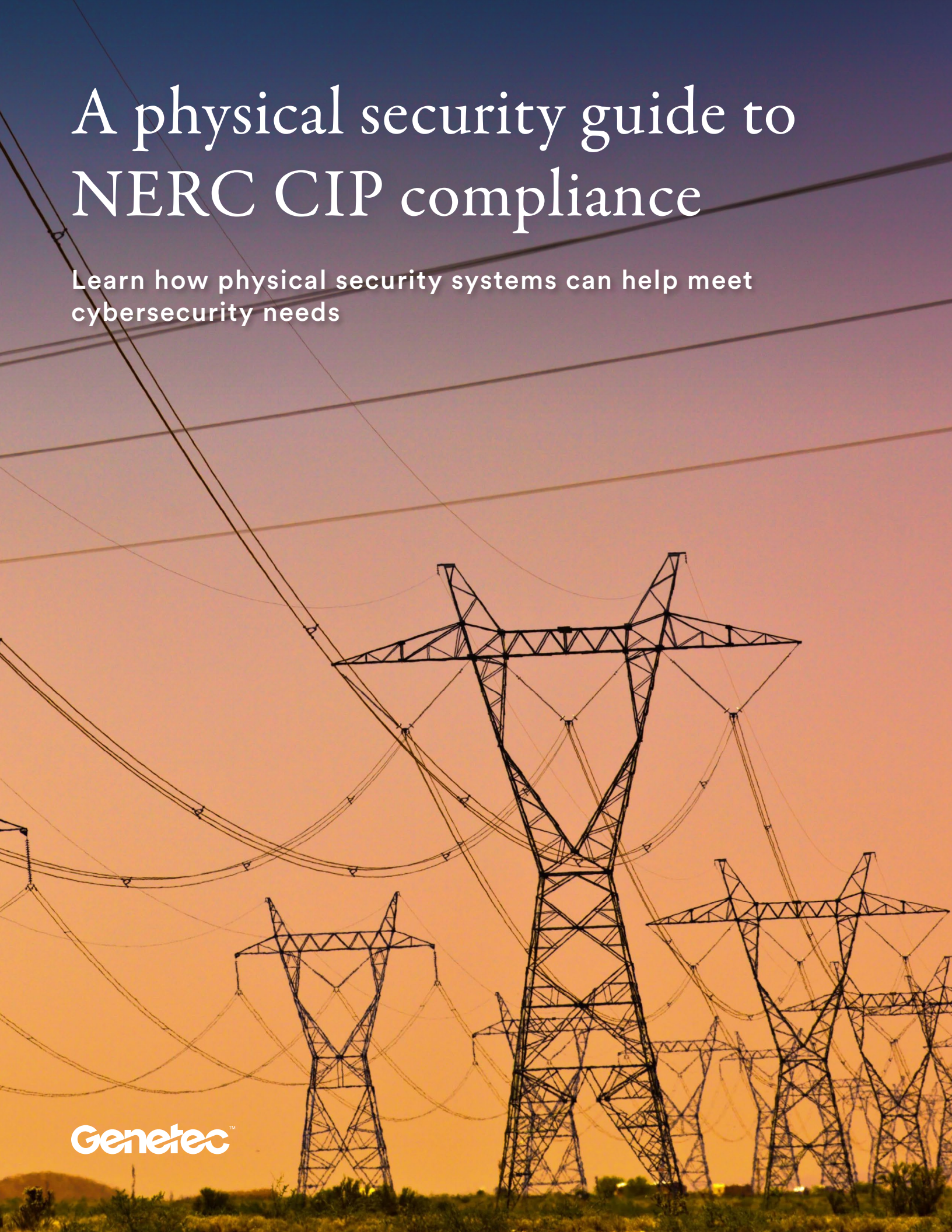
# A physical security guide to NERC CIP compliance

**Learn how physical security systems can help meet cybersecurity needs**



Genetec™

# Contents

# Who is NERC?

The North American Electric Reliability Corporation (NERC) is a non-profit regulatory authority with the mission of assuring the effective and efficient reduction of risks to the reliability and security of the North American bulk power system.

NERC has the responsibility of developing standards for the power system operations and monitoring and enforcing compliance of these regulatory standards.

# What is NERC CIP?

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) plan is the set of standards put together by NERC aimed at regulating, enforcing, monitoring, and managing the security of the Bulk Electric System (BES) in North America.

In this NERC CIP guidebook, you will find an overview of each NERC CIP requirement, a quick summary of what each requirement seeks to achieve, as well as recommendations on what to look for in a system to meet these requirements. We also included expert tips that will help you achieve compliance.

| CIP Critical Infrastructure Protection | | Checklist |
|---|---|---|
| CIP-002-5.1a | Cybersecurity – BES Cyber System Categorization | |
| CIP-003-8 | Cybersecurity – Security Management Controls | |
| CIP-004-6 | Cybersecurity – Personnel & Training | |
| CIP-005-6 | Electronic Security Perimeter(s) | |
| CIP-006-6 | Physical Security of BES Cyber Systems | |
| CIP-007-6 | System Security Management | |
| CIP-008-6 | Cybersecurity – Incident Reporting & Response Planning | |
| CIP-009-6 | Cybersecurity– Recovery Plans for BES Cyber Systems | |
| CIP-010-3 | Cybersecurity – Configuration Change Management & Vulnerability Assessments | |
| CIP-011-2 | Cybersecurity – Information Protection | |
| CIP-013-1 | Cybersecurity – Supply Chain Risk Management | |
| CIP-014-2 | Physical Security | |

1

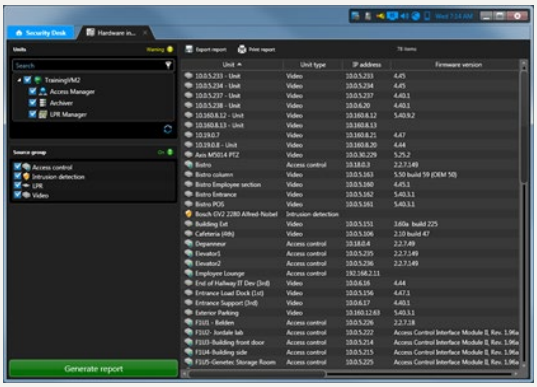
# CIP-002-5.1a: Cybersecurity – management controls

## Purpose of the requirement:

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cybersecurity 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.

| What to achieve? | What can help? | Tip |
|---|---|---|
| Categorize different BES Cyber Systems based on potential impact level (High, Medium, Low) to better understand how to manage vulnerabilities and protect these assets while regularly maintaining and reviewing them. | Look for systems that can provide you with an up-to-date breakdown of all connected devices and their statuses. | This will help you simplify your review process as you will have a clear view of all your device statuses in real-time to know which requires immediate attention. |

**Genetec solution**



Customers need to address the impact of their security system, along with other assets.

Should the physical security system be part of the list, Security Center can provide, through the Hardware Inventory task, a list of peripherals connected with their status. To simplify maintenance of these connected devices, Security Center also enables you to keep an up-to-date list of connected peripherals on the system in its hardware inventory.

Additionally, data on each peripheral connected and their statuses may be leveraged to support audits.

2

# CIP-003-8: Cybersecurity – security management controls

## Purpose of the requirement:

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 Electric System (BES).

| What to achieve? | What can help? | Tip |
|---|---|---|
| Define and regularly review cybersecurity policies and establish clear responsibility and accountability, procedures, and plan of action in the event of any cybersecurity incidents in your BES Cyber Security Systems. | Invest in a security system that can help guide your security teams through their incident responses with digitized SOPs that are following your organization-specific processes and compliance requirements. | This will help reduce potential human error and ensure compliance while simplifying the audit and reporting process. |

**Genetec solution**

While policies, procedures, and plans are the responsibility of the customer, Genetec provides the following services and features that can be part of the plan:

- Technical training certification to ensure users can operate our physical security system securely and efficiently.
- Access control to the system is assured with secure authentication and a sophisticated set of role-based user privileges that follow the least access principle.
- A decision management system, Mission Control™ that collects and qualifies data from thousands of sensors, and security devices (SCADA, OPC, RADAR, cameras, readers etc.), identifies the most complex incidents or situations and guides security teams through their responses following organization-specific processes and compliance requirements.
- Built-in failover role (NEC clustering and Windows failover clustering).
- Comprehensive audit trails.
- Encryption in transit is assured by TLS1.3, and encryption at rest follows the latest encryption standards.

3

# CIP-004-6: Cyber security – Personnel and Training

## Purpose of the requirement:

To minimize the risk of 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.

| What to achieve? | What can help? | Tip |
|---|---|---|
| Minimize potential vulnerabilities and errors caused by employees when accessing BES Cyber Systems to conduct security awareness training programs, running regular background checks on employees with high levels of access, and ensuring that user accounts, account groups, role categories, and their specific privileges are accurate and up to date. | Look for a system that can support you in managing identity and access rights based on each employee's attributes whether contracted or staffed, while being fully unified with your access control system. | This will streamline your efforts in managing different cardholder accesses going into your protected areas. |

**Genetec solution**

Security Center Synergis™ IP access control provides the following features that can help you comply with these requirements:

- Access rules, which specify who can pass through a door and when. A very granular and specific set of rules, on schedules, can be applied to each cardholder.
- Cardholder expiration, which can be automatically set to ensure compliance with regular verification of access rights.
- Visitors or cardholders who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.
- Visitor management, which automates the check-in and check-out process for visitors, monitors their accesses and provides reports of their visit.
- Security Center supports integration with Active Directory which permits centralized user management at the Windows level. User groups from Active Directory can be synchronized with Security Center so that when new users are added or removed from an Active Directory user group, they will be added or removed from Security Center.
- If the cloud is supported by your organization, ClearID™, a self-service identity and access management (IAM) solution, can help track which staff members have gone to which training and when. ClearID is a management layer designed to automate and optimize your security provisioning, de-provisioning, and structured audit policies.

4

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

## Purpose of the requirement:

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.

| What to achieve? | What can help? | Tip |
|---|---|---|
| Secure access to BES Cyber Systems by keeping your critical assets within a designated electronic security perimeter to be able to closely monitor them in case of suspicious activity. | Ensure all systems that are connected to your network infrastructure require secure authentication and communications that are encrypted using the latest security protocol and users that have role-based permissions to access critical assets. | Make sure an activity trail report of access is available for you to simplify investigations or audits. |

**Genetec solution**

While network infrastructure is the responsibility of the customer, Genetec Security Center provides the following features to help with these requirements:

- Security Center extends encryption standards up to the edge to protect the last network segment established with video and access control devices. Security Center ensures communications are secured between client-servers, servers-servers and, if the edge (video unit, access control) permits it, between edge-client applications and edge-servers.
- Required Security Center ports are documented and should be the only ones configured on the firewall.
- Built-in capability to leverage “proxy” configurations allowing you to minimize ports that need to be open to a firewall.
- No dial-up connectivity is required with Security Center.

**Genetec solution**

- For an on-premises deployment, communications would reside within the ESP. When remote communications are necessary, they are secured using TLS 1.3, which leverages both encryption and digital certificates that are authenticated. (Web interface or remote sites). These communications can also be managed through VPN or network restrictions.
- Security Center supports passive authentication (also known as web-based authentication) to provide multifactor authentication functions. To achieve a seamless and secure single sign-on experience, Security Center supports third-party authentication using OpenID Connect and SAML 2.0. These authentication protocols are used by leading identity providers. Security Center also provides multifactor authentication through Microsoft Active Directory.
- Any user session, remote or otherwise, can be seen in Security Center by a system administrator and terminated by setting the user account to “inactive”.
- All user sessions, remote or otherwise, are logged within the activity trail audit report.

5

# CIP-006-6: Cybersecurity – physical security of BES cyber systems

## Purpose of the requirement:

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.

| What to achieve? | What can help? | Tip |
|---|---|---|
| Protect and manage physical access to BES Cyber Systems by defining a physical security plan to manage intrusions and unauthorized access into protected areas. | Look for a reliable physical access control system that can be seamlessly paired with a visitor management solution to heighten your organization's security and increase your readiness to respond to incidents while meeting all compliance requirements. | Ensure that a full reporting functionality is available for you to keep track of log access attempts and cardholder & visitor activity for incident investigations. |

**Genetec solution**

Synergis, the IP access control system heightens the organization's security and increases readiness to respond to incidents. As part of Security Center, Synergis provides the following features that allow compliance with the requirements above:

- Restricts unescorted physical access to authorized cardholders.
- Allows multiple credentials requirements (Card and/or PIN, biometrics, etc).
- Issue alarms for unauthorized access attempts and other unwanted behavior (door held open too long, tailgating).
- Log access attempts and cardholder activities, including location and timestamp.
- Visitors or cardholders who have an escort are not granted access through access points until both they and their assigned escort (cardholder) present their credentials within a certain delay.
- Communications are encrypted using TLS1.3, which leverages both digital certificates and encryption.
- Security Center can send alerts when components become offline, which helps mitigate risks associated with device tampering.
- Cardholder activities, as well as user activities are logged and retained for the required duration.

## Genetec solution

- “Host groups” can enforce not only simple visitor escort capabilities but also compound visitor escort capabilities

**Security Center also provides two methods to manage visitors.**

- First, through a native visitor management module within Security Center. With this module, your operators and staff can manage visitors alongside other security activities, such as pre-enrolling visitors using a web or client application, making it easier for your security staff or administrative assistants to check in visitors when they show up at the front entrance. A full report and tracking are also available. You can investigate events related to visitors (access denied, first person in, last person out, anti-passback violation, and so on), using the Visitor activities report. In Security Desk, the user interface application, you can see all the areas and doors that a visitor accessed during their stay. If you want to check for any critical events that occurred on your site on the last day with visitors, you can set a time range for the report.

- Mission Control is a decision management system in Security Center and provides new levels of situational intelligence, visualization, and complete incident management capabilities. Incidents that cover unescorted visitors can be created and manually triggered when such situations are identified and will include step-by-step instructions that will guide operators to resolution following required policies. Records of these activities are accessible via the Mission Control reporting features for tracking purposes and to offer full transparency during audits and investigations.

- We support several third-party visitor management solutions that are already able to be integrated with Genetec.

- Alternatively, if your organization can support the cloud, Genetec ClearID can be used as an add-on. ClearID, the management layer designed to automate and optimize your security processes and policies, provides a visitor management module, which includes a registration portal, mobile check-in, and self-service kiosk. In the Visitor Registration portal, you can use the intuitive dashboard to invite visitors to specific locations for specific dates and times. You can select a meet-up location, parking location, and more. By entering a visitor’s email, the system will know if the person is a recurring visitor or not, making the process quicker, and will create a transparent profile for the user. Once you have created the visitor profile, you can add hosts, get visitor notifications when someone arrives, and send confirmation and meeting information to visitors through email, which they can add to their personal calendars. The system includes full reporting functionality as well.

6

# CIP-007-6: Cyber security - Systems Security Management

## Purpose of the requirement:

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).

| What to achieve? | What can help? | Tip |
|---|---|---|
| Reinforce BES Cyber Systems protection by defining and implementing technical, operational, and procedural requirements that include open ports and services, patch management, malicious code detection and alert, event logs, and user access control. | To ensure security policies are actively enforced, look for systems that can provide you with system health dashboards, automatic firmware updates/ patches, alerts on failed log-in attempts with activity trail as well as the ability to govern and synchronize user access rights that automatically updates within your identity and access management system. | Look for a unified access control and identity management system to reduce your need to work with multiple disparate systems. |

**Genetec solution**

Security Center features that support the above requirement:

- Provides a list of required logical ports with their use. Security Center also allows only authorized users to export data from the database. When using Genetec Streamvault appliances, the operating system, databases, and software are pre-installed. The pre-loaded hardened OS changes over 200 settings in Windows to configure GPO, registry keys, anti-virus, NetBIOS, and more to provide extra layers of cybersecurity.
- Supplies a cybersecurity dashboard widget to track system security and identify potential vulnerabilities in real-time.
- Undergoes stringent security testing for each release, such as vulnerability assessments and penetration testing conducted by specialized third parties. When security patches or updates are necessary, Security Center includes an automatic update service called the Genetec Update Service (GUS), which is like the Microsoft Windows Update.
- The Genetec Update Service (GUS) works in proxy mode.
- Firmware upgrades can also be managed through Security Center for a centralized approach. The latest tested firmware versions are also available through the Genetec Update Service.

## Genetec solution

**Security Center supports two types of user management:**

- Firmware is certified and secured by Genetec to ensure its authenticity.
- Provides a comprehensive Activity Trail Report, which logs successful and failed login attempts, for the required period. Alerts can be generated for failed login attempts and Activity trail reports can be generated automatically by an authorized administrator and sent for review by the responsible entities within the report pane of Security Center.
- **Local user management (native to Security Center):** In this case, users or user groups are created locally using the User Management module of Security Center. Our User Management module has advanced features including setting password expiry and policy, which are not available through the local Windows user management functionality.
- **User management through Active Directory:** In this case, user management is centralized at the Active Directory level. Security Center handles synchronizing user groups and managing their rights and permissions. This integration centralizes user management at the Windows level. User groups from Active Directory can be synchronized with Security Center so that when new users are added or removed from an Active Directory User Group, they will be added or removed from Security Center. Security Center can provide multifactor authentication through Microsoft Active Directory for authentication and single sign-on.

7

# CIP-008-6: Cyber security - Incident Reporting and Response Planning

## Purpose of the requirement:

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

| What to achieve? | What can help? | Tip |
|---|---|---|
| Put in place procedures to identify, classify, and respond to cybersecurity incidents and keep complete records of the incident and management process for reporting to the Electricity Information Sharing and Analysis Center (E-ISAC) for forensic analysis. | Having a centralized system that keeps a complete log of network activity and access, as well as a full history of the asset configuration data will simplify your investigation and recovery process when required. | Look for technology partners that can provide you with emergency support in case of a catastrophic system failure or cyberattacks. |

**Genetec solution**

While the Cyber Security Incident response plan is the responsibility of the customer, the GTAC Crisis Response Center from Genetec is available 24 hours a day, and 7 days a week to offer you emergency support by email, phone, and even onsite at your facility. Our engineers are specialized in rapid response to support you in situations such as catastrophic system failure or cyberattack.

8

# CIP-009-6: Cyber security - Recovery Plans for BES Cyber Systems

## Purpose of the requirement:

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.

| What to achieve? | What can help? | Tip |
|---|---|---|
| Define a recovery plan for the BES Cyber Systems in the event of a cyber-attack on the Bulk Electric System (BES). | To better support potential disaster recovery, look for systems that provide full failover and redundancy architecture, as well as the ability to distribute them across multiple servers and geographical sites. | Place a Disaster Recovery Directory at an off-site location where it will only kick in when all other Directory servers are down. |

**Genetec solution**

While the recovery plan is the responsibility of the customer, Security Center provides a high availability and disaster recovery configuration called Failover to help plan the recovery in case of failure.

- The main components of Security Center are roles. The roles execute a specific set of tasks related to any of the core systems. They also provide a full failover and redundancy architecture, as well as the possibility of distributing them across several servers and multiple geographic sites.
- A high-availability and failover functionality are provided through the built-in Failover role or off-the-shelf industry standards, such as NEC Clustering and Windows failover clustering. Either one, or both together, can be used depending on the level of operation required and the distribution of the services.
- Security Center also includes an option to designate one or many of the Directory servers as a “Disaster Recovery” server. The Disaster Recovery Directory is then excluded from load balancing (the others stay in load balancing mode). This is ideal for implementations where the Disaster Recovery Directory is placed at an off-site location, as no traffic will go through it, and it will only kick in when all other Directory servers are down.

9

# CIP-010-3: Cyber security - Configuration Change Management and Vulnerability Assessments

## Purpose of the requirement:

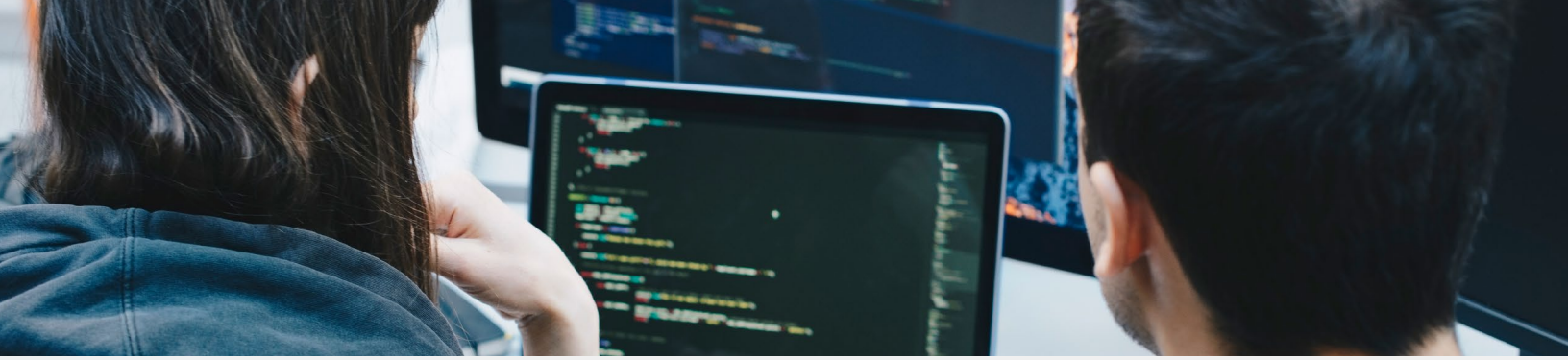
To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

| What to achieve? | What can help? | Tip |
|---|---|---|
| Develop a baseline configuration for each critical cyber asset and monitor them for any deviations from that baseline to better assess each asset's vulnerabilities. | Make sure the critical systems you invest in can provide you with a comprehensive audit trail report that tracks all changes made by system administrators and configuration files so that they can be easily compiled for the NERC CIP compliance audit. | Technology partners that regularly conduct vulnerability assessments and penetration tests on their products can support the documentation of your system assessment reporting. |

**Genetec solution**

While configuration management remains the customer's responsibility, Security Center provides configuration files and a comprehensive Audit trail report that tracks all changes made by system administrators.

Genetec regularly conducts vulnerability assessments and penetration tests on each of its products. Although it does not replace assessments required on the customer's system, a summary of the penetration results, available under NDA, can be added to the required documentation.



10

# CIP-011-2: Cyber security - Information Protection

## Purpose of the requirement:

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).

| What to achieve? | What can help? | Tip |
|---|---|---|
| Put in place measures to protect and securely handle the storage, transit, use and retrieval of data related to BES Cyber Systems to prevent data theft or hacking. | Only permit those who are essential to the operation of the BES to have access to the system.<br><br>Ensure that information stored in your databases is encrypted at rest and in transit. | Put in place a “least possible rights” control mechanism for access with multi-factor authentication. |

**Genetec solution**

Information stored in Security Center databases is encrypted at rest. Network communication is secured using TLS1.3, which leverages both digital certificates and encryption. Access to information is controlled by a role-based least possible rights mechanism. Authentication in the system is secured through multifactor authentication. These best practices can be included in the documentation about information protection..

Data export, in Security Center, can only be accomplished by authorized system administrators. Information at rest is encrypted, reducing the risk of data misuse. Data storage media purge and destruction remain the responsibility of the customer.

11

# CIP-013-1: Cyber security - Supply Chain Risk Management

## Purpose of the requirement:

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 mis-operation or instability in the Bulk Electric System (BES).

| What to achieve? | What can help? | Tip |
|---|---|---|
| Develop a supply chain cyber security risk management plan to identify and assess risk to BES posed by vendor products or services. | Ensure all critical vendors that are supporting the smooth functioning of the BES have clear cyber security guidelines in place that will not put the BES at risk. | Tip: Ensure that your system providers do not have access to your system by default without consent, particularly in a system-to-system remote access scenario.<br><br>Here are 6 questions you should ask your vendors to better manage your supply chain risk. |

**Genetec solution**

At Genetec, there is a trained incident response team to respond to security incidents. Security incidents will also be published as a security advisory on our website. An email will be sent to all affected end customers. You can also subscribe to our security advisory channel to stay on top of all advisories. More information is available here.

12

# CIP-014-2: Physical Security

## Purpose of the requirement:

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

| What to achieve? | What can help? | Tip |
|---|---|---|
| Identify and protect critical infrastructure within BES and implement measures to ensure their protection from physical attacks that may result in power outages. | Invest in a unified physical security platform that allows you to manage video surveillance, access control and perimeter intrusion detection systems together on a single pane of glass.<br><br>This will give you complete visibility of your entire operations and allow you to view all local and remote sites on the same user interface. | Take proactive measures to identify potential intruders at your protected site with solutions that enable you to monitor beyond your fence line to pre-classify potential intruder threat levels, and reduce nuisance alarms. |

**Genetec solution**

Although planning and evaluation of physical threats is the responsibility of the customer, using physical access control, perimeter protection, intrusion detection and even drones can be part of that plan. Security Center offers a unified platform that allows managing these different physical protection assets (video surveillance, access control, perimeter intrusion detection, license plate recognition systems etc.) through one pane of glass.

With the ability to unify third-party security and business systems with Security Center, you can seamlessly control all operations, while providing users with the power to rapidly respond to emerging situations. A unified system not only provides greater control, but can also help you avoid the pitfalls of traditional security systems, such as limited connectivity between various applications, compatibility issues, and complicated and costly maintenance.

When used as a unified platform, Security Center allows for the management and monitoring of all the above-mentioned sub-systems from a single client application. There is no need to load multiple applications or get trained on separate user interfaces. Monitoring, reporting, and configuration tasks are consolidated within Security Center, providing your team with the most efficient approach to managing your security systems.

Additionally, Security Center Restricted Security Area (RSA) Surveillance brings detection technologies such as radar, lidar, laser, video analytics and fence sensors to be managed together in a single view in Security Center. With advanced tracking, zone management, threat identification, and classification capabilities embedded in the solution, your team will have greater situational awareness and control over any incident.

# Recommendation

Regulatory changes and evolving security risks can place stress on an infrastructure owner's need to stay ahead of the curve. Investing in a unified security portfolio will help your team lower security risk, improve your safety response, and improve compliance with regulations.

The Genetec portfolio of solutions for the energy and utility sector offers critical infrastructure owners a one-stop shop for unified security solutions that will change the way you collaborate with safety and operational compliance teams so that you build a safer place to work.

Learn more about our solution offerings for critical infrastructure here.

genetec.com/industries/energy-utilities/portfolio

**As part of the IoT, IP-based physical security systems play a big role in our public and private networks, and, given their increasing size and distribution, it's important that we keep them secure. Hardening our security systems against criminal cyber activity is becoming a primary concern for governments and organizations alike. It's clear we need to be better prepared.**

**At Genetec™, we develop solutions that can secure all aspects of your physical security system, including communications, servers and data, both on-premises and in the Cloud. With strategies including security at the edge, encryption, authentication and authorization, we are working to ensure the security of your security system.**

**Omnicast:** Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

**Synergis:** The Synergis™ IP access control system (ACS) provides full control over your access points and secured areas. Your team can work unimpeded while your system is always available with built-in failover and peer-to-peer communications.

**ClearID:** Automate your security policies and build a strong access management plan throughout multiple sites with Genetec ClearID™. Centrally manage the access rights of visitors, employees, and contractors to help maintain compliance and security.

**Restricted Security Area Surveillance:** Detect intruders before they reach your fence line while reducing the likelihood of false alarms. Leverage a combination of laser and radar detection technology to detect, deter, and respond to intruders and drones.

**Mission Control:** Effectively guide your security operators through security and safety incidents as well as operational tasks with Genetec Mission Control™. Ensure that your team is complying with regulations like NERC-CIP by creating SOPs designed with compliance in mind.

**Clearance:** Use Genetec Clearance™ to securely collect, manage, and share digital evidence from different sites with regulators and law enforcement. Genetec Clearance is ideal for flare monitoring and for reporting intrusion incidents to regulators.

## To learn more about how you can protect your physical security system, visit:

genetec.com/trust-cybersecurity

**Genetec Inc.**
Genetec.com
info@genetec.com
@genetec

UDPT: 11-AUG-2022