tyco | Software House

C•CURE 9000 and iSTAR NERC-CIP Compliance Guide

8200-1907-01 B0

Johnson Controls

Overview

This compliance guide describes how the C•CURE 9000 v2.9 physical access control system and iSTAR door controllers may be configured to meet the compliance requirements of NERC-CIP. When used in conjunction with the C•CURE 9000 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 C•CURE 9000 v2.9, earlier versions of C•CURE 9000, including the previous release, v2.8, may still be configured to be in compliance with NERC-CIP.

Additional information is available in the C•CURE 9000 V2.9 and iSTAR Hardening Guide.

Conventions

Not applicable: These controls are the sole responsibility of the Entity required to meet the control of NERC-CIP. Where possible, details on how the C•CURE 9000 and iSTAR system may assist in meeting these requirements.

Shared: These controls, while still the responsibility of the Entity, may be aided through features of the C•CURE 9000 and iSTAR system.

Revision History:

10/2020 A0-B0

- Replaced CIP-003-6 with CIP-003-8
- Replaced CIP-005-5 with CIP-005-6
- Replaced CIP-008-5 with CIP-008-6
- Replaced CIP-010-2 with CIP-010-3
- Added CIP-011-2
- Added CIP-012-1
- Added CIP-013-1
- Added CIP-014-2

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.

The responses to NERC-CIP requirements within this document are based on the capabilities of C•CURE 9000 v2.9 and iSTAR v6.7.0. Use of the most current releases of these products is recommended. If older versions are utilized, it may be necessary to perform different steps to achieve compliance.

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 above.

Req ID	Requirement	C•CURE 9000 and iSTAR
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	C•CURE 9000 and iSTAR
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–003–8: 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 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	C•CURE 9000 and iSTAR
1.1	For its high impact and medium impact BES Cyber Systems, if any: 1.1.1 Personnel and training (CIP-004) 1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access. 1.1.3 Physical security of BES Cyber Systems (CIP 006) 1.1.4 System security management (CIP-007) 1.1.5 Incident reporting and response planning (CIP-008) 1.1.6 Recovery plans for BES Cyber Systems (CIP-009) 1.1.7 Configuration change management and vulnerability assessments (CIP-010) 1.1.8 Information protection (CIP-011) 1.1.9 Declaring and responding to CIP Exceptional Circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** Software House Product Security Team can assist in vulnerability management of Software House products. **Note:** The Crossfire service manages communication between the C•CURE 9000 server and the iSTAR controllers, database, and client devices. By default, the Crossfire service uses AES-256 encryption that has been FIPS 197 validated.
1.2	For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any: 1.2.1 Cyber security awareness 1.2.2 Physical security controls. 1.2.3 Electronic access controls 1.2.4 Cyber Security Incident response 1.2.5 Transient Cyber Assets and Removable Media malicious code risk mitigation; and 1.2.6 Declaring and responding to CIP Exceptional Circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** iSTAR network ports are physically protected within the enclosure of the panel with lock and tamper detection

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 plan(s) 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	C•CURE 9000 and iSTAR
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 program(s) 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	C•CURE 9000 and iSTAR
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. **Note:** Software House provides training for the installation and use C•CURE 9000 and iSTAR.

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. **Note:** Software House provides training for the installation and use C•CURE 9000 and iSTAR.
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. **Note:** Software House provides training for the installation and use C•CURE 9000 and iSTAR.

R3 – Requirements and Measures; Personnel risk Assessment Program

Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) 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 CIP-004-6 Table R3 – Personnel Risk Assessment Program.

Req ID	Requirement	C•CURE 9000 and iSTAR
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 Program

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

Req ID	Requirement	C•CURE 9000 and iSTAR
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:** C●CURE 9000 has the ability to assign unescorted physical access within the perimeter, or define escorted access. Levels of access are defined and controlled by the iSTAR. Integrators and end users with sufficient privileges in C●CURE maintain this feature. The iSTAR maintains physical access control based on defined privileges in C●CURE. C●CURE can temporarily grant access to portals for personnel if monitored by person with correct privileges. Electronic access to C●CURE is defined by operator roles configured by an administrator and implemented with Windows authentication.
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:** C●CURE can have credentials expire on set dates. Journals can be audited on set dates. The journal auditing can be set to display all users with unescorted physical access and end user can verify if authorization still applies.
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:** Journal auditing can be employed with C●CURE 9000 Journal auditing feature. End users can set journal audits for user accounts and their privileges at any time interval. The Responsible Entity will review the journal and confirm that users still allowed privileges or group access. If user should no longer have access, updates can be deployed within C●CURE 9000
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. **Note:** Access workflow feature of C•CURE can be used to validate roles and privileges. The Responsible Entity will review the access workflow and confirm that users still allowed privileges or group access. If user should no longer have access, the role or privilege may be removed from the user in C•CURE 9000.

R5 – Requirements and Measures; Access Revocation Programs

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

Req ID	Requirement	C•CURE 9000 and iSTAR
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).	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 shall be configured to synchronize personnel records from Microsoft Active Directory. Synchronization with Microsoft Active Directory occurs as a periodic background task. Revocation or authorization changes to individual credentials occur immediately in C•CURE 9000 and iSTAR. Journal auditing can be used to verify individual authorization against other databases to verify location. An alert can be generated for changes in daily run journals to notify users of change in authorizations.
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.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 shall be configured to synchronize personnel records from Microsoft Active Directory. Synchronization with Microsoft Active Directory occurs as a periodic background task. Revocation or authorization changes to individual credentials occur immediately in C•CURE 9000 and iSTAR. Journal auditing can be used to verify individual authorization against other databases to verify location. An alert can be generated for changes in daily run journals to notify users of change in authorizations.
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	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 shall be configured to synchronize personnel records from Microsoft Active Directory. Synchronization with Microsoft Active Directory occurs as a periodic background task. Revocation or authorization changes to individual credentials occur immediately in C•CURE 9000 and iSTAR. Journal auditing can be used to verify individual authorization against other databases to verify location. An alert can be generated for changes in daily run journals to notify users of change in authorizations.

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.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 shall be configured to synchronize personnel records from Microsoft Active Directory. Synchronization with Microsoft Active Directory occurs as a periodic background task. Revocation or authorization changes to individual credentials occur immediately in C•CURE 9000 and iSTAR. Journal auditing can be used to verify individual authorization against other databases to verify location. An alert can be generated for changes in daily run journals to notify users of change in authorizations.
5.5	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) 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 password(s) within 10 calendar days following the end of the operating circumstances.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** Revocation or authorization changes to individual credentials occur immediately in C●CURE 9000 and iSTAR. Journal auditing can be used to verify individual authorization against other databases to verify location. An alert can be generated for changes in daily run journals to notify users of change in authorizations. **Note:** Journal audit can be set to run at 30 days and 10 day intervals from termination notification to confirm user password changes. iSTAR diagnostic webpage and ICU, along with C●CURE 9000 login for user would be required to be part of audit comparison.

CIP–005–6: Cyber Security - Electronic Security Perimeter(s)

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-005-6 Table R1 – Electronic Security Perimeter

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** RFID cards, card readers, input sensors and door locks sit outside the boundary. The devices are not IP. iSTAR and C•CURE host 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. **Note:** Required C•CURE communication ports are documented and only required ports should be configured on firewalls to be open. Access to C•CURE should be restricted to certain level of privileges defined by the Responsible Entity. iSTAR diagnostic webpage is password protected which would only allow access to personnel with correct privileges. Diagnostic webpage is recommended to be disabled for security reasons. Levels of privileges are defined by the Responsible Entity and should be maintained and further defined by 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; Remote Access Management

Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 – Remote Access Management.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	For all Interactive Remote Access, 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. **Note:** C•CURE does not require interactive remote access.
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. **Note:** C•CURE does not require interactive remote access. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has achieved FIPS 197 validation. C•CURE 9000 creates the host server and CA certificates at the C•CURE 9000 host computer and then directs the controller to generate new public and private keys.

2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	**Not applicable -** The Responsible Entity is primarily responsible for this requirement. **Note:** C•CURE does not require interactive remote access. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has achieved FIPS 197 validation. C•CURE 9000 creates the host server and CA certificates at the C•CURE 9000 host computer and then directs the controller to generate new public and private keys.
2.4	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	**Not applicable -** The Responsible Entity is primarily responsible for this requirement. **Note:** C•CURE does not require interactive remote access. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has achieved FIPS 197 validation. C•CURE 9000 creates the host server and CA certificates at the C•CURE 9000 host computer and then directs the controller to generate new public and private keys.
2.5	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	**Not applicable -** The Responsible Entity is primarily responsible for this requirement. **Note:** C•CURE does not require interactive remote access. The encryption between C•CURE 9000 and the iSTAR Ultra and iSTAR Edge controllers has achieved FIPS 197 validation. C•CURE 9000 creates the host server and CA certificates at the C•CURE 9000 host computer and then directs the controller to generate new public and private keys.

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 plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Define operational or procedural controls to restrict physical access.	**Not applicable -** Policies and procedures and training are the responsibility of the Responsible Entity. **Note:** Software House provides training for the installation and use of C•CURE 9000 and iSTAR. C•CURE 9000 has the ability to assign unescorted physical access within the perimeter, or define escorted access. Levels of access are defined and controlled by the iSTAR. Integrators and end users with sufficient privileges in C•CURE maintain this feature. The iSTAR maintains physical access control based on defined privileges in C•CURE. C•CURE can temporarily grant access to portals for personnel if monitored by person with correct privileges. Electronic access to C•CURE is defined by operator roles configured by an administrator and implemented with Windows authentication.
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 -** Policies and procedures and training are the responsibility of the Responsible Entity. **Note:** Software House provides training for the installation and use of C•CURE 9000 and iSTAR. C•CURE 9000 has the ability to assign unescorted physical access within the perimeter, or define escorted access. Levels of access are defined and controlled by the iSTAR. Integrators and end users with sufficient privileges in C•CURE maintain this feature. The iSTAR maintains physical access control based on defined privileges in C•CURE. C•CURE can temporarily grant access to portals for personnel if monitored by person with correct privileges. Electronic access to C•CURE is defined by operator roles configured by an administrator and implemented with Windows authentication.
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. **Note:** C•CURE 9000 and iSTAR door controllers can be used to provide multiple physical access controls which restrict access to only those individuals who have authorized unescorted physical access.

1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	**Not applicable -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s). **Note:** C•CURE records invalid access attempts within its journals. iSTAR controllers and card readers are installed with tamper detection. Additional supervised inputs may be employed to add tamper detection of ancillary equipment. **Note:** It is the responsibility of the Entity to ensure that access to the C•CURE 9000 server and workstations are protected.
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.	**Not applicable -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s). **Note:** When installed in accordance to setup instructions, C•CURE / iSTAR Controller will issue alerts within the 15 minutes requirement. This has been verified by UL as part of C•CURE and iSTAR's UL1076 approvals. **Note:** If an Event/Alarm is Unacknowledged and/or Cleared for longer than the operator defined duration (maximum value is 99 hours, 59 minutes, 59 seconds), an overdue Event may be activated for additional notification.
1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	**Not applicable -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s). **Note:** C•CURE records invalid access attempts within its journals. iSTAR controllers and card readers are installed with tamper detection. Additional supervised inputs may be employed to add tamper detection of ancillary equipment. **Note:** It is the responsibility of the Entity to ensure that access to the C•CURE 9000 server and workstations are protected.

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 -** It is the responsibility of the Entity to ensure alarms are transmitted to the identified personnel and to ensure that access to the C•CURE 9000 server and workstations are protected. **Note:** C•CURE records invalid access attempts within its journals. iSTAR controllers and card readers are installed with tamper detection. Additional supervised inputs may be employed to add tamper detection of ancillary equipment. These tamper events can be configured to trigger and alarms at the C•CURE monitoring station in less than 15 minutes. This has been validated as part of the C•CURE 9000 and iSTAR UL1076 listing.
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.	**Not applicable -** It is the responsibility of the Entity to ensure log entries are recorded. **Note:** C•CURE 9000 will automatically log all access granted (and rejected) including identity, date and time, and location of access granted.
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. **Note:** C•CURE 9000 logs may be stored automatically with a scheduled event or based on a journal trigger. Retention of the logs is the responsibility of the Entity. **Note:** The C•CURE 9000 “Log Volume Management” and “Log Backup Management” feature supports the backup (archiving) and restoral of journal and audit data. This feature provides the ability to perform automated backups of journal log and audit log data by setting variables which define transaction limits or number of days.

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:** C•CURE shall be configured to encrypt all transmitted data. By default C•CURE 9000 and iSTAR will alert on communication failures. **Note:** Integrator can ensure cabling to be in conduit according to UL2050 in addition to configuring encryption for C•CURE communication paths.

R2 – Requirements and Measures; Visitor Control program

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

Req ID	Requirement	C•CURE 9000 and iSTAR
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. **Note:** C•CURE 9000 provides an Escorted Access feature which allows for the system to control, track, and report on the movements of personnel designated as Escorted Visitors.
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. **Note:** C•CURE 9000 provides an Escorted Access feature which allows for the system to control, track, and report on the movements of personnel designated as Escorted Visitors. C•CURE 9000 also offers an optional visitor management module, providing an efficient means to pre-register visitors and efficiently check-in visitors either through a self-service kiosk or through a receptionist portal.
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. **Note:** C•CURE 9000 logs may be stored automatically with a scheduled event or based on a journal trigger. Retention of the logs is the responsibility of the Entity.

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 program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.

Req ID	Requirement	C•CURE 9000 and iSTAR
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. **Note:** C•CURE 9000 includes a Maintenance Mode feature where selected objects (doors, input points, readers, etc.) may be placed in Maintenance Mode, and testing activities will not disrupt the normal alarm management functions of the Monitoring Station.

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 process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.

Req ID	Requirement	C•CURE 9000 and iSTAR
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.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 documentation listed in Appendix A provides details on the Software House Security Patch Management. It is recommended that the responsible party register for Software House cyber security advisory email notifications - https://tycosecurityproducts.com/CyberProtection/Registration.aspx
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 C•CURE 9000 server and workstations. **Note:** iSTAR network ports are physically protected within the enclosure of the panel with lock and tamper detection.

R2 – Requirements and Measures; Security Patch Management

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

Req ID	Requirement	C•CURE 9000 and iSTAR
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.	**Not applicable -** 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 Perimeter(s). **Note:** C•CURE 9000 documentation listed in Appendix A provides details on the Software House Security Patch Management. It is recommended that the responsible party register for Software House cyber security advisory email notifications - https://tycosecurityproducts.com/CyberProtection/Registration.aspx
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.	**Not applicable -** 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 Perimeter(s). **Note:** C•CURE 9000 documentation listed in Appendix A provides details on the Software House Security Patch Management. It is recommended that the responsible party register for Software House cyber security advisory email notifications - https://tycosecurityproducts.com/CyberProtection/Registration.aspx
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.	**Not applicable -** 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 Perimeter(s). **Note:** C•CURE 9000 documentation listed in Appendix A provides details on the Software House Security Patch Management. It is recommended that the responsible party register for Software House cyber security advisory email notifications - https://tycosecurityproducts.com/CyberProtection/Registration.aspx
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 process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.

Req ID	Requirement	C•CURE 9000 and iSTAR
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:** C•CURE 9000 is compatible with anti-virus 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.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R4 – Requirements and Measures; Security Monitoring

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

Req ID	Requirement	C•CURE 9000 and iSTAR
4.1.	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per 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: 4.1.1 Detected successful login attempts 4.1.2 Detected failed access attempts and failed login attempts 4.1.3 Detected malicious code.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 should be configured to use Windows Authentication. Successful login attempts are logged in C•CURE 9000. Both successful and unsuccessful login attempts will be recorded in Windows Active Directory access logs. **Note:** C•CURE 9000 applications are deployed in a Windows environment which can have anti-virus software installed for the purpose of detecting malicious code.
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 (per Cyber Asset or BES Cyber System capability): 4.2.1 Detected malicious code from Part 4.1. 4.2.2 Detected failure of Part 4.1 event logging.	**Not applicable -** Detection of malicious code is performed outside the CCURE 9000 environment and maintained by others. **Note:** It is possible to configure a limit and alert of unsuccessful authentication of C•CURE 9000 through Windows policy. **Note:** It is not technically feasible to limit or generate an alert of unsuccessful authentication attempt of the iSTAR Diagnostic Webpage or ICU. **Note:** It is possible to limit and alert of unsuccessful authentication of C•CURE 9000 through Windows policy. **Note:** C•CURE 9000 should be configured to use Windows Authentication for login. Successful login attempts are logged in C•CURE 9000. Both successful and unsuccessful login attempts will be recorded in Windows access logs.

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.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 should be configured to use Windows Authentication for login. Successful login attempts are logged in C•CURE 9000. Both successful and unsuccessful login attempts will be recorded in Windows access 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 process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.

Req ID	Requirement	C•CURE 9000 and iSTAR
5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** C•CURE 9000 should be configured for Windows authentication. **Note:** iSTAR Diagnostic Webpage: Web page requires a password set through C•CURE 9000. **Note:** iSTAR ICU: ICU commands require cluster password set through C•CURE 9000
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 type(s).	**Not applicable -** It is the responsibility of the Entity to identify and inventory all accounts. **Note:** No default C•CURE 9000 accounts. **Note:** iSTAR Diagnostic Webpage – generic account, responsible Entity should change the password. **Note:** ICU - generic account
5.3	Identify individuals who have authorized access to shared accounts.	**Not applicable -** The Entity is responsible to identify shared accounts. **Note:** C•CURE 9000 does not require shared accounts. **Note:** iSTAR Diagnostic Webpage – generic account **Note:** ICU - generic account
5.4	Change known default passwords, per Cyber Asset capability.	**Not applicable -** The Entity is responsible to change all default passwords. **Note:** C•CURE 9000 does not have default passwords. **Note:** iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual **Note:** ICU - Cluster password can be changed through C•CURE 9000 configuration. See C•CURE 9000 user manual

5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1 Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.	**Not applicable -** The Entity is responsible to enforce password complexity. **Note:** C•CURE 9000 should be configured for Windows authentication with the password complexity & lifespan set through the Microsoft Active Directory policy. **Note:** iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual. This requires a procedural enforcement. **Note:** ICU - Cluster password can be changed through C•CURE 9000 configuration. See C•CURE 9000 user manual. 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.	**Not applicable -** The Entity is responsible to enforce password complexity. **Note:** C•CURE 9000 should be configured for Windows authentication with the password complexity & lifespan set through the Microsoft Active Directory policy. **Note:** iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual. This requires a procedural enforcement. **Note:** ICU - Cluster password can be changed through C•CURE 9000 configuration. See C•CURE 9000 user manual. 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.	**Not applicable -** The Entity is responsible to enforce password changes. **Note:** C•CURE 9000 should be configured for Windows authentication with a policy to limit and alert of unsuccessful authentication. **Note:** It is not technically feasible to limit or generate an alert of unsuccessful authentication attempt of the iSTAR Diagnostic Webpage or ICU.

CIP–008–6: 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 plan(s) that collectively include each of the applicable requirement parts in CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications.

Req ID	Requirement	C•CURE 9000 and iSTAR
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: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 To provide notification per Requirement R4.	**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-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	Test each Cyber Security Incident response plan(s) 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 plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) 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 and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	**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-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1 Document any lessons learned or document the absence of any lessons learned; 3.1.2 Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 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: 3.2.1. Update the Cyber Security Incident response plan(s); and 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.

R4 – Requirements and Measures; Notifications and Reporting for Cyber Security Incidents

Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), 1 or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.

Req ID	Requirement	C•CURE 9000 and iSTAR
4.1	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

4.2	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
4.3	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	**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 plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Conditions for activation of the recovery plan(s).	**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, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). 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 plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.

Req ID	Requirement	C•CURE 9000 and iSTAR
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 plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery. 3.1.1 Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned. 3.1.2 Update the recovery plan based on any documented lessons learned associated with the plan. 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. 3.2.1 Update the recovery plan. 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.

CIP–010–3: Cyber Security – Configuration Change Management and Vulnerability Assessments

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

R1 – Requirements and Measures; Vulnerability Assessments

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R1 – Configuration Change Management.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1 Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2 Any commercially available or open-source application software (including version) intentionally installed; 1.1.3 Any custom software installed; 1.1.4 Any logical network accessible ports; and 1.1.5 Any security patches applied.	**Not applicable -** 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 Perimeter(s). **Note:** C•CURE 9000 documentation listed in Appendix A provides details on the Software House Security Patch Management. It is recommended that the responsible party register for Software House cyber security advisory email notifications - https://tycosecurityproducts.com/CyberProtection/Registration.aspx
1.2	Authorize and document changes that deviate from the existing baseline configuration.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.4	For a change that deviates from the existing baseline configuration: 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2 Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3 Document the results of the verification.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

1.5	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1 Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.6	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1 Verify the identity of the software source; and 1.6.2 Verify the integrity of the software obtained from the software source.	Not applicable - Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Cyber Security – Configuration Monitoring

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R2 – Configuration Monitoring.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Cyber Security; Vulnerability Assessments.

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R3– Vulnerability Assessments.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

3.2	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

CIP–011–2: Cyber Security – Information Protection

Assessments

Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection 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; Information Protection

Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Method(s) to identify information that meets the definition of BES Cyber System Information.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; BES Cyber Asset Reuse and Disposal

Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** For encrypting the system data at rest, see Microsoft SQL TDE
2.2	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** For encrypting the system data at rest, see Microsoft SQL TDE

CIP–012–1: Cyber Security – Communications between Control Centers

Assessments

Purpose: To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

R1 – Requirements and Measures; Information Protection

The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** To protect against unauthorized access to cyber assets see C-CURE 9000 v2.9 Hardening Guide, GPS0003-CE-20202905-EN
1.2	Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** To protect against unauthorized access to cyber assets see C-CURE 9000 v2.9 Hardening Guide, GPS0003-CE-20202905-EN
1.3	If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

CIP–013–1: Cyber Security – Supply Chain Risk Management

Assessments

Purpose: To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems..

R1 – Requirements and Measures; Information Protection

Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: 1.2.1 Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity; 1.2.2 Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity; 1.2.3 Notification by vendors when remote or onsite access should no longer be granted to vendor representatives; 1.2.4 Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity; 1.2.5 Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and 1.2.6 Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity. **Note:** for information on these topics go to https://www.swhouse.com/Products/software_CCURE9000.aspx

R2 – Cyber Security – Supply Chain Risk Management

Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

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

R3 – Cyber Security; Supply Chain Risk Management

Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

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

CIP–014–2: Physical Security

Assessments

Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

R1 – Requirements and Measures; Physical Security

Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Subsequent risk assessments shall be performed: • At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or • At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
1.2	The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R2 – Requirements and Measures; Physical Security

Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	Each Transmission Owner shall select an unaffiliated verifying entity that is either: • A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or • An entity that has transmission planning or analysis experience.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.2	The unaffiliated third party verification shall verify the Transmission Owner’s risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

2.3	If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation: • Modify its identification under Requirement R1 consistent with the recommendation; or • Document the technical basis for not modifying the identification in accordance with the recommendation.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
2.4	Each Transmission Owner shall implement procedures, such as the use of nondisclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R3 – Requirements and Measures; Physical Security

For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.1	If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R4 – Requirements and Measures; Physical Security

Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

Req ID	Requirement	C•CURE 9000 and iSTAR
4.1	Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
4.2	Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
4.3	Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R5 – Requirements and Measures; Physical Security

Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

Req ID	Requirement	C•CURE 9000 and iSTAR
5.1	Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
5.2	Law enforcement contact and coordination information.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
5.3	A timeline for executing the physical security enhancements and modifications specified in the physical security plan.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
5.4	Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

R6 – Requirements and Measures; Physical Security

Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.

Req ID	Requirement	C•CURE 9000 and iSTAR
6.1	Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following: • An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification. • An entity or organization approved by the ERO. • A governmental agency with physical security expertise. • An entity or organization with demonstrated law enforcement, government, or military physical security expertise.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
6.2	The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
6.3	If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation: • Modify its evaluation or security plan(s) consistent with the recommendation; or • Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.
6.4	Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.	**Not applicable -** Policies, procedures and training are the responsibility of the Responsible Entity.

APPENDIX A – Resources and References

For Tyco Security product cybersecurity resources visit the Johnson Controls Cyber Solutions page at www.johnsoncontrols.com/cyber-solutions/cyber-learning.

Here you can find the following documentation:

VideoEdge v5.6 Hardening Guide
VideoEdge v5.4 NERC-CIP v6 Compliance Guide
VideoEdge and victor v5.0 Port Assignments
Windows Firewall for Intellex
VideoEdge DISA Compliance Guide
VideoEdge FISMA Compliance Guide
victor FISMA Compliance Guide
C•CURE 9000 v2.9 Hardening Guide
C•CURE 9000 v2.9 and iSTAR Hardening Guide v1
C•CURE 9000/iSTAR Port Assignments
C•CURE 9000/iSTAR FISMA-Ready Compliance Guide
C•CURE 9000 v2.80/iSTAR NERC-CIP v6 Compliance Guide
C•CURE 9000/iSTAR Cybersecurity Overview Whitepaper