

# NERC CIP Best Practices

with Inductive Automation and Ignition



(800) 266-7798

[inductiveautomation.com](http://inductiveautomation.com)

## Table of Contents

Introduction	2
Getting Started	2
Ignition by Inductive Automation	2
What is NERC and CIP?	2
NERC ERO Enterprise and Regional Entities	3
About This Guide	3
Organizations and Guidance	4
NERC	4
FERC	4
E-ISAC	4
NATF	5
Critical Infrastructure Protection (CIP) Standards	6
Convention	7
Key Concepts	7
Shared Responsibility Model	7
Customer	7
Software Vendor	8
Vendor support Matrix	8
Consultants or System Integrators	9
Cloud Service Providers	9
Software/Platform as a Service (SaaS/PaaS)	9
CIP Vendor Best Practices with Inductive Automation	10
Ignition Best Practices in a secure environment	15
NERC CIP Compliance with Inductive Automation and Ignition	18
CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)	18
CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments	21
CIP-013-2 – Cyber Security - Supply Chain Risk Management	25
Rationale	28
Appendix A - Glossary of Terms	29
Appendix B - References	31
Source References	31
Derivative reference material	31

# Introduction

## Getting Started

Welcome to Inductive Automation's (IA) guide on best practices using Ignition and working with software vendors in a CIP-compliant way. This guide depends on a Shared Responsibility model and is written with the United States in mind, but can be adapted to other areas that adhere to NERC CIP such as certain Canadian provinces and Mexican states. [NERC CIP Compliance with IA and Ignition](#) provides Responsible Entities (RE) with recommendations based on specific CIP standards. This guide recommends adhering to accepted process norms and applying modern technologies and security patterns, even when not explicitly required. This will provide better outcomes, align with regulatory intent and future direction, and should be valued by auditors.

## Ignition Software in NERC CIP-Regulated Environments

Inductive Automation is committed to enabling customer success with regulated applications.

### What is NERC and CIP?

Critical Infrastructure Protection (CIP) is a set of standards promulgated by North American Electric Reliability Corporation (NERC), designed to secure assets operating as part of North America's Bulk Electric System (BES).

## NERC ERO Enterprise and Regional Entities

NERC organizes as the Electric Reliability Organization (ERO) Enterprise that consists of NERC and six Regional Entities (REs) that perform complementary roles.

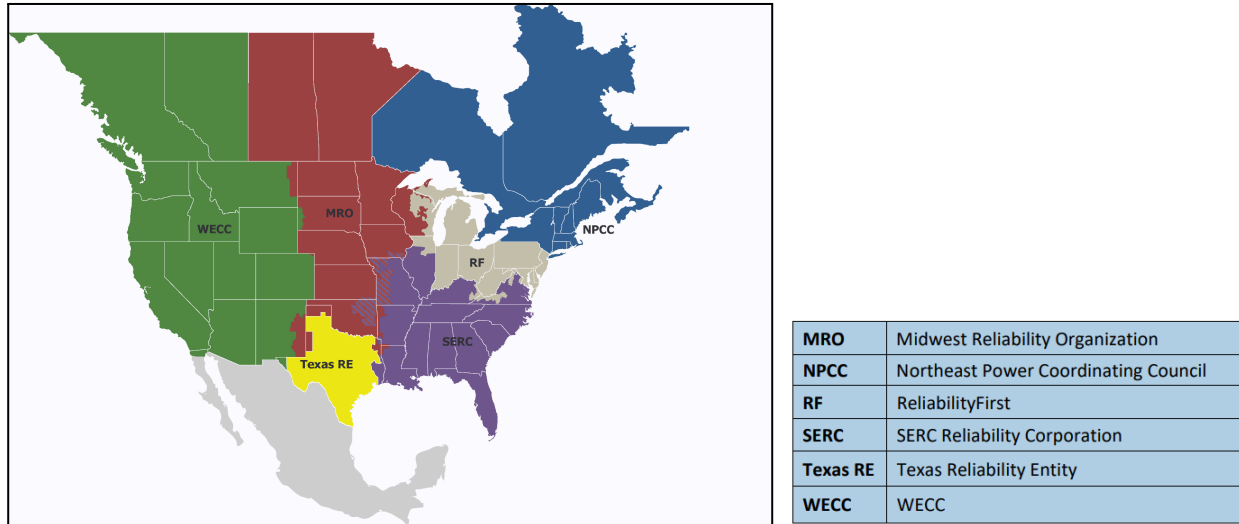


Figure 1: Governance

The US Federal Energy Regulatory Commission (FERC) is an Executive Branch entity under the US Department of Energy. FERC is granted legal authority under the Energy Policy Act of 2005 (US Public Law 109-58) and other congressional orders and regulations ([FERC Legal](#)). FERC designated NERC as the Electric Reliability Organization ([ERO Rules](#), 18 CFR Part 39). The ERO proposes and enforces Reliability Standards for the Bulk-Power System in the United States. This includes maintaining standards, compliance monitoring, and compliance enforcement through Regional Entities ([NERC Compliance & Enforcement](#)).

## About This Guide

The purpose of this document is to provide industry-specific background information and show how compliant applications can be built using Ignition with standard technologies. It proposes a “shared responsibility” model between the customer, software vendors, and service providers.

The most directly relevant portion for most stakeholders is probably addressing CIP-013 cybersecurity supply chain risk management for vendors, with information specific to Ignition and Inductive Automation.

Many requirements can be satisfied with customer procedural and administrative controls, requiring few technical controls. However, it is a common pitfall to approach each requirement in isolation. This can lead to ineffective implementation decisions, such as considering security as an entirely “application layer” problem. Inductive Automation believes that the best way to



succeed with CIP applications is to understand appropriate guidance, adhere to industry best practices, consider modern IT and OT technologies based on customer requirements, and risk assessment backed by subject matter expertise. Modern external systems offer strong security controls that can meet or exceed CIP requirements, but can also introduce new risks based on the reliance upon outside entities. The same concept applies to System Integrator and service provider deliverables. It is ultimately the Responsible Entity's responsibility to meet CIP compliance, which includes auditing their vendors and service providers.

## Organizations and Guidance

### NERC

"The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

"NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves nearly 400 million people." About NERC: <https://www.nerc.com/AboutNERC/>.

NERC offers a One-Stop Shop (Compliance Monitoring & Enforcement Program) (<https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx>). This includes NIST Cybersecurity Framework (CSF) mapping to NERC CIP among other useful resources.

### FERC

The Federal Energy Regulatory Commission, or FERC, is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects.

FERC issues numbered Orders and Rules, including Final Rules, Notices, Letter Orders, Delegated Orders, and other issuances.

### E-ISAC

The Electricity Information Sharing and Analysis Center (E-ISAC) reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration.

Created in 1999, the E-ISAC offers the electricity industry quality analysis and rapid sharing of security information on how to mitigate complex, constantly evolving threats to the grid. This includes a 24/7 Watch, expert in-house analysis of ongoing incidents, and a suite of analytical products and services accessible through the secure E-ISAC Portal.

The E-ISAC Portal serves as the central information hub for approved users at its member and partner organizations. Through the Portal, users can voluntarily post and exchange information about cyber and physical incidents with full control of how they share it. Interested individuals can learn more about joining the E-ISAC and benefits at the [Join the E-ISAC page](#).

The E-ISAC is operated by the North American Electric Reliability Corporation (NERC) and is organizationally isolated from NERC's enforcement processes. NERC and the E-ISAC adhere to a strict Code of Conduct.

### NATF

The North American Transmission Forum ([NATF](#)) is a member organization with the mission “to promote excellence in the safe, reliable, secure, and resilient operation of the electric transmission system.” Membership eligibility is “any organization that owns, operates, or controls at least 45 circuit miles of integrated (network) transmission facilities at 100 kV or above, operates a “24/7” transmission control center with NERC certified transmission or reliability operators, or has an open access transmission tariff or equivalent on file with a regulatory authority, may join the NATF.”






NATF hosts a free Supply Chain Cyber Security Industry Coordination [portal](#), which includes resources on their Supply Chain Security Assessment Model, CIP-13 vendor assessment, and risk management plans.

Inductive Automation can fill out the NATF “Supply Chain Security Criteria” spreadsheet to assist customers with the CIP-13 vetting process.

## Critical Infrastructure Protection (CIP) Standards

Standard	Note
<a href="#">CIP-001-1</a> Sabotage Reporting (06/04/07)	Retired
<a href="#">CIP-002-6</a> Cyber Security — BES Cyber System Categorization (5/14/20)	Identify and categorize Bulk Electric System (BES) cyber assets to apply security controls commensurate with potential adverse impact on the reliable operation of the BES.
<a href="#">CIP-003-9</a> Cyber Security — Security Management Controls (11/16/22)	Establish responsibility and accountability to protect BES.  <b>Note:</b> As of <b>Mar 22, 2023</b> , per R1 1.2, “low impact BES Cyber Systems” now require 1.2.1-1.2.7: cyber security (CS) awareness, physical security, electronic access, CS incident response, transient access and removable media, vendor electronic access, and declaring/responding to CIP exceptional circumstances.
<a href="#">CIP-004-7</a> Cyber Security — Personnel & Training (12/10/21)	Risk Assessment, training, and security awareness.
<a href="#">CIP-005-7</a> Cyber Security — Electronic Security Perimeter(s) (10/01/22)	<b>Response table below.</b> Manage cyber security perimeter around BES.
<a href="#">CIP-006-6</a> Cyber Security — Physical Security of BES Cyber Systems (01/21/16)	
<a href="#">CIP-007-6</a> Cyber Security — System Security Management (01/21/16)	
<a href="#">CIP-008-6</a> - Cyber Security — Incident Reporting and Response Planning (02/06/19)	
<a href="#">CIP-009-6</a> Cyber Security — Recovery Plans for BES Cyber Systems (01/21/16)	
<a href="#">CIP-010-4</a> Cyber Security — Configuration Change Management and Vulnerability Assessments (10/01/22)	<b>Response table below.</b>  *Effective 10/01/22 includes EACMS vendor requirements
<a href="#">CIP-011-3</a> Cyber Security — Information Protection (12/10/21)	Discussed in <a href="#">vendor best practices</a> under Cyber Security Information Protection and Secure Disposal.
<a href="#">CIP-012-1</a> Cyber Security – Communications between Control Centers (02/17/20)	
<a href="#">CIP-013-2</a> . Cyber Security - Supply Chain Risk Management (10/01/22)	<b>Response table below. Tip:</b> Use the NATF Supply Chain Cyber Security Industry Coordination <a href="#">portal</a> . Inductive Automation can fill out the “Supply Chain Security Criteria” spreadsheet to assist customers with the CIP-13 vetting process.
<a href="#">CIP-014-3</a> . Physical Security (06/16/22)	12/15/22 FERC <a href="#">Order</a> directing NERC to study efficacy of physical security standards after 12/03/22 North Carolina attacks and 11/22 Pacific Northwest attacks.

## Convention

Font	Meaning
<i>Italics</i>	NERC CIP source or key terminology
Plain Text	Guide information or recommendation
<b>Bold</b>	Emphasized concept or category label
	<b>Additional Information.</b> Supplemental information may go beyond minimal CIP requirements with best practices.
	<b>Tip</b> or Industry Best Practice.
	<b>Ignition capability.</b> Configuration details or example implementation options.
	<b>Customer responsibility.</b> It may be possible to designate the activity to System Integrator, consultant, or Software as a Service (SaaS) provider. The customer should still be involved through oversight and auditing.
	<b>Customer choice.</b> Optional system or service to help satisfy requirements.

## Key Concepts

### Shared Responsibility Model

This guide proposes that the customer, their vendors, and optionally their service providers each have responsibilities to achieve success with 21 CFR Part 11-compliant projects.

#### Customer



**Customer responsibility:** The customer is ultimately responsible for compliance. The customer will have flexibility in deciding between *Operational and Administrative Controls* (executed by people as opposed to systems) and *Technical Controls* (implemented through hardware or software). Customers often rely on System Integrators to help achieve compliance.

Responsible Entities should:

- Maintain policies and procedures that hold users accountable, developed in accordance with a risk-based approach



- Address how vendors are assessed
- Provide training
- Perform validation
- Enforce change control
- Audit vendors and service providers to ensure that requirements are being met and compliance is maintained.

## Software Vendor

CIP applications characteristically integrate multiple hardware and software products within their *Electronic Security Perimeter* (ESP). Vendors should demonstrate how they, as part of the critical supply chain, adhere to best practices with quality and security. Vendors should provide configuration recommendations for using their software in a regulated environment including configuration recommendations and integration with external systems and technologies.

Inductive Automation provides information at the Security and Trust Portal at:

<https://security.inductiveautomation.com>.



**Ignition capability:** Indicates that a requirement can be met using Ignition, generally requiring configuration but not third party systems.

## Vendor support Matrix

Vendor support. <b><i>Bold-italic Term</i></b>	Meaning
<b><i>Provides</i></b>	Vendor makes information available that can be given to an auditor or vendor that feeds into an artifact or accessible system.
<b><i>Validates</i></b>	Can be used to prove presence or effectiveness of control.  Often performed by a combination of asset owners, system integrators, and service providers.
<b><i>Supports</i></b>	Feeds information into a system or process supporting requirements.  Often system-to-system communication.
<b><i>Not Applicable</i></b>	Does not apply. Justification and recommendations provided as applicable.

**Note:** Inductive Automation (IA) provides software that is installed, configured, and maintained within the Responsible Entities Electronic Security Perimeter. IA does not provide software, platform, or infrastructure as a service (XaaS) and does not have access to customers' data,

systems, networks, sites, or assets. For that reason, most CIP requirements that IA supports fall under **Provides**.

### Consultants or System Integrators



**Customer choice:** Consultants or System Integrators (SIs) may offer Part 11-compliant implementation services using Ignition and other hardware or software products. Some may provide services such as qualification testing, user training, and procedure templates to help customers navigate the compliance process.

Inductive Automation maintains a listing of over 3,000 Integrators worldwide and provides certification standards. Please contact your sales representative for specific SI references.

<https://www.inductiveautomation.com/integrators/>

### Cloud Service Providers



**Customer choice:** Cloud Service Providers (CSP) include best practices for running NERC CIP-compliant or similar applications within their infrastructure. These tend to provide a high level of validated assurance “lower in the stack” and leave the application portion (where Ignition resides as a SCADA system) to the customer. For example: [AWS best practices](#), [Azure and NERC CIP standards](#), many of which are informed by NIST and FedRAMP standards.



**Tip:** CSPs offer virtual networks, which are isolated customer environments that can be interconnected with customer infrastructure through secure connections including “cloud peering” without the public Internet. Ignition supports “n-tiered” architectures and most secure remote access technologies.

### Software/Platform as a Service (SaaS/PaaS)



**Customer choice:** Software- and Platform-as-a-Service (SaaS/PaaS) models provide customer options where vendors can assume responsibility based on managing infrastructure that processes customer data. Service providers are able to perform compliance activities, such as computer system validation, change control, process automation, and user training. SaaS/PaaS offerings enable a high degree of inherited assurance through architecture and service automation (orchestration of “the technology stack”), greatly exceeding what is feasible with most on-premise environments. SIs may be able to assist with customization needed from SaaS/PaaS offerings. The RE should plan on regularly auditing SaaS and PaaS providers.

**Tip:** It is a natural fit for SaaS/PaaS service providers to offer customers dedicated VPCs running on the well known CSPs (e.g., AWS, Microsoft Azure, Google Cloud Platform) configured in accordance with best practices. Secure interconnects and web services technologies provide safe options to access shared services.

## CIP Vendor Best Practices with Inductive Automation



**Tip:** Following Ignition best practices simplifies the validation process by demonstrating high levels of assurance. CIP compliance does not depend on any specific technology or configuration. This guide recommends a risk-based decision-making approach based on customer requirements and industry standards, backed by subject matter expertise.

Inductive Automation provides an [Ignition Security Hardening Guide](#) and a [Server Sizing and Architecture Guide](#) to assist with best practices.

1. **Secure Remote Access.** Include vendor access requirements and work with IT/OT. See the most recent CIP-003. For example, CIP-003-9, as of Mar 22, 2023, requires Vendor Electronic Remote Access Security Controls for low impact BES cyber systems. Section 6 specifies requirements including having one or more methods to determine vendor electronic remote access, disable vendor electronic remote access, and detect known or suspected malicious communications for vendor remote access.



**Recommendation:** consider modern proven technologies such as bastion hosts, firewalls, VPN technologies, Identity and Access Management (IAM) solutions, and Zero Trust methodologies.

Note: Inductive Automation does not require vendor remote access. Remote support is usually a customer-initiated synchronous screen-sharing session, with the option for phone support only. It is usually an option to utilize secure remote access systems provided by the RE, which is recommended for CIP applications. In all cases, out-of-band transfer of system logs is often necessary for troubleshooting, and access to RE production data is rarely needed.

Note: The new trend refers to “authenticated vendor-initiated remote connections” instead of “Interactive Remote Access” and “system-to-system”. (FERC Order 850). This helps avoid the “hall of mirrors” effect where accessing an EACMS system must be done through an intermediate system, which itself is an EACMS system (*CIP-005-7 2.4 and 2.5*). **Additional recommendations:**

- i. Maintain artifacts together as a matter of practice. For example, the event associated with a single Ignition support case could include: Responsible Entity

- operator logs, remote access logs, Ignition support ticket documentation, and resulting change control artifacts. Include who the support representative was, what was done, and when.
- ii. Scrutinize and document justification for “vendor-initiated Interactive Remote Access”. CIP-013-2 1.26 requires a documented security risk management plan for medium and high impact BES systems.
    - i. Inductive Automation generally does not require this. System Integrators might in order to perform contracted maintenance.
  - iii. “System-to-system remote access”. CIP-013-2 1.26 requires a documented security risk management plan for medium and high impact BES systems.
    - i. Favor outbound initiated technologies (e.g., REST API calls) and consider “read only” connections (e.g., secured MQTT)
    - ii. Consider the use of compensating security control such as proxies and firewalls.
2. **Vendor Identity and Software Integrity Verification.** Enshrine due diligence throughout your processes.
- i. **Vendor validation instructions.** Vendors should provide instructions on validating the authenticity of their software. Formalize the performance and documentation of available integrity checks in your processes and procedures.
    - i. Inductive Automation offers guidance on performing a file integrity check via hash calculation on each downloaded file, and code signing checks via the operating system to compare against expected certificates.  
<https://www.docs.inductiveautomation.com/docs/8.1/getting-started/installing-and-upgrading#verify-that-ignition-software-is-genuine>
3. **Vendor Risk Management and procurement controls.** Consider the classes of possible incidents based on a per-vendor basis using a risk assessment methodology. Impact will depend on the nature of the product or service provided, how it is integrated in the RE environment, compensating controls, and local processes and policies.
- i. **Vendor Assessment.** Document vendor identity and software integrity practices obtained through the initial due diligence period. Update results regularly.
    - i. Consider: reputation and business practices, how vendors protect their IT and software development environment, how vendor products and services can be configured and protected in the context of the RE architecture, and the security and quality assurance process of the vendor software development lifecycle.
      1. Inductive Automation shares practices on a Security and Trust Portal. <https://security.inductiveautomation.com>
  - ii. **On-premise software vulnerabilities.** Track the most expedient and reliable notification methods on a per-vendor basis. Include a risk-informed methodology

in your incident response plan that considers safety and reliability when deciding on actions.

- i. Inductive Automation posts software advisories and recommendations on a Security and Trust Portal as part of a Coordinated Vulnerability Disclosure (CVD) Program. Email subscription is possible.  
<https://security.inductiveautomation.com>
- iii. **Cyber Security Information Protection.** CIP-011-3 outlines Cyber Security — Information Protection requirements. This largely falls to asset owner IT and OT policy, procedure, and process.
  - i. BES Cyber System Information (BCSI). CIP-011-3 Part 1.1.
    - 1. Include BCSI: handling procedures, data classification, labeling, and marking in your information security program
    - 2. CIP-011-3 Table R1 measures (examples):
      - a. Document method(s) to identify BCSI
      - b. Mark (human readable) and label (machine coding) BCSI
      - c. Include BCSI in user training
      - d. Designate BCSI storage location(s)
  - ii. BES Cyber System Information (BCSI) confidentiality. CIP-011-3 Part 1.2.
    - 1. Protect and securely handle BCSI
      - a. Data at rest. Encrypt stored data according to organizational policy. This can be done at multiple layers including hard drive, storage array, data volume, database, database elements, or individual files. Multiple layers of encryption is not uncommon. Consider key management and performance.
        - i. Ignition applications do not inherently provide application layer encryption. Ignition systems rely on lower-level encryption mechanisms to achieve data-at-rest encryption.
      - b. Data in transit. Encrypt data in transit according to organizational policy. Layering encrypted data tunnels can be a good idea, but each layer adds network data header overhead. Excessive layers can lead to performance issues such as network fragmentation.
        - i. Apply strong network segmentation. Secure communication between network security zones with standard technologies such as VPNs or Zero Trust methodologies. This is especially important between trusted and untrustworthy zones.



- ii. Configure Ignition to use TLS for data encryption according to the [Ignition Security Hardening Guide](#).
      - 1. Some legacy Operational Technology communication protocols do not support modern security. This communication can only be segmented and protected externally.
  - 2. Keep records of handling according to organizational policy
    - a. Electronic records may be used (e.g., logs, key management)
    - b. Physical technical methods may be used (e.g., keys, badges, biometrics)
      - i. Ignition supports multi-factor authentication via federated identity providers (OpenID connect or SAML protocols). This approach can incorporate *something you have* with *something you know* as identification factors.
    - c. Administrative methods may be used (e.g., assessments, audits, agreements, etc)
- iv. **Secure Disposal.** CIP-011-3 table R2 outlines BES cyber asset reuse and disposal.
  - i. Responsible entities shall take action to prevent unauthorized retrieval of BCSI prior to release or reuse (part 2.1) and asset disposal (part 2.2).
    - 1. See [Secure Disposal Guide](#) for Ignition recommendations. NIST Special Publication 800-88 provides guidelines on media sanitization.
    - 2. Keep records on data protection (e.g., encryption) and sanitization actions (e.g., storage media destruction).
    - 3. Keep records of actions taken to prevent unauthorized retrieval of BCSI prior to disposal, release, or reuse (e.g., handling, training).
- v. **Hardware vulnerabilities.** Outside the scope of this document. Adhere to organizational policies and best practices. Maintain accurate inventories and keep firmware up to date.
- vi. **Software as a Service (SaaS) vulnerabilities.** SaaS presents unique challenges based on the inherent shared responsibility model. Discuss these with vendors in advance.
  - i. **Persistent connection.** Consider “pre-planned responses” (PPRs) in advance if a persistent network connection is required. What are the operational impacts for each option? Is it possible to disconnect or limit access?
  - ii. **Stewardship.** Does a vendor host and protect your data, assets, or services? Establish an understanding of what the vendor does to protect

your interests including actions taken during an incident. External standards and checks typically come into play to convey confidence: SOC 2 audits, ISO certifications, demonstrated Third-Party assessments, etc.

- iii. Inductive Automation does not provide SaaS services, nor has access to RE data, networks, or systems.

4. **Transient Cyber Assets and Removable Media malicious code risk mitigation.** Required for low impact BES cyber systems (CIP-003-9 1.2.5, as of Mar 22, 2023).

- i. Responsible Entity policy needs to address any actors connecting cyber assets or media to BES cyber systems. **This includes vendors bringing laptops or media.**
  - i. If viable, provide managed assets for vendors to work on. Supervise activity.
- ii. See the latest CIP-003 for recommendations. For example, CIP-003-9 5.1-5.3 covers application whitelisting, A/V review, and scanning removable media for malware.
  - i. **Recommendation.** Work with IT/OT for the best modern solutions that align with organizational policy. For example, modern “endpoint” solutions connected to central Security Event and Information Management (SEIM) products could cover all requirements, plus help with more (e.g., asset management, software updates, A/V, application whitelisting, etc.).

5. **Incident Response.**

- i. Customer responsibility. Cyber Security – Incident Reporting and Response Planning Implementation Guidance for [CIP-008-6](#).
  - i. The Cybersecurity & Infrastructure Security Agency (CISA) under the Department of Homeland Security provides [Incident Response guidance](#).

6. **Other requirements.**

- i. CIP applications have requirements that exceed the scope of this guide. Per CIP-003-9 (R1.1.2), as of Mar 22, 2023, even “low impact BES Cyber Systems” will have documented cyber security policies that address: cyber security awareness, physical security controls, electronic access controls, and additional items discussed in this guide.
- ii. Other CIP requirements exceed the scope of this guide. For example, CIP-011-3 requires documented information protection programs for BES Cyber Security Information (BCSI) for Medium and High Impact BES Cyber Systems and associated EACMS/PACS. **These requirements should be viewed as complementary to best practices recommended by this guide.**

7. **Keep up to date with best practices and guidance.**

- i. FERC orders and weekly guidance.
  - i. FERC [eLibrary](#)
- ii. NERC or the E-ISAC
  - i. NERC [One-Stop Shop](#) (compliance e-Library)

- iii. ICS-CERT, CISA, and NIST.
  - i. NERC provides [mappings](#) to CISA Control System Goals (CSGs)
  - ii. NERC provides [mappings](#) to NIST Cybersecurity Framework v1.1 (CSF)
- iv. Canadian Cyber Incident Response Centre (CCIRC)
  - i. CCIRC [Tools and services](#)
- v. Vendor specific recommendations
  - i. [Inductive Automation Security and Trust Portal](#)

## Ignition Best Practices in a Secure Environment

1. Follow the [Ignition Security Hardening Guide](#) for security best practices with Ignition and the immediate computing environment. Include supporting IT and OT departments from the start. They likely have people, processes, and tools to help. From the Ignition Security Hardening Guide:
  - i. Consider a foundational model and strategy. “Zero Trust,” “Defense in Depth,” “Zones and Conduits,” and “Purdue Model” are examples. Align with organizational best practices.
  - ii. Force secure client communication with Ignition using HTTPS with genuine TLS certificates. Employ “strong headers” with HSTS redirects and consider disabling older cipher suites.
  - iii. Follow Identity and Access guidance. This includes using secure LDAP (LDAPS) for Active Directory connections and SAML or OpenID Connect for Identity Providers. Adhere to your organizational policy on account usage and lifecycle.
  - iv. Consider additional authentication factors. Role-Based Security is a great starting point. Ignition supports additional features such as location, security zones, and security levels. Identity providers are moving in the direction of pattern of use, device health checks, and other non-traditional factors.
  - v. Apply good cybersecurity hygiene. Remove unnecessary applications, lock down the host operating system, keep systems up to date, and stay consistent with organizational best practices. This might include the IT or OT department maintaining endpoint protection systems and central monitoring tools such as Security Information and Event Management (SIEM) tools.
2. Use an external Identity Source for user authentication (verifying identity) and authorization (managing access rights). This could be an on-premise Enterprise system such as Microsoft Active Directory or a third-party Identity Provider (IdP), which can be locally managed or provided by a cloud service. Local OS or application managed user accounts are generally weaker and not recommended for secure applications. The most secure and realistic options will require strong or multi-factor authentication for all users through an identity and access management service, which can be local, cloud-hosted, or a hybrid of the two.

- i. Assign Ignition roles based on IdP groups, such as Active Directory Groups.
  - ii. The most current Microsoft approach uses Azure AD (Entra). On-premise solutions are possible such as Apache Keycloak, Red Hat Identity Manager, or HashiCorp Vault. Third-party solutions such as Duo, Okta, and Ping offer powerful hybrids. Enterprise solutions are offered from Oracle, IBM, RSA, Symantec (Broadcom), and others.
3. Consider people (training), processes, and technology to holistically address requirements. Tools are useful, but will not lead to a strong CIP program alone.
4. Extra consideration of database protections is warranted for CIP applications.
  - i. Discuss the best options with IT, OT, and cybersecurity stakeholders.
  - ii. Configure dedicated Ignition database connections for the project, Audit Log, and Historian. Apply separate credentials for each. Apply best practices for security controls and auditing consistent with company policy, vendor recommendations, and project risk analysis. For example, grant SELECT and INSERT (not UPDATE or DELETE) on an audit schema.

Name	Description
Application	Custom database available for project use
AuditLog	Append-only database connection for audit log
Historian	Append-only database connection optimized for time-series data

- iii. Force disk cache usage for database interactions. Forcing disk cache usage preserves records in the event of a power outage where records have not yet been written to a database or store-and-forward cache. Additional mitigation is possible with environmental controls such as local UPS and fuel-based generator support.

Advanced: Only Forward From Cache

☒ If enabled, all records will be forced to go through the disk cache before being forwarded. Otherwise, the system will pull from either the disk cache, memory buffer, or both to try to satisfy the forward write size setting.  
(default: false)

5. **Architecture.** It may be appropriate to start with a single Ignition gateway. However, Ignition “scale-out” architectures offer improved security, performance, and survivability characteristics. Follow the [Server Sizing and Architecture Guide](#) when scaling out.



**Tip:** Secure architectures are possible using Ignition gateways to apply the *Principle of Least Privilege* with network segmentation. The concept is that most nodes (e.g., clients, databases, network and OT devices) can only communicate within a zone, preferably only to the nearest Ignition gateway. Ignition gateways relay traffic by securely inter-communicating between zones using secure

“Gateway Network” (GWN) or MQTT connections (“conduits”) with certificate-based, secure TLS connections over a single TCP port. External firewalls are recommended between zones.



**Tip:** “Stateless” *frontend* (aka “*visualization*”) gateways run projects and communicate securely with Ignition clients, often through a load balancer. “I/O” gateways maintain “state,” which includes the tag system, script and logic execution, device, and database connections. I/O gateways can be protected with Ignition Redundancy where a secondary gateway is ready to take over. “Edge” devices running Ignition offer proximity advantage. In the event of a network or server failure, local control is possible with Edge devices. A “store-and-forward” buffer retains historical data. Many legacy OT protocols used to communicate with industrial control systems are inherently weak. Ignition Edge allows segmentation in accordance with best practices such as ISA/IEC 62443 “Zones and Conduits” or ISA-95 “Purdue Model” segmentation. This is typically accomplished with network segmentation (dividing) and segregation (controlling communication) such as VLAN and VPN technologies.

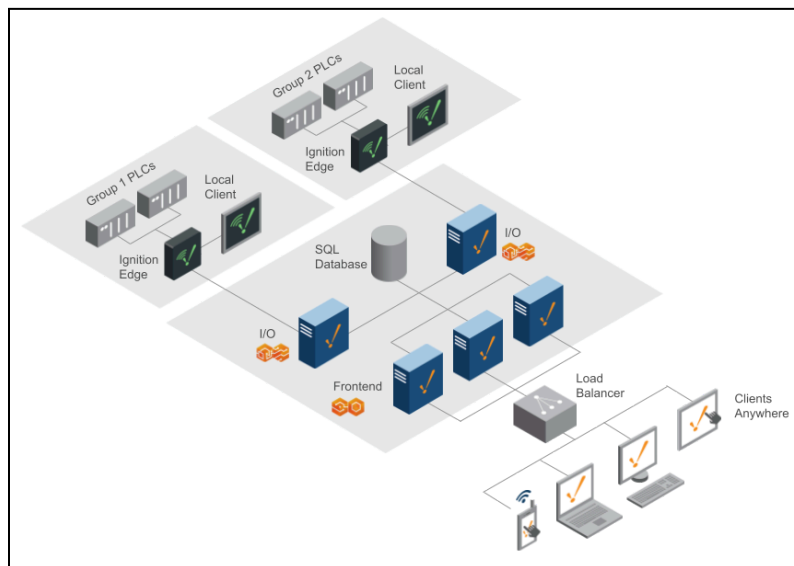



Figure 2 Reference: Scale-out architecture example



# NERC CIP Compliance with Inductive Automation and Ignition

## CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)

Ignition usually qualifies as an “Applicable System” as an Electronic Access Control or Monitoring Systems (**EACMS**). Parts 3.1 and 3.2 in *CIP-005-7 Table R3 - Vendor Remote Access Management for EACMS and PACS* is the applicable section. Other sections are considered as best practices.

Requirement (IA Summary)	Notes / IA Recommendations
<b>A - <a href="#">CIP-005-7</a> Introduction</b>	Title, Purpose, Applicability
<p><b>Purpose:</b> To manage electronic access to BES Cyber Systems by specifying a controlled <i>Electronic Security Perimeter (ESP)</i> in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.</p> <p><b>Applicability:</b> Defines <b>Responsible Entities (RE)</b>. Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, and Transmission Owner.</p> <p>Electronic Access Control or Monitoring Systems (<b>EACMS</b>) – Applies to each EACMS System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.</p>	
<b>B - Requirements and Measures</b>	
<p><b>R1.</b> Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter. <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]</i></p> <p><b>M1.</b> Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in <i>CIP-005-7 Table R1 – Electronic Security Perimeter</i> and additional evidence to demonstrate implementation as described in the <b>Measures</b> column of the table (see source document). IA recommendations will align.</p>	
	<p><i>CIP-005-7 Table R1 - Electronic Security Perimeter. <b>Not Applicable.</b> Ignition architecture is recommended to align with Protected Cyber Asset (PCA) requirements.</i></p>
<ul style="list-style-type: none"> <li>All network-connected assets reside within defined <i>Electronic Security Perimeter (ESP)</i></li> </ul>	

- All external routable connectivity must be through an identified Electronic Access Point (EAP)
- “Deny all” rules by default. Justify and document “accept” rules
- Perform authentication where technically feasible
- Detect malicious inbound and outbound communication



*CIP-005-7 Table R2 - Remote Access Management. **Not Applicable**.* The best practice is to align Ignition procedures with Protected Cyber Asset (PCA) requirements. Interactive Remote Access Recommendations:

- Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- Utilize encryption that terminates at an Intermediate System.
- Require multi-factor authentication for all Interactive Remote Access sessions.
- Have one or more methods for determining active vendor remote access sessions
- Have one or more method(s) to disable active vendor remote access



CIP customers can provide a secure remote access capability to IA tech support on a “just in time” basis, and/or initiate connections from the RE environment.

**R3.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-7 Table R3 –Vendor Remote Access Management for **EACMS** and **PACS**. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

**M3.** Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R3 – Vendor Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

**3.1** Have one or more method(s) to determine authenticated vendor-initiated remote connections.



Tip: A strong ESP and EAP architecture and associated IT/OT tools will simplify this requirement.

**3.2** Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.



CIP-005-7 examples: terminate shell/process/session, disable accounts/token, restrict access via firewall, disconnect physical cable.

### **C - Compliance**

**1.** Compliance Monitoring Process (*summarized*). See CIP-005-7 for full details.




**1.1 Compliance Enforcement Authority:** NERC, Regional Entity, or otherwise designated.









**1.2 Evidence Retention:** RE shall retain evidence for 3 years. If non-compliant, until mitigation is complete and approved. CEA shall keep the last audit records.

**1.3. Compliance Monitoring and Enforcement Program:** The identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.








## CIP-010-4 – Cyber Security — Configuration Change Management and Vulnerability Assessments




Ignition usually qualifies as an “Applicable System” as an Electronic Access Control or Monitoring Systems (**EACMS**). Most parts are applicable. Parts with “Applicable System” listed as “High Impact BES Cyber Systems”, such as **1.5** and **3.2** may not be strictly required for Ignition, but are recommended to be treated as best practices.

Requirement (IA Summary)	Notes
<b>A <a href="#">CIP-010-4</a> - Introduction</b>	
<p><b>Purpose:</b> 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).</p> <p><b>Applicability:</b> Defines <b>Responsible Entities (RE)</b>. Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, and Transmission Owner.</p> <p>Electronic Access Control or Monitoring Systems (<b>EACMS</b>) – Applies to each EACMS System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.</p>	
<b>B - Requirements and Measures</b>	
<p><b>R1.</b> 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 and their associated <b>Electronic Access Control or Monitoring Systems (EACMS)</b> and <b>Physical Access Control Systems (PACS)</b>. The plan(s) shall include: <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]</i></p>	
<p><b>1.1</b> One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:</p>	 RE responsibility to conduct or oversee risk assessments
<p>(i) procuring and installing vendor equipment and software;</p>	 RE process.  Conduct standard assessments on vendor hardware and software.








(ii) transitions from one vendor(s) to another vendor(s).	 RE responsibility  Include transition documentation as a part of RFPs and project changes.
<b>1.2</b> One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:	 RE process
<b>1.2.1</b> 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	 <b>Provides.</b> Inductive Automation posts software advisories and recommendations on a Security and Trust Portal as part of a Coordinated Vulnerability Disclosure (CVD) Program.  Email subscription is recommended. <a href="https://security.inductiveautomation.com">https://security.inductiveautomation.com</a>
<b>1.2.2</b> 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	 RE Incident Response process.  Align with <i>CIP-008-6 — Cyber Security — Incident Reporting and Response Planning</i> requirements.  Consider CISA Incident Response Recommendations. <a href="https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response">https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response</a>
<b>1.2.3.</b> Notification by vendors when remote or onsite access should no longer be granted to vendor representatives	 <b>Not Applicable.</b> Inductive Automation is a software provider that does not obtain onsite or remote access.  IA tech support offers optional customer-initiated “Interactive Remote Access.” <a href="https://www.inductiveautomation.com/support/policy/">https://www.inductiveautomation.com/support/policy/</a>  Coordinate notification with service providers or System Integrators who have access to Responsible Entity assets.















<p><b>1.2.4.</b> Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity</p>	<p> <b>Provides.</b> See the Security and Trust Portal. Email subscription is recommended. <a href="https://security.inductiveautomation.com">https://security.inductiveautomation.com</a></p> <p>Note: IA aggressively pursues Ignition vulnerabilities. This includes hiring Third-Party Application Penetration tests for each version and annually volunteering as a target for Ethical ICS hacking (Pwn2Own) competition.</p>
<p><b>1.2.5.</b> Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS</p>	<p> <b>Provides.</b> See instructions for verifying software integrity and authenticity. This includes file hash computation from the download and code signing certificate verification in the Operating System.</p> <p><a href="https://www.docs.inductiveautomation.com/docs/8.1/getting-started/installing-and-upgrading#verify-that-ignition-software-is-genuine">https://www.docs.inductiveautomation.com/docs/8.1/getting-started/installing-and-upgrading#verify-that-ignition-software-is-genuine</a></p>
<p><b>1.2.6.</b> Coordination of controls for vendor-initiated remote access.</p>	<p> <b>Not Applicable.</b> IA does not obtain vendor-initiated Interactive Remote Access.</p> <p> IA Tech Support can usually accommodate RE's choice of technology for customer-initiated "Interactive Remote Access." Phone support only is possible. Expect the need to transfer log files and other troubleshooting artifacts.</p>
<p><b>M1.</b> Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.</p>	<p> RE responsibility</p> <p> Consider tools or platforms that help document and track NERC CIP requirements.</p>
<p><b>R2.</b> Each Responsible Entity shall implement its supply chain cyber security risk management plan(s)</p>	<p> RE responsibility</p>

specified in Requirement <b>R1</b> . <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]</i>  [Note omitted for brevity]	
<b>M2.</b> Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.	 Track vendor security assessments completed during acquisition.
<b>R3.</b> 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. <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]</i>	 RE responsibility
<b>M3.</b> Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.	 RE responsibility
<b>C - Compliance</b>	
<p><b>1.</b> Compliance Monitoring Process (<i>summarized</i>). See CIP-013-1 for full details.</p> <p><b>1.1 Compliance Enforcement Authority:</b> NERC, Regional Entity, or otherwise designated.</p> <p><b>1.2 Evidence Retention:</b> RE shall retain evidence for 3 years. If non-compliant, until mitigation is complete and approved. CEA shall keep the last audit records.</p> <p><b>1.3. Compliance Monitoring and Enforcement Program:</b> the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.</p>	



## CIP-013-2 – Cyber Security - Supply Chain Risk Management

Requirement (IA Summary)	Notes
<b>A <a href="#">CIP-013-2</a> - Introduction</b>	
<p><b>Purpose:</b> 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.</p> <p><b>Applicability:</b> Defines <b>Responsible Entities (RE)</b>. Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, and Transmission Owner.</p> <p><b>Note:</b> CIP-013-2 superseded CIP-013-1. Scope changes are the addition of EACMS and PACS.</p>	
<b>B - Requirements and Measures</b>	
<p><b>R1.</b> 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 and their associated <b>Electronic Access Control or Monitoring Systems (EACMS)</b> and <b>Physical Access Control Systems (PACS)</b>. The plan(s) shall include: <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]</i></p>	
<p><b>1.1</b> One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from:</p>	 Responsible Entity (RE) responsibility to conduct or oversee risk assessments
<p>(i) procuring and installing vendor equipment and software;</p>	 RE process  Conduct standard assessments on vendor hardware and software.
<p>(ii) transitions from one vendor(s) to another vendor(s).</p>	 RE responsibility  Include transition documentation as a part of RFPs and project changes.
<p><b>1.2</b> One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:</p>	 RE process
<p><b>1.2.1</b> Notification by the vendor of vendor-identified incidents related to the</p>	 <b>Provides.</b> Inductive Automation posts software advisories and

products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity	recommendations on a Security and Trust Portal as part of a Coordinated Vulnerability Disclosure (CVD) Program. Email subscription is possible. <a href="https://security.inductiveautomation.com">https://security.inductiveautomation.com</a>
<b>1.2.2</b> 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	 RE Incident Response process.  Align with <i>CIP-008-6 — Cyber Security — Incident Reporting and Response Planning</i> requirements.  See CISA Incident Response Recommendations. <a href="https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response">https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response</a>
<b>1.2.3.</b> Notification by vendors when remote or onsite access should no longer be granted to vendor representatives	 <b>Provides.</b> IA is a software provider that does not obtain onsite or remote access.  IA tech support offers optional customer-initiated “Interactive Remote Access.” <a href="https://www.inductiveautomation.com/support/policy/">https://www.inductiveautomation.com/support/policy/</a>  Coordinate notification with service providers or System Integrators who have access to Responsible Entity assets.
<b>1.2.4.</b> Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity	 See CVD program and additional information on the Security and Trust Portal. <a href="https://security.inductiveautomation.com">https://security.inductiveautomation.com</a>  IA aggressively pursues Ignition vulnerabilities. This includes hiring Third-Party Application Penetration tests for each version and volunteering as a target for Ethical ICS hacking (Pwn2Own) competition.

<p><b>1.2.5.</b> Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS</p>	<p> <b>Provides.</b> IA publicly publishes instructions for verifying software integrity and authenticity. This includes file hash computation from the download and code signing certificate verification in the Operating System.</p> <p>It is the RE's responsibility to incorporate verification in their process.</p> <p><a href="https://www.docs.inductiveautomation.com/docs/8.1/getting-started/installing-and-upgrading#verify-that-ignition-software-is-genuine">https://www.docs.inductiveautomation.com/docs/8.1/getting-started/installing-and-upgrading#verify-that-ignition-software-is-genuine</a></p>
<p><b>1.2.6.</b> Coordination of controls for vendor-initiated remote access.</p>	<p> <b>Not Applicable.</b> Inductive Automation does not provide vendor-initiated Interactive Remote Access.</p> <p> IA Tech Support can usually accommodate RE's choice of technology for customer-initiated "Interactive Remote Access." Phone support only is possible. Expect the need to transfer log files and other troubleshooting artifacts.</p>
<p><b>M1.</b> Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.</p>	<p> RE responsibility</p> <p> Consider tools or platforms that help document and track NERC CIP requirements.</p>
<p><b>R2.</b> Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement <b>R1</b>. <i>[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]</i></p> <p>[Note omitted for brevity]</p>	<p> RE responsibility</p>
<p><b>M2.</b> Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy</p>	<p> Track vendor security assessments completed during acquisition.</p>



documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.	
<b>R3.</b> 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. <i>[Violation Risk Factor: Medium]</i> <i>[Time Horizon: Operations Planning]</i>	 RE responsibility
<b>M3.</b> Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.	 RE responsibility
<b>C - Compliance</b>	
<p><b>1.</b> Compliance Monitoring Process (<i>summarized</i>). See CIP-013-1 for full details.</p> <p><b>1.1 Compliance Enforcement Authority:</b> NERC, Regional Entity, or otherwise designated.</p> <p><b>1.2 Evidence Retention:</b> RE shall retain evidence for 3 years. If non-compliant, until mitigation is complete and approved. CEA shall keep the last audit records.</p> <p><b>1.3. Compliance Monitoring and Enforcement Program:</b> the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.</p>	

## Rationale

Per CIP-013-1, “The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain.

The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

1. Software integrity and authenticity;
2. Vendor remote access;
3. Information system planning; and
4. Vendor risk management and procurement controls.”

## Appendix A - Glossary of Terms

**BES** ([Project 2010-17](#)). Bulk Electric System. All Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy (long modification list).

**BCSI** ([Project 2008-06](#)). BES Cyber System Information. Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

**CIP**. Critical Infrastructure Protection. A set of standards (maintained by NERC) aimed at regulating, enforcing, monitoring, and managing the security of the Bulk Electric System (BES) in North America.

**EACMS** ([Project 2008-06](#), [Order 706](#)). Electronic Access Control or Monitoring Systems. Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

**Electronic Security Perimeter** ([Project 2008-06](#), [Order 706](#)). The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

**FERC** ([About](#)). The Federal Energy Regulatory Commission, or FERC, is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects.

**Intermediate Systems** ([Project 2008-06](#)). A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

**IRE** ([Project 2008-06](#)). Interactive Remote Access. User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications

**NERC** ([About](#)). The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves nearly 400 million people.

**PACS** ([Project 2008-06 Cyber Security Order 706](#)). Physical Access Control Systems. Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

**PCA** ([CIP-005-7](#)). Protected Cyber Assets. Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Note: Ignition is generally categorized as an EACMS, but this is implementation specific.

Glossary of terms:

[https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)

Proposed term changes:

[https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016\\_CIP\\_Definitions\\_Informal\\_Posting\\_08092019.pdf](https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016_CIP_Definitions_Informal_Posting_08092019.pdf)

## Appendix B - References

### Source References

NERC “One Stop Shop” [spreadsheet of links](#) to source material.

[Energy Policy Act of 2005 Fact Sheet](#), FERC

[ERO rules](#) (18 CFR Part 39). Qualifies NERC to qualify to be the Electric Reliability Organization (ERO) which the Commission will certify as the organization that will propose and enforce Reliability Standards for the Bulk-Power System in the United States.

### Derivative reference material

[AWS Operational Best Practices for NERC CIP BCSI](#)

[Azure and NERC CIP Standards](#)

[NERC CIP with Rockwell Software](#). Includes Allen-Bradley hardware such as ControlLogix PLCs.

[Meeting NERC Change Control Requirements for HMI/SCADA and Control Systems](#) (GE)

[Verve Industrial Blog - What are the NERC CIP Standards in ICS Security](#)

[Proven Compliance Blog post](#)