussion: Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive and tape drive, when used for backups) within an operating system.

This requirement addresses protection of user-generated data, as well as operating system-specific configuration data. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate, in accordance with the security category and/or classification of the information.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system. In support of this control, VideoEdge provides functionality to backup and restore user-level and system-level information.

Rule Version (STIG-ID): SRG-OS-000191-GPOS-00080

Rule Title: The operating system must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where HBSS is used; 30 days, for any additional internal network scans not covered by HBSS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Vulnerability Discussion: Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.

To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using HBSS and periodic scanning using other tools, as specified in the requirement.

VideoEdge: Partial Compliance

Responsibility for this control is shared by the organization and the system. To meet a 30 day requirement the organization would need to implement this.

In support of this control, Tyco performs a vulnerability scan on each release of VideoEdge as part of its regulatory and compliance activity. Tyco also periodically engages a third-party information assurance consultant to perform independent vulnerability scan testing.

Rule Version (STIG-ID): SRG-OS-000205-GPOS-00083

Rule Title: The operating system must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

Vulnerability Discussion: Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

VideoEdge: Compliant

The organization has primary responsibility for identifying the potentially security-relevant error conditions. VideoEdge supports this control by reporting server failures and other error conditions.

Error conditions do not present themselves in a way which will disclose sensitive or harmful information.

Rule Version (STIG-ID): SRG-OS-000206-GPOS-00084

Rule Title: The operating system must reveal error messages only to authorized users.

Vulnerability Discussion: Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000228-GPOS-00088

Rule Title: Any publically accessible connection to the operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Vulnerability Discussion: Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

"I've read & consent to terms in IS user agreem't."

VideoEdge: Compliant

The System Use Banner can be configured to display an approved system use notification message or banner before the user logs on to the system either locally or remotely. It also can be used to provide privacy and security notices consistent with applicable federal laws, executive orders, directives, polices, regulations, standards, and guidance.

Rule Version (STIG-ID): SRG-OS-000239-GPOS-00089

Rule Title: The operating system must audit all account modifications.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify an existing account. Auditing account modification actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000240-GPOS-00090

Rule Title: The operating system must audit all account disabling actions.

Vulnerability Discussion: When operating system accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the operating system processes themselves. In order to detect and respond to events affecting user accessibility and system processing, operating systems must audit account disabling actions and, as required, notify the appropriate individuals so they can investigate the event. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000241-GPOS-00091

Rule Title: The operating system must audit all account removal actions.

Vulnerability Discussion: When operating system accounts are removed, user accessibility is affected. Accounts are utilized for identifying individual users or for

identifying the operating system processes themselves. In order to detect and respond to events affecting user accessibility and system processing, operating systems must audit account removal actions and, as required, notify the appropriate individuals so they can investigate the event. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000250-GPOS-00093

Rule Title: The operating system must implement cryptography to protect the integrity of remote access sessions.

Vulnerability Discussion: Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

VideoEdge: Compliant

VideoEdge supports SSL connections for remote sessions.

Rule Version (STIG-ID): SRG-OS-000254-GPOS-00095

Rule Title: The operating system must initiate session audits at system start-up.

Vulnerability Discussion: If auditing is enabled late in the start-up process, the actions of some start-up processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000255-GPOS-00096

Rule Title: The operating system must produce audit records containing information to establish the identity of any individual or process associated with the event.

Vulnerability Discussion: Without information that establishes the identity of the subjects (i.e., users or processes acting on behalf of users) associated with the events, security personnel cannot determine responsibility for the potentially harmful event.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000256-GPOS-00097

Rule Title: The operating system must protect audit tools from unauthorized access.

Vulnerability Discussion: Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys in order to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000257-GPOS-00098

Rule Title: The operating system must protect audit tools from unauthorized modification.

Vulnerability Discussion: Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding

rights the user has in order to make access decisions regarding the modification of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000258-GPOS-00099

Rule Title: The operating system must protect audit tools from unauthorized deletion.

Vulnerability Discussion: Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

Operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user has in order to make access decisions regarding the deletion of audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000259-GPOS-00100

Rule Title: The operating system must limit privileges to change software resident within software libraries.

Vulnerability Discussion: If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals shall be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000266-GPOS-00101

Rule Title: The operating system must enforce password complexity by requiring that at least one special character be used.

Vulnerability Discussion: Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity or strength is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are those characters that are not alphanumeric. Examples include: ~
! @ # \$ % ^ *.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000269-GPOS-00103

Rule Title: In the event of a system failure, the operating system must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.

Vulnerability Discussion: Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system.

Preserving operating system state information helps to facilitate operating system restart and return to the operational mode of the organization with least disruption to mission/business processes.

VideoEdge: Compliant

In support of this control, VideoEdge provides backup and restore functionality and documented procedures with the system manuals.

Rule Version (STIG-ID): SRG-OS-000274-GPOS-00104

Rule Title: The operating system must notify system administrators and ISSOs when accounts are created.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the creation of operating system user accounts and notifies administrators and ISSOs that it exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000275-GPOS-00105

Rule Title: The operating system must notify system administrators and ISSOs when accounts are modified.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to modify an existing account. Notification of account modification is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail which documents the modification of operating system user accounts and notifies the system administrator and ISSO of changes. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000276-GPOS-00106

The operating system must notify system administrators and ISSOs when accounts are disabled.

Vulnerability Discussion: When operating system accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual operating system users or for identifying the operating system processes themselves. Sending notification of account disabling events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000277-GPOS-00107

Rule Title: The operating system must notify system administrators and ISSOs when accounts are removed.

Vulnerability Discussion: When operating system accounts are removed, user accessibility is affected. Accounts are utilized for identifying individual operating system users or for identifying the operating system processes themselves. Sending notification of account removal events to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000278-GPOS-00108

Rule Title: The operating system must use cryptographic mechanisms to protect the integrity of audit tools.

Vulnerability Discussion: Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

VideoEdge: Non-Complaint

VideoEdge mitigates this requirement, by only allowing administrators to access view or manipulate audit logs. Also if an admin remotes into VideoEdge they can use SSL for the remote session.

Rule Version (STIG-ID): SRG-OS-000279-GPOS-00109

Rule Title: The operating system must automatically terminate a user session after inactivity time-outs have expired or at shutdown.

Vulnerability Discussion: Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific operating system functionality where the system owner, data owner, or organization requires additional assurance.

VideoEdge : Compliant

VideoEdge Administrator Interface user accounts can be configured to automatically log out the user after a configurable period of inactivity (between 5 and 60 minutes).

Rule Version (STIG-ID): SRG-OS-000280-GPOS-00110

Rule Title: The operating system must provide a logoff capability for user-initiated communications sessions when requiring user access authentication.

Vulnerability Discussion: If a user cannot explicitly end an operating system session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session.

Information resources to which users gain access via authentication include, for example, local workstations and remote services. For some types of interactive sessions, including, for example, remote logon, information systems typically send logoff messages as final messages prior to terminating sessions.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000281-GPOS-00111

Rule Title: The operating system must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.

Vulnerability Discussion: If a user cannot explicitly end an operating system session, the session may remain open and be exploited by an attacker; this is referred to as a zombie session. Users need to be aware of whether or not the session has been terminated.

Information resources to which users gain access via authentication include, for example, local workstations and remote services. Logoff messages can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions, including, for example, remote logon, information systems typically send logoff messages as final messages prior to terminating sessions.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000297-GPOS-00115

Rule Title: The operating system must control remote access methods.

Vulnerability Discussion: Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Operating system functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

VideoEdge: Compliant

VideoEdge supports remote access from authorized system components. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge.

Rule Version (STIG-ID): SRG-OS-000298-GPOS-00116

Rule Title: The operating system must provide the capability to immediately disconnect or disable remote access to the operating system.

Vulnerability Discussion: Without the ability to immediately disconnect or disable remote access, an attack or other compromise taking place would not be immediately stopped.

Operating system remote access functionality must have the capability to immediately disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions functions and the need to eliminate immediate or future remote access to organizational information systems.

The remote access functionality (e.g., RDP) may implement features such as automatic disconnect (or user-initiated disconnect) in case of adverse information based on an indicator of compromise or attack.

VideoEdge: Compliant

Remote web access to the VideoEdge Administration Interface can be restricted or deactivated. The configuration allows external web and mobile device access to be disabled and concurrent web sessions to be restricted.

Rule Version (STIG-ID): SRG-OS-000299-GPOS-00117

Rule Title: The operating system must protect wireless access to and from the system using encryption.

Vulnerability Discussion: Allowing devices and users to connect to or from the system without first authenticating them allows untrusted access and can lead to a compromise or attack. Since wireless communications can be intercepted, it is necessary to use encryption to protect the confidentiality of information in transit.

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

This requirement applies to those operating systems that control wireless devices.

VideoEdge: Not Applicable

The VideoEdge Appliance does not support wireless communication

Rule Version (STIG-ID): SRG-OS-000300-GPOS-00118

Rule Title: The operating system must protect wireless access to the system using authentication of users and/or devices.

Vulnerability Discussion: Allowing devices and users to connect to the system without first authenticating them allows untrusted access and can lead to a compromise or attack.

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

This requirement applies to those operating systems that control wireless devices.

VideoEdge: Not Applicable

The VideoEdge Appliance does not support wireless communication

Rule Version (STIG-ID): SRG-OS-000303-GPOS-00120

Rule Title: The operating system must audit all account enabling actions.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable a new or disabled account. Auditing account modification actions provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000304-GPOS-00121

Rule Title: The operating system must notify system administrators and ISSOs of account enabling actions.

Vulnerability Discussion: Once an attacker establishes access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to enable an existing disabled account. Sending notification of account enabling actions to the system administrator and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that operating system accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

In order to detect and respond to events that affect user accessibility and application processing, operating systems must audit account enabling actions and, as required, notify the appropriate individuals so they can investigate the event.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000312-GPOS-00122

Rule Title: The operating system must allow operating system admins to pass information to any other operating system admin or user.

Vulnerability Discussion: Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

VideoEdge: Not Applicable

This feature is not offered by VideoEdge, but something the organization could roll out using Active Directory and Microsoft Exchange or another mail server.

Rule Version (STIG-ID): SRG-OS-000312-GPOS-00123

Rule Title: The operating system must allow operating system admins to grant their privileges to other operating system admins.

Vulnerability Discussion: Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000312-GPOS-00124

Rule Title: The operating system must allow operating system admins to change security attributes on users, the operating system, or the operating systems components.

Vulnerability Discussion: Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000324-GPOS-00125

Rule Title: The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Vulnerability Discussion: Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000326-GPOS-00126

Rule Title: The operating system must prevent all software from executing at higher privilege levels than users executing the software.

Vulnerability Discussion: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by the organizations.

Some programs and processes are required to operate at a higher privilege level and therefore should be excluded from the organization-defined software list after review.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000327-GPOS-00127

Rule Title: The operating system must audit the execution of privileged functions.

Vulnerability Discussion: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000329-GPOS-00128

Rule Title: The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes occur.

Vulnerability Discussion: By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account

VideoEdge: Compliant

User accounts for VideoEdge Administrator Interface and VideoEdge Client may be set to permanently or temporarily lock after a configurable number of invalid login attempts.

Rule Version (STIG-ID): SRG-OS-000337-GPOS-00129

Rule Title: The operating system must provide the capability for assigned IMOs/ISSOs or designated SAs to change the auditing to be performed on all operating system components, based on all selectable event criteria in near real time.

Vulnerability Discussion: If authorized individuals do not have the ability to modify auditing parameters in response to a changing threat environment, the organization may not be able to effectively respond, and important forensic information may be lost.

This requirement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting.

VideoEdge: Not Applicable

VideoEdge auditing cannot be changed on the fly it is configured via code and would need to be update in house to meet ongoing customer needs.

Rule Version (STIG-ID): SRG-OS-000338-GPOS-00130

Rule Title: The operating system must provide the capability for authorized users to select a user session to capture/record or view/hear.

Vulnerability Discussion: Without the capability to select a user session to capture/record or view/hear, investigations into suspicious or harmful events would be hampered by the volume of information captured. The volume of information captured may also adversely impact the operation of the network.

Session audits may include monitoring keystrokes, screen monitoring software, remote desktop recording, screen mirroring, and recording information and/or file transfers.

VideoEdge: Not Applicable

VideoEdge does not provide this feature, but could be implemented with third party software.

Rule Version (STIG-ID): SRG-OS-000339-GPOS-00131

Rule Title: The operating system must provide the capability for authorized users to remotely view/hear, in real time, all content related to an established user session from a component separate from the operating system being monitored.

Vulnerability Discussion: Without the capability to remotely view/hear all content related to a user session, investigations into suspicious user activity would be hampered. Real-time monitoring allows authorized personnel to take action before additional damage is done. The ability to observe user sessions as they are happening allows for interceding in ongoing events that after-the-fact review of captured content would not allow.

VideoEdge: Not Applicable

VideoEdge does not provide this feature, but could be implemented with third party software.

Rule Version (STIG-ID): SRG-OS-000341-GPOS-00132

Rule Title: The operating system must allocate audit record storage capacity to store at least one week's worth of audit records, when audit records are not immediately sent to a central audit record storage facility.

Vulnerability Discussion: In order to ensure operating systems have a sufficient storage capacity in which to write the audit logs, operating systems need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000342-GPOS-00133

Rule Title: The operating system must off-load audit records onto a different system or media from the system being audited.

Vulnerability Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000343-GPOS-00134

Rule Title: The operating system must immediately notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Vulnerability Discussion: If security personnel are not notified immediately when storage volume reaches 75% utilization, they are unable to plan for audit record storage capacity expansion.

VideoEdge: Compliant

VideoEdge provides a warning when the audit record storage area reaches a system-defined “percentage full” level.

When the audit record storage area reaches 100% full, VideoEdge records new audit events by overwriting the oldest audit records.

It is the organization's responsibility to use organization IT tools to monitor the status of VideoEdge server components to trigger alerts to organization officials in case of failure. It is assumed that the organization's network infrastructure and email system can support this capability.

Rule Version (STIG-ID): SRG-OS-000344-GPOS-00135

Rule Title: The operating system must provide an immediate real-time alert to the SA and ISSO, at a minimum, of all audit failure events requiring real-time alerts.

Vulnerability Discussion: It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

VideoEdge: Compliant

Audit logging functionality exists in VideoEdge to support SI-4 and the implementation of this SI-4 control enhancement.

Rule Version (STIG-ID): SRG-OS-000348-GPOS-00136

Rule Title: The operating system must provide an audit reduction capability that supports on-demand audit review and analysis.

Vulnerability Discussion: The ability to perform on-demand audit review and analysis, including after the audit data has been subjected to audit reduction, greatly facilitates the organization's ability to generate incident reports, as needed, to better handle larger-scale or more complex security incidents.

Audit reduction is a technique used to reduce the volume of audit records in order to facilitate a manual review. Audit reduction does not alter original audit records. The report generation capability provided by the application must support on-demand (i.e., customizable, ad hoc, and as-needed) reports.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000349-GPOS-00137

Rule Title: The operating system must provide an audit reduction capability that supports after-the-fact investigations of security incidents.

Vulnerability Discussion: If the audit reduction capability does not support after-the-fact investigations, it is difficult to establish, correlate, and investigate the events leading up to an outage or attack or identify those responses for one. This capability is also required to comply with applicable Federal laws and DoD policies.

Audit reduction capability must support after-the-fact investigations of security incidents either natively or through the use of third-party tools.

This requirement is specific to operating systems with audit reduction capabilities.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000350-GPOS-00138

Rule Title: The operating system must provide a report generation capability that supports on-demand audit review and analysis.

Vulnerability Discussion: The report generation capability must support on-demand review and analysis in order to facilitate the organization's ability to generate incident reports, as needed, to better handle larger-scale or more complex security incidents.

Report generation must be capable of generating on-demand (i.e., customizable, ad hoc, and as-needed) reports. On-demand reporting allows personnel to report issues more rapidly to more effectively meet reporting requirements. Collecting log data and aggregating it to present the data in a single, consolidated report achieves this objective.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000351-GPOS-00139

Rule Title: The operating system must provide a report generation capability that supports on-demand reporting requirements.

Vulnerability Discussion: The report generation capability must support on-demand reporting in order to facilitate the organization's ability to generate incident reports, as needed, to better handle larger-scale or more complex security incidents.

Report generation must be capable of generating on-demand (i.e., customizable, ad hoc, and as-needed) reports. On-demand reporting allows personnel to report issues more rapidly to more effectively meet reporting requirements. Collecting log data and aggregating it to present the data in a single, consolidated report achieves this objective.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000352-GPOS-00140

Rule Title: The operating system must provide a report generation capability that supports after-the-fact investigations of security incidents.

Vulnerability Discussion: If the report generation capability does not support after-the-fact investigations, it is difficult to establish, correlate, and investigate the events leading up to an outage or attack or identify those responses for one. This capability is also required to comply with applicable Federal laws and DoD policies.

The report generation capability must support after-the-fact investigations of security incidents either natively or through the use of third-party tools.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000353-GPOS-00141

Rule Title: The operating system must not alter original content or time ordering of audit records when it provides an audit reduction capability.

Vulnerability Discussion: If the audit reduction capability alters the content or time ordering of audit records, the integrity of the audit records is compromised, and the records are no longer usable for forensic analysis.

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Time ordering refers to the chronological organization of records based on time stamps. The degree of time stamp precision can affect this.

This requirement is specific to operating systems providing audit reduction capabilities. The audit reduction capability can be met either natively or through the use of third-party tools.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000354-GPOS-00142

Rule Title: The operating system must not alter original content or time ordering of audit records when it provides a report generation capability.

Vulnerability Discussion: If the report generation capability alters the content or time ordering of audit records, the integrity of the audit records is compromised, and the records are no longer usable for forensic analysis.

Time ordering refers to the chronological organization of records based on time stamps. The degree of time stamp precision can affect this.

This requirement is specific to operating systems providing report generation capabilities. The report generation capability can be met either natively or through the use of third-party tools.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000355-GPOS-00143

Rule Title: The operating system must, for networked systems, compare internal information system clocks at least every 24 hours with a server which is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

VideoEdge: Compliant

VideoEdge gets its time stamp from the SUSE Linux Enterprise Server (SLES) operating system it comes on, the SLES can be configured to use NTP and the organization can set the frequency it synchronizes the time.

Rule Version (STIG-ID): SRG-OS-000356-GPOS-00144

Rule Title: The operating system must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.

Vulnerability Discussion: Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Organizations should consider setting time periods for different types of systems (e.g., financial, legal, or mission-critical systems).

Organizations should also consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints). This requirement is related to the comparison done every 24 hours in SRG-OS-000355 because a comparison must be done in order to determine the time difference.

VideoEdge: Compliant

VideoEdge gets its time stamp from the SUSE Linux Enterprise Server (SLES) operating system it comes on, the SLES can be configured to use NTP and the organization can set the frequency it synchronizes the time.

Rule Version (STIG-ID): SRG-OS-000358-GPOS-00145

Rule Title: The operating system must record time stamps for audit records that meet a minimum granularity of one second for a minimum degree of precision.

Vulnerability Discussion: Without sufficient granularity of time stamps, it is not possible to adequately determine the chronological order of records.

Time stamps generated by the operating system include date and time. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000359-GPOS-00146

Rule Title: The operating system must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

Vulnerability Discussion: If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000360-GPOS-00147

Rule Title: The operating system must enforce dual authorization for movement and/or deletion of all audit information, when such movement or deletion is not part of an authorized automatic process.

Vulnerability Discussion: An authorized user may intentionally or accidentally move or delete audit records without those specific actions being authorized.

All bulk manipulation of audit information must be authorized via automatic processes. Any manual manipulation of audit information must require dual authorization. Dual authorization mechanisms require the approval of two authorized individuals to execute.

VideoEdge: Compliant

VideoEdge logs privileged actions performed by user accounts with authorized roles.

Rule Version (STIG-ID): SRG-OS-000362-GPOS-00149

Rule Title: The operating system must prohibit user installation of system software without explicit privileged status.

Vulnerability Discussion: Allowing regular users to install software, without explicit privileges, creates the risk that untested or potentially malicious software will be installed on the system. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

Operating system functionality will vary, and while users are not permitted to install unapproved software, there may be instances where the organization allows the user to install approved software packages, such as from an approved software repository.

The operating system or software configuration management utility must enforce control of software installation by users based upon what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

VideoEdge: Compliant

VideoEdge permits only privileged user accounts to install diagnostic or external software on the system.

Rule Version (STIG-ID): SRG-OS-000363-GPOS-00150

Rule Title: The operating system must notify designated personnel if baseline configurations are changed in an unauthorized manner.

Vulnerability Discussion: Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

VideoEdge: Compliant

Alerts can be generated via email and victor Client under various configurable categories. Email alerts can use authenticated SMTP servers (including Microsoft Exchange) and can encrypt emails using SSL or TLS. These alerts can be configured to assist or expand the capabilities of existing security policies including video data retention, camera malfunction, and user access control.

Rule Version (STIG-ID): SRG-OS-000364-GPOS-00151

Rule Title: The operating system must enforce access restrictions.

Vulnerability Discussion: Failure to provide logical access restrictions associated with changes to system configuration may have significant effects on the overall security of the system.

When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the operating system can have significant effects on the overall security of the system.

Accordingly, only qualified and authorized individuals should be allowed to obtain access to operating system components for the purposes of initiating changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000365-GPOS-00152

Rule Title: The operating system must audit the enforcement actions used to restrict access associated with changes to the system.

Vulnerability Discussion: Without auditing the enforcement of access restrictions against changes to the application configuration, it will be difficult to identify attempted attacks and an audit trail will not be available for forensic investigation for after-the-fact actions.

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. Enforcement action methods may be as simple as denying access to a file based on the application of file permissions (access restriction). Audit items may consist of lists of actions blocked by access restrictions or changes identified after the fact.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000366-GPOS-00153

Rule Title: The operating system must prevent the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.

Vulnerability Discussion: Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

VideoEdge: Compliant

VideoEdge software updates and patches follow Tyco's release development process and are qualified before being released from manufacturing.

Rule Version (STIG-ID): SRG-OS-000368-GPOS-00154

Rule Title: The operating system must prevent program execution in accordance with local policies regarding software program usage and restrictions and/or rules authorizing the terms and conditions of software program usage.

Vulnerability Discussion: Control of program execution is a mechanism used to prevent execution of unauthorized programs. Some operating systems may provide a capability that runs counter to the mission or provides users with functionality that exceeds mission requirements. This includes functions and services installed at the operating system-level.

Some of the programs, installed by default, may be harmful or may not be necessary to support essential organizational operations (e.g., key missions, functions). Removal of executable programs is not always possible; therefore, establishing a method of preventing program execution is critical to maintaining a secure system baseline.

Methods for complying with this requirement include restricting execution of programs in certain environments, while preventing execution in other environments; or limiting

execution of certain program functionality based on organization-defined criteria (e.g., privileges, subnets, sandboxed environments, or roles).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000370-GPOS-00155

Rule Title: The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

Vulnerability Discussion: Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Verification of white-listed software occurs prior to execution or at system startup.

This requirement applies to operating system programs, functions, and services designed to manage system processes and configurations (e.g., group policies).

VideoEdge: Not Applicable

The control is the responsibility of the organization.

Rule Version (STIG-ID): SRG-OS-000373-GPOS-00156

Rule Title: The operating system must require users to re-authenticate for privilege escalation.

Vulnerability Discussion: Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

VideoEdge: Compliant

VideoEdge provides accounts at the application and operating system level. Application accounts are grouped into role-based access permissions. Access to the information system requires authentication prior to granting access.

Rule Version (STIG-ID): SRG-OS-000373-GPOS-00157

Rule Title: The operating system must require users to re-authenticate when changing roles.

Vulnerability Discussion: Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to change security roles, it is critical the user re-authenticate.

VideoEdge: Compliant

VideoEdge provides accounts at the application and operating system level. Application accounts are grouped into role-based access permissions. Access to the information system requires authentication prior to granting access.

Rule Version (STIG-ID): SRG-OS-000373-GPOS-00158

Rule Title: The operating system must require users to re-authenticate when changing authenticators.

Vulnerability Discussion: Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to change user authenticators, it is critical the user re-authenticate.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000374-GPOS-00159

Rule Title: The operating system must require devices to re-authenticate when changing authenticators.

Vulnerability Discussion: Without re-authentication, devices may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to change device authenticators, it is critical the device re-authenticate.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000375-GPOS-00160

Rule Title: The operating system must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.

Vulnerability Discussion: Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Requires further clarification from NIST.

VideoEdge: Compliant

VideoEdge has the ability to meet this control.

Rule Version (STIG-ID): SRG-OS-000376-GPOS-00161

Rule Title: The operating system must accept Personal Identity Verification (PIV) credentials.

Vulnerability Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

VideoEdge: Not Applicable

VideoEdge does not provide CAC ability, but the operating system that the organization is using can implement this control. TYCO Security Products has put this feature request in there roadmap for future builds.

Rule Version (STIG-ID): SRG-OS-000377-GPOS-00162

Rule Title: The operating system must electronically verify Personal Identity Verification (PIV) credentials.

Vulnerability Discussion: The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DoD has mandated the use of the CAC to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

VideoEdge: Not Applicable

VideoEdge does not provide CAC ability, but the operating system that the organization is using can implement this control. TYCO Security Products has put this feature request in there roadmap for future builds.

Rule Version (STIG-ID): SRG-OS-000378-GPOS-00163

Rule Title: The operating system must authenticate peripherals before establishing a connection.

Vulnerability Discussion: Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000379-GPOS-00164

Rule Title: The operating system must authenticate all endpoint devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

Vulnerability Discussion: Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk.

Bidirectional authentication solutions include, but are not limited to, IEEE 802.1x and Extensible Authentication Protocol [EAP], RADIUS server with EAP-Transport Layer Security [TLS] authentication, Kerberos, and SSL mutual authentication.

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area network, wide area network, or the Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet).

Because of the challenges of applying this requirement on a large scale, organizations are encouraged to only apply this requirement to those limited number (and type) of devices that truly need to support this capability.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system. VideoEdge supports authenticated connections.

Rule Version (STIG-ID): SRG-OS-000380-GPOS-00165

Rule Title: The operating system must allow the use of a temporary password for system logons with an immediate change to a permanent password.

Vulnerability Discussion: Without providing this capability, an account may be created without a password. Non-repudiation cannot be guaranteed once an account is created if a user is not forced to change the temporary password upon initial logon.

Temporary passwords are typically used to allow access when new accounts are created or passwords are changed. It is common practice for administrators to create temporary passwords for user accounts which allow the users to log on, yet force them to change the password once they have successfully authenticated.

VideoEdge: Compliant

VideoEdge NVRs ship with preset passwords on all accounts. When activated, the VideoEdge Administrator Interface advises users that these passwords should be changed. The enhanced password validation feature enforces restrictions when setting or changing passwords:

- Passwords must be different than the previous three passwords
- Passwords must differ from the previous password by a minimum of three characters Passwords must be a minimum of seven characters long and must contain a mixture of upper and lower case letters, numbers, and special characters

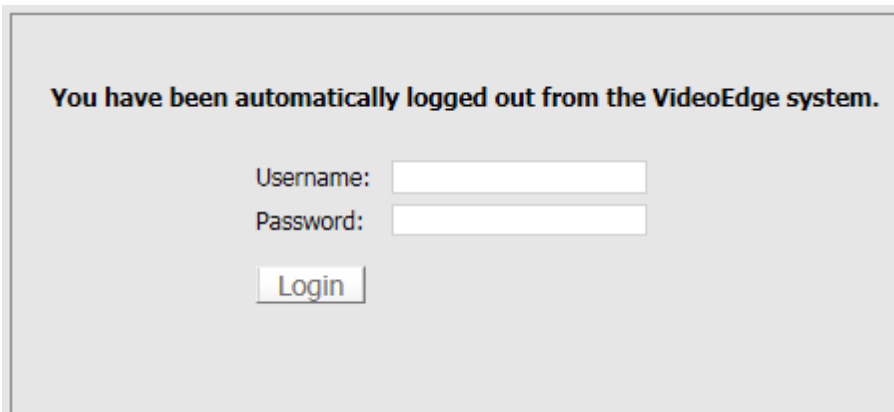
Rule Version (STIG-ID): SRG-OS-000383-GPOS-00166

Rule Title: The operating system must prohibit the use of cached authenticators after one day.

Vulnerability Discussion: If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

VideoEdge: Compliant

VideoEdge Administrator Interface user accounts can be configured to automatically log out the user after a configurable period of inactivity (between 5 and 60 minutes).



You have been automatically logged out from the VideoEdge system.

Username:

Password:

Rule Version (STIG-ID): SRG-OS-000384-GPOS-00167

Rule Title: The operating system, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.

Vulnerability Discussion: Without configuring a local cache of revocation data, there is the potential to allow access to users who are no longer authorized (users with revoked certificates).

VideoEdge: Not Applicable

VideoEdge does not provide CAC ability, but the operating system that the organization is using can implement this control. TYCO Security Products has put this feature request in there roadmap for future builds.

Rule Version (STIG-ID): SRG-OS-000392-GPOS-00172

Rule Title: The operating system must audit all activities performed during nonlocal maintenance and diagnostic sessions.

Vulnerability Discussion: If events associated with nonlocal administrative access or diagnostic sessions are not logged, a major tool for assessing and investigating attacks would not be available.

This requirement addresses auditing-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the

Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.

VideoEdge: Compliant

Remote access to VideoEdge can be accomplished through a VPN. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge. Audit logging functionality exists in VideoEdge to support SI-4 and the implementation of this SI-4 control enhancement.

Rule Version (STIG-ID): SRG-OS-000393-GPOS-00173

Rule Title: The operating system must implement cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications, when used for nonlocal maintenance sessions.

Vulnerability Discussion: Privileged access contains control and configuration information and is particularly sensitive, so additional protections are necessary. This is maintained by using cryptographic mechanisms, such as a hash function or digital signature, to protect integrity.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

The operating system can meet this requirement through leveraging a cryptographic module. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch).

VideoEdge: Compliant

VideoEdge supports SSL connections for remote sessions.

Rule Version (STIG-ID): SRG-OS-000394-GPOS-00174

Rule Title: The operating system must implement cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications, when used for nonlocal maintenance sessions.

Vulnerability Discussion: Privileged access contains control and configuration information and is particularly sensitive, so additional protections are necessary. This is maintained by using cryptographic mechanisms such as encryption to protect confidentiality.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those

activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

This requirement applies to hardware/software diagnostic test equipment or tools. This requirement does not cover hardware/software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch).

The operating system can meet this requirement through leveraging a cryptographic module.

VideoEdge: Compliant

VideoEdge supports SSL connections for remote sessions.

Rule Version (STIG-ID): SRG-OS-000395-GPOS-00175

Rule Title: The operating system must verify remote disconnection at the termination of nonlocal maintenance and diagnostic sessions, when used for nonlocal maintenance sessions.

Vulnerability Discussion: If the remote connection is not closed and verified as closed, the session may remain open and be exploited by an attacker; this is referred to as a zombie session. Remote connections must be disconnected and verified as disconnected when nonlocal maintenance sessions have been terminated and are no longer available for use.

VideoEdge: Not Applicable

The organization is responsible for remote access policies and authorizations. VideoEdge supports remote access from authorized system components. The organization's network configuration and remote access mechanisms are responsible for permitting or restricting the establishment of a remote session with VideoEdge.

Rule Version (STIG-ID): SRG-OS-000396-GPOS-00176

Rule Title: The operating system must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

VideoEdge: Not Applicable

VideoEdge is designed to be used in an unclassified environment, classified data will not be present on the system.

Rule Version (STIG-ID): SRG-OS-000399-GPOS-00178

Rule Title: The operating system must request data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed, which would result in query

failure or DoS. Data origin authentication must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity of response data.

This is not applicable if DNSSEC is not implemented on the local network.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge supports this control through the use of a DNS to resolve queries.

Rule Version (STIG-ID): SRG-OS-000400-GPOS-00179

Rule Title: The operating system must request data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed which would result in query

failure or denial of service. Data integrity verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This is not applicable if DNSSEC is not implemented on the local network.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge supports this control through the use of a DNS to resolve queries.

Rule Version (STIG-ID): SRG-OS-000401-GPOS-00180

Rule Title: The operating system must perform data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed which would result in query failure or denial of service. Data integrity verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This is not applicable if DNSSEC is not implemented on the local network.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge supports this control through the use of a DNS to resolve queries.

Rule Version (STIG-ID): SRG-OS-000402-GPOS-00181

Rule Title: The operating system must perform data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.

Vulnerability Discussion: If data origin authentication and data integrity verification are not performed, the resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed which would result in query failure or denial of service. Data origin authentication verification must be performed to thwart these types of attacks.

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching Domain Name System (DNS) servers. DNS client resolvers either

perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations.

This is not applicable if DNSSEC is not implemented on the local network.

VideoEdge: Compliant

Responsibility for this control is shared by the organization and the system.

VideoEdge supports this control through the use of a DNS to resolve queries.

Rule Version (STIG-ID): SRG-OS-000403-GPOS-00182

Rule Title: The operating system must only allow the use of DoD PKI-established certificate authorities for verification of the establishment of protected sessions.

Vulnerability Discussion: Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DoD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DoD-approved CA, trust of this CA has not been established.

The DoD will only accept PKI-certificates obtained from a DoD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of SSL/TLS certificates.

VideoEdge: Not Applicable

VideoEdge does not provide CAC ability, but the operating system that the organization is using can implement this control. TYCO Security Products has put this feature request in there roadmap for future builds.

Rule Version (STIG-ID): SRG-OS-000404-GPOS-00183

Rule Title: The operating system must implement cryptographic mechanisms to prevent unauthorized modification of all information at rest on all operating system components.

Vulnerability Discussion: Operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

VideoEdge: Not Applicable

VideoEdge is not an "at rest" data product.

Rule Version (STIG-ID): SRG-OS-000405-GPOS-00184

Rule Title: The operating system must implement cryptographic mechanisms to prevent unauthorized disclosure of all information at rest on all operating system components.

Vulnerability Discussion: Operating systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

VideoEdge: Not Applicable

VideoEdge is not an "at rest" data product

Rule Version (STIG-ID): SRG-OS-000420-GPOS-00186

Rule Title: The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

Vulnerability Discussion: DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For

each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

DoS attacks on video systems are generally managed through network segmentation and firewall implementations.

Rule Version (STIG-ID): SRG-OS-000423-GPOS-00187

Rule Title: The operating system must protect the confidentiality and integrity of transmitted information.

Vulnerability Discussion: Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of

protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Rule Version (STIG-ID): SRG-OS-000424-GPOS-00188

Rule Title: The operating system must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).

Vulnerability Discussion: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to leverage transmission protection mechanisms such as TLS, SSL VPNs, or IPsec.

Alternative physical protection measures include PDS. PDSs are used to transmit unencrypted classified National Security Information (NSI) through an area of lesser classification or control. Since the classified NSI is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation.

VideoEdge: Compliant

The VideoEdge NVR employs TLS.

Rule Version (STIG-ID): SRG-OS-000425-GPOS-00189

Rule Title: The operating system must maintain the confidentiality and integrity of information during preparation for transmission.

Vulnerability Discussion: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When transmitting data, operating systems need to support transmission protection mechanisms such as TLS, SSL VPNs, or IPsec.

VideoEdge: Compliant

The VideoEdge NVR employs TLS.

Rule Version (STIG-ID): SRG-OS-000426-GPOS-00190

Rule Title: The operating system must maintain the confidentiality and integrity of information during reception.

Vulnerability Discussion: Information can be either unintentionally or maliciously disclosed or modified during reception, including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Ensuring the confidentiality of transmitted information requires the operating system to take measures in preparing information for transmission. This can be accomplished via access control and encryption.

Use of this requirement will be limited to situations where the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process. When receiving data, operating systems need to leverage protection mechanisms such as TLS, SSL VPNs, or IPsec.

VideoEdge: Compliant

The VideoEdge NVR employs TLS.

Rule Version (STIG-ID): SRG-OS-000432-GPOS-00191

Rule Title: The operating system must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.

Vulnerability Discussion: A common vulnerability of operating system is unpredictable behavior when invalid inputs are received. This requirement guards against adverse or unintended system behavior caused by invalid inputs, where information system responses to the invalid input may be disruptive or cause the system to fail into an unsafe state.

The behavior will be derived from the organizational and system requirements and includes, but is not limited to, notification of the appropriate personnel, creating an audit record, and rejecting invalid input.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000433-GPOS-00192

Rule Title: The operating system must implement non-executable data to protect its memory from unauthorized code execution.

Vulnerability Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Rule Version (STIG-ID): SRG-OS-000433-GPOS-00193

Rule Title: The operating system must implement address space layout randomization to protect its memory from unauthorized code execution.

Vulnerability Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Rule Version (STIG-ID): SRG-OS-000437-GPOS-00194

Rule Title: The operating system must remove all software components after updated versions have been installed.

Vulnerability Discussion: Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000445-GPOS-00199

Rule Title: The operating system must verify correct operation of all security functions.

Vulnerability Discussion: Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

VideoEdge: Compliant

The VideoEdge development process includes processes, procedures and tools that implement this control.

Rule Version (STIG-ID): SRG-OS-000446-GPOS-00200

Rule Title: The operating system must perform verification of the correct operation of security functions: upon system start-up and/or restart; upon command by a user with privileged access; and/or every 30 days.

Vulnerability Discussion: Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications, such as lights.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

VideoEdge: Not Applicable

These controls would be employed by the Organization to support the management of the security controls. The SLES operating system can be configured to meet security controls.

Rule Version (STIG-ID): SRG-OS-000447-GPOS-00201

Rule Title: The operating system must shut down the information system, restart the information system, and/or notify the system administrator when anomalies in the operation of any security functions are discovered.

Vulnerability Discussion: If anomalies are not acted upon, security functions may fail to secure the system.

Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Notifications provided by information systems include messages to local computer consoles, and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000458-GPOS-00203

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to access security objects occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000461-GPOS-00205

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000462-GPOS-00206

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to modify privileges occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000463-GPOS-00207

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to modify security objects occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000465-GPOS-00209

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000466-GPOS-00210

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to delete privileges occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000467-GPOS-00211

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to delete security levels occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000468-GPOS-00212

Rule Title: The operating system must generate audit records when successful/unsuccessful attempts to delete security objects occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000470-GPOS-00214

Rule Title: The operating system must generate audit records when successful/unsuccessful logon attempts occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000471-GPOS-00215

Rule Title: The operating system must generate audit records for privileged activities or other system-level access.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000471-GPOS-00216

Rule Title: The audit system must be configured to audit the loading and unloading of dynamic kernel modules.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Not Applicable

These controls would be employed by the Organization to support the management of the security controls. The SLES operating system can be configured to meet security controls.

Rule Version (STIG-ID): SRG-OS-000472-GPOS-00217

Rule Title: The operating system must generate audit records showing starting and ending time for user access to the system.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000473-GPOS-00218

Rule Title: The operating system must generate audit records when concurrent logons to the same account occur from different sources.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Best practice is to only allow one login session at a time. VideoEdge is configurable to allow only one login session at a time.

Rule Version (STIG-ID): SRG-OS-000474-GPOS-00219

Rule Title: The operating system must generate audit records when successful/unsuccessful accesses to objects occur.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000475-GPOS-00220

Rule Title: The operating system must generate audit records for all direct access to the information system.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Not Applicable

These controls would be employed by the Organization to support the management of the security controls. The SLES operating system can be configured to meet security controls.

Rule Version (STIG-ID): SRG-OS-000476-GPOS-00221

Rule Title: The operating system must generate audit records for all account creations, modifications, disabling, and termination events.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Not Applicable

These controls would be employed by the Organization to support the management of the security controls. The SLES operating system can be configured to meet security controls.

Rule Version (STIG-ID): SRG-OS-000477-GPOS-00222

Rule Title: The operating system must generate audit records for all kernel module load, unload, and restart actions, and also for all program initiations.

Vulnerability Discussion: Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

VideoEdge: Not Applicable

These controls would be employed by the Organization to support the management of the security controls. The SLES operating system can be configured to meet security controls.

Rule Version (STIG-ID): SRG-OS-000478-GPOS-00223

Rule Title: The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Vulnerability Discussion: Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000479-GPOS-00224

Rule Title: The operating system must, at a minimum, off-load interconnected systems in real time and off-load standalone systems weekly.

Vulnerability Discussion: Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

VideoEdge: Compliant

The responsibility for this control is shared by the organization and VideoEdge.

VideoEdge may need to be configured to access an FTP server to support the off-loading of audit logs and critical data.

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00225

Rule Title: The operating system must prevent the use of dictionary words for passwords.

Vulnerability Discussion: If the operating system allows the user to select passwords based on dictionary words, then this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00226

Rule Title: The operating system must enforce a delay of at least 4 seconds between logon prompts following a failed logon attempt.

Vulnerability Discussion: Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

VideoEdge: Compliant

VideoEdge provides the capability to configure a login retry delay time. This determines the duration that the user account will be locked before a new log in can be attempted.

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00227

Rule Title: The operating system must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

Vulnerability Discussion: Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

VideoEdge: Not Applicable

Technical controls are the responsibility of the organization to meet their standards.

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00228

Rule Title: The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Vulnerability Discussion: Setting the most restrictive default permissions ensures that when new accounts are created they do not have unnecessary access.

VideoEdge: Not Applicable

Permissions on user files on the operating system will be implemented by the organization.

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00229

Rule Title: The operating system must not allow an unattended or automatic logon to the system.

Vulnerability Discussion: Failure to restrict system access to authenticated users negatively impacts operating system security.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00230

Rule Title: The operating system must limit the ability of non-privileged users to grant other users direct access to the contents of their home directories/folders.

Vulnerability Discussion: Users' home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

VideoEdge: Compliant

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00231

Rule Title: The operating system must employ a deny-all, allow-by-exception firewall policy for allowing connections to other systems.

Vulnerability Discussion: Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

VideoEdge: Not Applicable

Permissions on user files on the operating system will be implemented by the organization.

Rule Version (STIG-ID): SRG-OS-000480-GPOS-00232

Rule Title: The operating system must enable an application firewall, if available.

Vulnerability Discussion: Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

VideoEdge: Not Applicable

This control is the responsibility of the organization.

Rule Version (STIG-ID): SRG-OS-000481-GPOS-000481

Rule Title: The operating system must protect the confidentiality and integrity of communications with wireless peripherals.

Vulnerability Discussion: Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with an operating system. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR Keyboards, Mice, and Pointing Devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the AO. Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the operating system. Communication paths outside the

physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

VideoEdge: Not Applicable

VideoEdge does not have wireless capabilities.