tyco | American Dynamics

VideoEdge

NERC-CIP V6 Compliance Guide

Version 5.4

October 2019

8200-1907-01 A0

Johnson Controls

8200-1907-01 A0

Overview

This compliance guide describes how the VideoEdge network video controllers may be configured to meet the compliance requirements of NERC-CIP version 6. When used in conjunction with the VideoEdge installation and configuration guides, this information should assist in the installation of a compliant system and provide the necessary information for an audit.

While the guidance provided is specific to the functionality of VideoEdge v5.4, earlier versions of VideoEdge, may still be configured to be in compliance with NERC-CIP version 6.

Additional information is available in the VideoEdge Cybersecurity Overview Whitepaper.

Conventions

Not applicable: These controls are the sole responsibility of the Entity required to meet the control of NERC-CIP v6. Where possible, details on how the VideoEdge system may assist in meeting these requirements.

Shared: These controls, while still the responsibility of the Entity, may be aided through features of the VideoEdge system.

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 NONINFRINGEMENT. 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.

Contents

CIP–002–5.1a: Cyber Security - Management Controls

Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

R1 – Requirements and Measures

Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

i. Control Centers and backup Control Centers.

ii. Transmission stations and substations. iii. Generation resources.

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

v. Special Protection Systems that support the reliable operation of the Bulk Electric System. vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1.

Req ID	Requirement	VideoEdge
1.1	Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset.	**Not applicable -** Identifying high impact BES Cyber systems is up to the Responsible Entity.
1.2	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset.	**Not applicable -** Identifying medium impact BES Cyber systems is up to the Responsible Entity.

1.3	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	**Not applicable -** Identifying low impact BES Cyber systems is up to the Responsible Entity.

R2 – Requirements and Measures

The Responsible Entity shall:

Req ID	Requirement	VideoEdge
2.1	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1.	**Not applicable -** Identifying high impact BES Cyber systems is up to the Responsible Entity.
2.2	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	**Not applicable -** Identifying high impact BES Cyber systems is up to the Responsible Entity.

CIP–003–6: Cyber Security - Management Controls

Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electrical System (BES).

R1 – Requirements and Measures; Senior Management Approval

Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

Req ID	Requirement	VideoEdge
1.1	For its high impact and medium impact BES Cyber Systems, if any:	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.1	Personnel and training (CIP-004)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.2	Electronic Security Perimeters (CIP-005) including Interactive Remote Access.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.3	Physical security of BES Cyber Systems (CIP 006)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.4	System security management (CIP-007)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. Note: VideoEdge has product documentation that helps in support of the

		creation of a system security plan. This documentation includes a VideoEdge Cyber Security Hardening Guide
1.1.5	Incident reporting and response planning (CIP-008)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.6	Recovery plans for BES Cyber Systems (CIP-009)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.1.7	Configuration change management and vulnerability assessments (CIP-010)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** Johnson Controls, Inc. Product Security Team can assist in vulnerability management of American Dynamics products.
1.1.8	Information protection (CIP-011)	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** The data at rest and in transit is encrypted In the event of a system failure, recovery of the NVR server's configuration data is possible by using a system backup file stored to a USB or local disk. You can import the backup file to the NVR to restore the saved configuration

1.1.9	Declaring and responding to CIP Exceptional Circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2.1	Cyber security awareness.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2.2	Physical security controls.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2.3	Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dialup Connectivity.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2.4	Cyber Security Incident response	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Cyber Security Policies

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plans for its low impact BES Cyber Systems that include the sections in Attachment 1.

Not applicable - Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Requirements and Measures; CIP Senior Manager

Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

Not applicable - Policies, procedures and training are the responsibility of the Responsible Entity.

R4 – Requirements and Measures; CIP Delegation

The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

Not applicable - Policies, procedures and training are the responsibility of the Responsible Entity.

CIP–004–6: Cyber Security - Personnel and Training

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

R1 – Requirements and Measures; Security Awareness Program

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program.

Req ID	Requirement	VideoEdge
1.1	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Cyber Security Training Program

Each Responsible Entity shall implement one or more cyber security training programs appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.

Req ID	Requirement	VideoEdge

2.1	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets	**Shared -** Policies, procedures and training are the responsibility of the Responsible Entity. American Dynamics provides training for the installation and use VideoEdge.
2.2	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	**Shared -** Policies, procedures and training are the responsibility of the Responsible Entity. American Dynamics provides training for the installation and use VideoEdge.

2.3	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	**Shared-** Policies, procedures and training are the responsibility of the Responsible Entity. American Dynamics provides training for the installation and use VideoEdge.

R3 – Requirements and Measures; Personnel risk Assessment Program

Each Responsible Entity shall implement one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP004-6 Table R3 – Personnel Risk Assessment Program.

Req ID	Requirement	VideoEdge
3.1	Process to confirm identity.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

3.2	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.3	Criteria or process to evaluate criminal history records checks for authorizing access.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.4	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.5	Process to ensure that individuals with unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 Within the last seven years.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R4 – Requirements and Measures; Access Management

Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program.

Req ID	Requirement	VideoEdge
4.1	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** VideoEdge has the ability to define users based on roles with the definition for authorized on the need to implement least privilege.

4.2	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** VideoEdge has the ability to track last use of user to assist in review of authorization.
4.3	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** VideoEdge has the ability to track last use of user to assist in review of authorization. VideoEdge has the capability to have users expire for inactivity. Under Security Configuration you can do a security audits to view as logon and password change so you can determine if that person needs access anymore.
4.4	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R5 – Requirements and Measures; Access Revocation

Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation.

Req ID	Requirement	VideoEdge
5.1	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	**Complaint -** VideoEdge supports the revocation of personnel access credentials by using its personnel configuration tools
5.2	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	**Complaint -** VideoEdge supports the revocation of personnel access credentials by using its personnel configuration tools

5.3	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination	**Complaint** - VideoEdge supports the revocation of personnel access credentials by using its personnel configuration tools
5.4	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	**Shared**- Responsible Entity has most of the charge for this requirement, but VideoEdge supports the revocation of personnel access credentials by using its personnel configuration tools .
5.5	For termination actions, change passwords for shared accounts known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared accounts known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the passwords within 10 calendar days following the end of the operating circumstances.	**Shared-** Responsible Entity has most of the charge for this requirement, but VideoEdge has the capability to have users expire for inactivity

CIP–005–5: Cyber Security - Electronic Security Perimeters

Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

R1 – Requirements and Measures; Electronic Security Perimeter

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter.

Req ID	Requirement	VideoEdge
1.1	All applicable Cyber Assets connected to a network by using a routable protocol shall reside within a defined ESP.	**Compliant -** VideoEdge server reside within the ESP. Monitoring stations through web clients have ability to reside outside the boundary but would be managed through the Responsible Entity VPN or network restrictions.
1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.4	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Interactive Remote Access Management

Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.

Req ID	Requirement	VideoEdge
2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	**Not applicable -** The Responsible Entity is primarily responsible for this requirement.
2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	**Not applicable -** The Responsible Entity is primarily responsible for this requirement. .
2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	**Not applicable -** The Responsible Entity is primarily responsible for this requirement.

CIP–006–6: Cyber Security - Physical Security

Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

R1 – Requirements and Measures; Physical Security Plan

Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.

Req ID	Requirement	VideoEdge
1.1	Define operational or procedural controls to restrict physical access.	**Not Applicable for VideoEdge -**The responsible Entity shall document and implement the operational and procedural controls to manage physical access points to the Physical Security.
1.2	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	**Not Applicable for VideoEdge –** The responsible Entity shall write procedures for visitor control
1.3	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	**Not Applicable -**The responsible Entity shall document and implement the operational and procedural controls to manage physical access points to the Physical Security

1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	**Shared -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeters. You can set VideoEdge to trigger events for areas that have motion sensors. They can trigger events that are sent to VideoEdge
1.5	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	**Shared -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeters. You can set VideoEdge to trigger events for areas that have motion sensors. They can trigger events that are sent to VideoEdge
1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	**Shared –** It is the responsibility of the Entity to ensure that access to the server and workstations are protected. To help determine if and when a camera has been tampered with, the NVR automatically performs an image detection test on every camera to determine if a camera has gone dark or is broadcasting black video. It can also send alerts when a camera reboots or goes offline.
1.7	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	**Compliant** – You can save events and clips with date and time. You can create a clip for motion detection on a portal

1.9	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	**Not applicable -** It is the responsibility of the Entity to ensure log entries are retained. .
1.10	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • An equally effective logical protection.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** VideoEdge uses encryption for data in transit .

R2 – Requirements and Measures; Visitor Control program

Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.

Req ID	Requirement	VideoEdge
2.1	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.2	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.3	Retain visitor logs for at least ninety calendar days.	**Not applicable -** It is the responsibility of the Entity to ensure log entries are retained. .

R3 – Requirements and Measures; Physical Access Control System Maintenance and testing Program

Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.

Req ID	Requirement	VideoEdge
3.1	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

CIP–007–6: Cyber Security - Systems Security Management

Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

R1 – Requirements and Measures; Ports and Services

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.

Req ID	Requirement	VideoEdge
1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	**Compliant:** See separate ports document
1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**Not applicable -** It is the responsibility of the Responsible Entity to protect the VideoEdge

R2 – Requirements and Measures; Security Patch Management

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.

Req ID	Requirement	VideoEdge
2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	**Shared-** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-010-2 Table R1, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeters. VideoEdge hardening guide provides details on the Security Patch Management.
2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	**Shared-** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-010-2 Table R1, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeters. VideoEdge hardening guide provides details on the Security Patch Management.

Req ID	Requirement	VideoEdge
2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	**Shared-** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-010-2 Table R1, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeters. VideoEdge hardening guide provides details on the Security Patch Management.
2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Requirements and Measures; Malicious Code Prevention

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.

Req ID	Requirement	VideoEdge

3.1	Deploy method(s) to deter, detect, or prevent malicious code.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.2	Mitigate the threat of detected malicious code.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** VideoEdge is compatible with antivirus security software.
3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	**Compliant -** VideoEdge updates are digitally signed

R4 – Requirements and Measures; Security Monitoring

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.

Req ID	Requirement	VideoEdge
4.1.	Log events at the BES Cyber System level (for each BES Cyber System capability) or at the Cyber Asset level (for each Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:	**Compliant** – VideoEdge has system and security logs. It records logon attempts, and if enabled, will lock the account. Logs are also created when firmware is updated, or changes are made to the system

4.1.1	Detected successful logon attempts	**Compliant** – VideoEdge has system and security logs. It records logon attempts, and if enabled, will lock the account. Logs are also created when firmware is updated, or changes are made to the system
4.1.2	Detected failed access attempts and failed logon attempts	**Compliant** – VideoEdge has system and security logs. It records logon attempts, and if enabled, will lock the account. Logs are also created when firmware is updated, or changes are made to the system .
4.1.3	Detected malicious code.	**Compliant** – VideoEdge has system and security logs. It records logon attempts, and if enabled, will lock the account. Logs are also created when firmware is updated, or changes are made to the system .
4.2.	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events for each Cyber Asset or BES Cyber System capability:	

4.2.1	Detected malicious code from Part 4.1.	**Not applicable -** The control is the responsibility of the organization
4.2.2	Detected failure of Part 4.1 event logging.	**Not applicable -** The control is the responsibility of the organization
4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	**Shared - Policies**, procedures and training are the responsibility of the Responsible Entity. VideoEdge has the ability to regain logs
4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	**Not applicable -** The Responsible Entity is primarily responsible for this requirement.

R5 – Requirements and Measures; System Access Control

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.

Req ID	**Requirement**	**VideoEdge**
5.1	Have a methods to enforce authentication of interactive user access, where technically feasible.	**Compliant-** logging into VideoEdge requires username and passwords. You can import the users through LDAP

5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system types.	**Shared –** It is the responsibility of the Entity to identify and inventory all accounts
5.3	Identify individuals who have authorized access to shared accounts.	**Not Applicable –** The Entity is responsible to identify shared accounts.
5.4	Change known default passwords, for each Cyber Asset capability.	**Not Applicable -** The Entity is responsible to change all default passwords
5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:	.Shared

5.5.1	Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and	**Shared** – The Entity is responsible to enforce password complexity. 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 This requires a procedural enforcement

Req ID	**Requirement**	**VideoEdge**
5.5.2	Minimum password complexity that is the lesser of three or more different types of characters (For example, uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	**Shared** – The Entity is responsible to enforce password complexity. 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 This requires a procedural enforcement.

5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	**Shared** – The Entity is responsible to enforce password complexity. 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 This requires a procedural enforcement
5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	**Shared** – The Entity is responsible to enforce password changes. There are three logon lockout polices available for use; None, Lockout and Delay. When Lockout is enabled the account will be locked if the account performs the configured number of consecutive failed logon attempts. When Delay is selected, the account will be locked in accordance with the configured number of consecutive failed logon attempts and subsequently unlocked, in other words, able to log on, after the configured period of time. There is also a log that shows the time between password updates on the VideoEdge.

CIP–008–5: Cyber Security - Incident Reporting and Response Planning

Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

R1 - Requirements and Measures; Cyber Security Incident Response Plan Specifications

Each Responsible Entity shall document one or more Cyber Security Incident response plans that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.

Req ID	Requirement	VideoEdge
1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

1.4	Incident handling procedures for Cyber Security Incidents.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Cyber Security Incident Response Plan

Implementation and Testing

Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.

Req ID	Requirement	VideoEdge
2.1	Test each Cyber Security Incident response plans at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.2	Use the Cyber Security Incident response plans under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plans taken during the response to the incident or exercise.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

2.3	Retain records related to Reportable Cyber Security Incidents.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Requirements and Measures; Cyber Security Incident Response Plan Review,

Update, and Communication

Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.

Req ID	Requirement	VideoEdge
3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plans test or actual Reportable Cyber Security Incident response:	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.1	Document any lessons learned or document the absence of any lessons learned;	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.2	Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.3	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.2.1	Update the Cyber Security Incident response plans.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.2.2	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

CIP–009–6: Cyber Security - Recovery Plan Specifications

Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

R1 – Requirements and Measures; Recovery Plan Specifications

Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.

Req ID	Requirement	VideoEdge
1.1	Conditions for activation of the recovery plans.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	Roles and responsibilities of responders.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

1.5	One or more processes to preserve data, for each Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plans. Data preservation should not impede or restrict recovery.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Recovery Plan Implementation and testing

Each Responsible Entity shall implement its documented recovery plans to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.

Req ID	Requirement	VideoEdge
2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Requirements and Measures; Recovery Plan Review, Update and Communication

Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.

Req ID	Requirement	VideoEdge
3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.1	Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.2.	Update the recovery plan based on any documented lessons learned associated with the plan.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.1.3	Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

3.2.1	Update the recovery plan.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.2.2	Notify each person or group with a defined role in the recovery plan of the updates.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

APPENDIX – Resources and References

Tyco Documents

- VideoEdge NVR Installation and User Guide
- victor and VideoEdge Port Assignments
- VideoEdge DISA Security Guide
- FISMA-Ready: VideoEdge System
- FISMA-Ready: victor System
- VideoEdge Hardening Guide