cyberprotection PROGRAM From Tyco Security Products

C•CURE 9000 and iSTAR
NERC-CIP V5
Compliance Guide

C•CURE 9000 v2.5
iSTAR v6.4

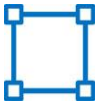
cyberprotection PROGRAM From Tyco Security Products

Proactively Monitoring and Managing Cybersecurity Risks

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

Secure Product Development Practices

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



Inclusive Protection of Components and Systems

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

Configuration Guidelines for Compliance

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

Testing Procedures

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

Rapid Response to Vulnerabilities

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

Education and Advocacy

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

Overview

This document provides an overview of the Tyco Security Products' NERC-CIP Ready Program and describes how the C•CURE 9000 and iSTAR System may be configured to meet the requirements of the NERC-CIP v5 requirements. 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.

Additional information is available in the *C•CURE 9000 and iSTAR Cybersecurity Overview Whitepaper*.

Conventions

Not Applicable: These controls are the sole responsibility of the Entity required to meet the control of NERC-CIP v5. 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.

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.

.

Contents

CIP–003–5: 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 BES.

R1 – 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	Personnel and training (CIP-004)	**Not Applicable -** The Responsible Entity is responsible for policy requirements.
1.2	Electronic Security Perimeters (CIP-005) including Interactive Remote Access.	**Not Applicable -** The Responsible Entity is responsible for policy requirements.
1.3	Physical security of BES Cyber Systems (CIP 006)	**Not Applicable -** The Responsible Entity is responsible for policy requirements.
1.4	System security management (CIP-007)	**Not Applicable -** The Responsible Entity is responsible for policy requirements.
1.5	Incident reporting and response planning (CIP-008)	**Not Applicable -** The Responsible Entity is responsible for policy requirements.
1.6	Recovery plans for BES Cyber Systems (CIP-009)	**Not Applicable -** The Responsible Entity is responsible for this requirement.
1.7	Configuration change management and vulnerability assessments (CIP-010)	**Not Applicable -** The Responsible Entity is responsible for this requirement. Software House Product Security Team can assist in vulnerability management.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.8	Information protection (CIP-011)	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.
1.9	Declaring and responding to CIP Exceptional Circumstances.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R2 – Cyber Security Policies

Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months:

2.1	Cyber security awareness.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
2.2	Physical security controls.	The C•CURE 9000 and iSTAR system has been tested and certified as an end-to-end physical access control system (PACS) with high assurance readers and validation software and approved as a fully compliant FICAM Solution by the U.S. General Services Administration (GSA).
2.3	Electronic access controls for external routable protocol connections and Dial-up Connectivity.	C•CURE 9000 Queries and Dynamic Views provide ability to create documentation of ESPs access points, and the Cyber Assets deployed for access control and monitoring of these points.

2.4	Incident response to a Cyber Security Incident.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R3 – 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 - The Responsible Entity is responsible for this requirement.

R4 – CIP Delegation

The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, 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 - The Responsible Entity is responsible for this requirement.

CIP–004–5.1: Cyber Security - Personnel and Training

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the 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 – Security Awareness Program

Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-5.1 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 -** The Responsible Entity is responsible for this requirement.

R2 – Cyber Security Training Program

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-5.1 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-** The Responsible Entity is responsible for this requirement. 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.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.3	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R3 – Personnel risk Assessment Program

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-5.1 Table R3 – Personnel Risk Assessment Program.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.1	Process to confirm identity.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
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 -** The Responsible Entity is responsible for this requirement.

Req ID	Requirement	C•CURE 9000 and iSTAR
3.3	Criteria or process to evaluate criminal history records checks for authorizing access.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
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 -** The Responsible Entity is responsible for this requirement.
3.5	Process to ensure that individuals with authorized electronic or authorized 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 -** The Responsible Entity is responsible for this requirement.

R4 – Access Management

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in CIP-004-5.1 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.	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.	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.

Req ID	Requirement	C•CURE 9000 and iSTAR
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.	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.	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

R5 – Access Revocation

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5.1 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).	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.	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	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.

Req ID	Requirement	C•CURE 9000 and iSTAR
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.	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.	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. 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–005–5: 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 – Electronic Security Perimeter

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

Req ID	Requirement	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.	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 -** The Responsible Entity is responsible for this requirement.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	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 and should be maintained and further defined by the Responsible Entity. C•CURE has documentation on firewall usage, only required ports to be opened. Access to C•CURE should be restricted to certain level of privileges defined by the Responsible Entity.
1.4	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R2 – Interactive Remote Access Management

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

Req ID	Requirement	C•CURE 9000 and iSTAR
2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	**Not Applicable -** The Responsible Entity is primarily responsible for this requirement.
2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	The encryption between C•CURE 9000 and the iSTAR Ultra, iSTAR Edge, and iSTAR eX controllers has achieved FIPS 140-2 and 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.	Utilizing Windows Active Directory, C•CURE 9000 may be employed using multi-factor authentication.

CIP–006–5: Cyber Security - Physical Security

Purpose: To manage physical access to 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 – Physical Security Plan

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.1	Define operational or procedural controls to restrict physical access.	**Shared –** The responsible entity shall document, implement, and maintain a physical security plan, approved by senior management. C•CURE 9000 provides a graphical maps feature which may be instrumental in the identification of physical access points through each Physical Security Perimeter.
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.	**Shared –** The responsible Entity shall write procedures for visitor control. C•CURE 9000 provides an Escorted Access feature which allows for the system to control, track and report on the movements of personnel designated Victors.

Req ID	Requirement	C•CURE 9000 and iSTAR
1.3	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	**Not Applicable -**The responsible Entity shall document and implement the operational and procedural controls to manage physical access points to the Physical Security.
1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	**Shared -** The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s). C•CURE 9000 is a powerful security and event management system which offers advanced monitoring capabilities to meet site specific security requirements. Alarm and /or Event activation can be linked to multiple triggers throughout the system to include door communication status of hardware device, etc.
1.5	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	**Shared** - The responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s). When installed in accordance to setup instructions, C•CURE/iSTAR will issue alerts within the 15 minutes requirement. This has been verified by UL as part of C•CURE and iSTAR's UL1076 approvals

Req ID	Requirement	C•CURE 9000 and iSTAR
1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	**Shared –** iSTAR controllers and card readers are installed with tamper detection. Additional supervised inputs may be employed to add tamper detection of ancillary equipment. 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.	**Shared –** 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. 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.
1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	**Compliant** – 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.	**Shared -** 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.

R2 – Visitor Control program

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in CIP-006-5 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.	**Compliant –** 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.	**Compliant –** 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.
2.3	Retain visitor logs for at least ninety calendar days.	**Shared -** 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 – Physical Access Control System Maintenance and testing Program

Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-5 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.	**Shared –** It is the responsibility of the Entity to implement a regular monitoring program. C•CURE 9000 and iSTAR monitor connection and can alert of malfunctions in real-time.

CIP–007–5: 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 BES.

R1 – Ports and Services

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 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.	See separate ports document
1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	**Shared –** iSTAR network ports are physically protected within the enclosure of the panel with lock and tamper detection. It is the responsibility of the Entity to protect the C•CURE 9000 server and workstations.

R2 – Security Patch Management

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 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.	**Shared** –Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, 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). See Software House Security Patch Management document.

Req ID	Requirement	C•CURE 9000 and iSTAR
2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	**Shared** –Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, 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). See Software House Security Patch Management document.
2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	**Shared** –Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, 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). See Software House Security Patch Management document.

Req ID	Requirement	C•CURE 9000 and iSTAR
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 -** The Responsible Entity is responsible for this requirement.

R3 – Malicious Code Prevention

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 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 -** The Responsible Entity is primarily responsible for this requirement.
3.2	Mitigate the threat of detected malicious code.	**Not Applicable -** The Responsible Entity is primarily responsible for this requirement.
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 -** The Responsible Entity is primarily responsible for this requirement. C•CURE 9000 and iSTAR updates are digitally signed

R4 – Security Monitoring

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 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.	C•CURE 9000 uses Windows access credentials for login. Successful login attempts are logged in C•CURE 9000. Both successful and unsuccessful login attempts will be recorded in Windows access logs.
4.2.	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; and 4.2.2. Detected failure of Part 4.1 event logging.	**Not Applicable -** This control is the responsibility of the organization.
4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	**Not Applicable -** The Responsible Entity is primarily responsible for this requirement..

Req ID	Requirement	C•CURE 9000 and iSTAR
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 – System Access Control

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-5 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.	C•CURE 9000 relies on the Windows authentication. iSTAR Diagnostic Webpage: Web page requires a password set through C•CURE 9000. 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).	**Shared –** It is the responsibility of the Entity to identify and inventory all accounts. No default C•CURE 9000 accounts. iSTAR Diagnostic Webpage – generic account ICU - generic account
5.3	Identify individuals who have authorized access to shared accounts.	**Not Applicable –** The Entity is responsible to identify shared accounts. C•CURE 9000 does not require shared accounts. iSTAR Diagnostic Webpage – generic account ICU - generic account

Req ID	Requirement	C•CURE 9000 and iSTAR
5.4	Change known default passwords, per Cyber Asset capability.	**Not Applicable -** The Entity is responsible to change all default passwords. C•CURE 9000 does not have default passwords. iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual 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.	**Shared** – The Entity is responsible to enforce password complexity. C•CURE 9000 password complexity can be set through Windows policy. iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual. This requires a procedural enforcement. ICU - Cluster password can be changed through C•CURE 9000 configuration. See C•CURE 9000 user manual. This requires a procedural enforcement.

Req ID	Requirement	C•CURE 9000 and iSTAR
5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	**Shared** – The Entity is responsible to enforce password changes. C•CURE 9000 password lifespan can be set through Windows policy. iSTAR Diagnostic Webpage password can be changed through C•CURE configuration. See C•CURE 9000 user manual. This requires a procedural enforcement. 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.	**Shared** – The Entity is responsible to enforce password changes. It is possible to limit and alert of unsuccessful authentication of C•CURE 9000 through Windows policy. It is not technically feasible to limit or generate an alert of unsuccessful authentication attempt of the iSTAR Diagnostic Webpage or ICU.

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

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

R1 - Cyber Security Incident Response Plan Specifications Part Applicable Systems Requirements

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-008-5 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 -** The Responsible Entity is responsible for this requirement.
1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
1.4	Incident handling procedures for Cyber Security Incidents.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R2 – Cyber Security Incident Response Plan Implementation and Testing

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

Req ID	Requirement	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 -** The Responsible Entity is responsible for this requirement.
2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
2.3	Retain records related to Reportable Cyber Security Incidents.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

R3 – Cyber Security Incident Response Plan Review, Update, and Communication

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

Not Applicable - The Responsible Entity is responsible for this requirement.

CIP–009–5: 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 – Recovery Plan Specifications

Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in CIP-009-5 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 -** The Responsible Entity is responsible for this requirement.
1.2	Roles and responsibilities of responders.	**Not Applicable -** The Responsible Entity is responsible for this requirement.
1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	**Shared -** The Responsible Entity is responsible for this requirement. The C•CURE 9000 Server Configuration Application Guide describes the details for performing system backup and restore. iSTAR controllers will automatically update their database when connected to C•CURE 9000. Stratus Technologies' everRun Enterprise and Express, and SplitSite provide a high availability, fault tolerant solution for C•CURE 9000 systems.

Req ID	Requirement	C•CURE 9000 and iSTAR
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 -** The Responsible Entity is responsible for this requirement.
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 -** The Responsible Entity is responsible for this requirement.

R2 – Recovery Plan Implementation and testing

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-5 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 -** The Responsible Entity is responsible for this requirement.
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 -** The Responsible Entity is responsible for this requirement.
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 -** The Responsible Entity is responsible for this requirement.

R3 – Recovery Plan Review, Update and Communication

Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in CIP-009-5 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; and 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 -** The Responsible Entity is responsible for this requirement.
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; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	**Not Applicable -** The Responsible Entity is responsible for this requirement.

APPENDIX – Resources and References

Tyco Documents

- VideoEdge NVR Security User Guide
- VideoEdge NVR Installation and User Guide
- VideoEdge, victor, and C•CURE Port Map
- FISMA-Ready: VideoEdge System
- FISMA-Ready: victor System
- FISMA-Ready: C•CURE 9000 System
- CCURE 9000 and iSTAR Cybersecurity Overview White Paper

Laws and Regulations

- Federal Information Security Management Act of 2002
- Federal Information System Modernization Act of 2014

FIPS Publications

- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS PUB 197, Advanced Encryption Standard
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems

NIST Publications

- NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST 800-30, Risk Management Guide for Information Technology Systems
- NIST 800-34, Contingency Planning Guide for Information Technology Systems
- NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems

- NIST 800-53 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
- NIST 800-60 Rev1, Guide for Mapping Types of Information and Information Systems to Security
- NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
- NIST 800-64, Security Considerations in the Information System Development Life Cycle
- Framework for Improving Critical Infrastructure Cybersecurity