Whitepaper

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and ISA/IEC 62443 Comparative Analysis

www.isagca.org

Table of Contents

Acknowledgments

The Utilities Technology Council, Cumulys and the International Society of Automation Global Cybersecurity Alliance (ISAGCA) prepared this report. This document is an interpretation of the ISA/IEC 62443 series of standards to facilitate awareness and appropriate applications of the standards. It is not a product of the ISA99 committee that develops the standards, and as such may not represent the views of the committee.

C. Briggs (Utilities Technology Council)

C. Muehrcke (Global Software Engineering representing ISAGCA)

A. Ristaino (ISA Global Cybersecurity Alliance)

T. Whitney (Cumulys Solutions Inc)

Executive Summary

The purpose of this paper is to demonstrate that, with few exceptions, the technical cybersecurity capabilities needed to comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards are substantially supported by the existing international ISA/IEC 62443 product cybersecurity standards. Therefore, entities responsible for NERC CIP compliance could benefit from leveraging existing ISA/IEC 62443 product certification programs in their procurement processes. Requirement-level mappings from NERC CIP-002-CIP-014 to the ISA/IEC 62443 standards align with supplier process requirements, as well as product security capabilities necessary to meet asset owner requirements under NERC CIP.

Background

The NERC CIP Standards have been in place since 2008. Since then, asset owners and operators have been solely responsible for complying with approximately one hundred fifty requirement parts encompassing thirteen standards:

Currently Enforceable NERC CIP Standards:

1. **CIP-002:** Bulk Electric System (BES) Cyber System Categorization
2. **CIP-003:** Security Management Controls
3. **CIP-004:** Personnel and Training
4. **CIP-005:** Electronic Security Perimeter(s)
5. **CIP-006:** Physical Security of BES Cyber Systems
6. **CIP-007:** System Security Management
7. **CIP-008:** Incident Reporting and Response Planning
8. **CIP-009:** Recovery Plans for BES Cyber Systems
9. **CIP-010:** Configuration Change Management and Vulnerability Assessments
10. **CIP-011:** Information Protection
11. **CIP-012:** Communications between Control Centers
12. **CIP-013:** Supply Chain Risk Management
13. **CIP-014:** Physical Security

Of these standards and requirements that address procedures and processes entities use to manage the day-to-day security of operations, many requirements entail specific efforts to configure technologies and systems to mitigate their cybersecurity risk to the grid. In those cases, owners and operators are dependent on the system's capability to be configured to address a wide array of CIP technical controls. Of the total enforceable CIP Standards, it has been determined that 62 of the CIP requirements support system-level configuration as a means to demonstrate compliance.

Since the early years of the CIP standards, a series of industry standards was developed by the International Society of Automation (ISA) through the ISA99[1] committee to address cybersecurity for operational technologies (OT). In 2009, the first of a series of OT security controls was released: ISA-99.00.01-2007, titled "Security for Industrial Automation and Control Systems: Concepts, Terminology, and Models."[2] Shortly thereafter, ISA and the International Electrotechnical Commission (IEC) agreed to collaborate on the development of these standards, which today are recognized as the ISA/IEC 62443 standards.[3] Several of these standards explicitly address the product development lifecycle and technical security capabilities of products. Third-party certifications against these standards have been available since the standards were published. This paper focuses on the cybersecurity development practices and technical capabilities described in the following ISA/IEC 62443 standards in relation to the security of supplier products:

- ISA/IEC 62443-4-1 – Product security development lifecycle requirements
- ISA/IEC 62443-3-3 – System security requirements and security levels
- ISA/IEC 62443-4-2 – Technical security requirements for IACS components

While the ISA/IEC 62443 standards have been in existence nearly as long as the CIP standards have been enforceable, minimal work has been done to recognize how the CIP-applicable assets and system-related requirements can be verified by an asset owner/operator as part of its procurement process for a supplier's OT product.

CIP-013 Supply Chain Risk Management

The supply chain risk management standards, approved by the Federal Energy Regulatory Commission in 2018, were developed to help mitigate the risk of third-party suppliers and their impact on the bulk electric system. With regard to ISA/IEC 62443, the standard that addresses "product security development lifecycle requirements" (ISA/IEC 62443-4-1) was developed to provide purchasing organizations with assurances that key supplier controls to integrate security into products were addressed. Given the similarities in purpose between the CIP-013 and ISA/IEC 62443-4-1, a detailed analysis was performed to compare the two sets of requirements. The results showed that the supply chain risk management technical requirements in CIP-013-2, CIP-005-7 and CIP-010-4 are substantially addressed by ISA/IEC 62443 requirements (see Table 1 below). Furthermore, a certification of supplier conformity to the lifecycle requirements standard (4-1) provides the utility asset owner with assurances about the supplier's practices and organizational controls for developing and supporting secure software

[1] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99
[2] https://www.isa.org/products/isa-tr99-00-01-2007-security-technologies-for
[3] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

and technologies. In fact, an ISA/IEC 62443-4-1 security capabilities vendor certification can be a proxy for the procurement aspect of the supply chain risk assessment requirement included in CIP-013-2 R1 (see Table 1):

> *"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: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s)"*

Technical Product Security Capabilities

In addition to analyzing the similarities in supplier security practices in CIP-013-2 and ISA/IEC 62443-4-1, this white paper analyzed how the ISA/IEC 62443 standards can support compliance with the CIP technical requirements. This includes a pre-purchase evaluation of grid technologies and products as well as their ability to be configured to meet the control objectives of the full body of NERC CIP technical requirements.

With respect to product security capabilities, the ISA/IEC 62443 standard has two parts. The first is 3-3, which describes the security capabilities of integrated systems such as an energy management system, which might be comprised of numerous related subsystems such as a master station, engineer's desktop and an operator workstation. An evaluation for ISA/IEC 62443-3-3 system certification assesses the security configurations of the integrated system as a whole to determine its adherence to the security capabilities required by the standard for security levels one through four. The second product standard is 4-2, which focuses on the security of individual components. For instance, a utility may purchase a remote terminal unit (RTU) or a protection relay to communicate to a system at a substation. The RTU/relay can be considered a component of the asset owner's SCADA system, and the RTU/relay device itself can be evaluated for certification to ISA/IEC 62443-4-2 independently of other systems or system components. This recognition of systems versus components is very similar to the concept of BES Cyber Asset and BES Cyber Systems in the NERC CIP Standards.[4] Component categories which may be evaluated for certification against ISA/IEC 62443-4-2 component requirements are listed below:

Software Applications - one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

[4] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

Embedded Devices -special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

Host Devices - general purpose device running an operating system (for example, Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

Network Device - device that facilitates data flow between devices or restricts the flow of data, but may not directly interact with a control process

The study reported in this paper exhaustively analyzed whether the relationship between ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 requirements could be a proxy for meeting the technical requirements of the CIP Standards. The resulting analysis has determined that suppliers and their products that conform to 3-3 or 4-2 directly support nearly all the technical system capabilities required to achieve NERC CIP compliance. The charts in the **Summary Figures** section have been provided to illustrate the analysis performed and key takeaways. These are summarized as follows:

- 100% of the CIP-013-2 controls can be verified by a conformity assessment that covers product security development lifecycle requirements in ISA/IEC 62443-4-1.[5] (See Table 1)
- There are many important security best practices that exceed the CIP Standards verified in technical security requirements for IACS components under ISA/IEC 62443-4-2 certifications (See Table 2 for notable capabilities among these; Table 3 is the complete list.)
- Only three of 62 technical security requirements of the CIP Standards are not addressed by conformity assessments that cover system security requirements and security levels in 62443-3-3 or technical security requirements for IACS components in ISA/IEC 62443-4-2 (See Table 4.)
- 95% of the technical security controls in the CIP standards can be verified by conformity assessments that cover system security requirements and security levels (62443-3-3) or technical security requirements for IACS components (62443-4-2) certifications (See Table 5.)

[5] Under 62443, any vendor accessing a system has the role of service provider (for integration or maintenance), which is distinguished from the role of product supplier. Therefore, the aspects of CIP-013-2 R1.2.3 and R1.2.6 regarding communication about controls for vendor access, are addressed by 62443-2-4 Security program requirements for IACS service providers rather than by 62443-4-1. It is expected that independent validation to requirements of 62443-2-4 for a utility's service providers, would also provide significant support for NERC CIP compliance, although an analysis of this topic is beyond the scope of the present study.

Conclusion

In conclusion, the supply chain risk management process is ideally suited to ensure that key cybersecurity capabilities are addressed by vendor or OEM supplied products. By recognizing the relationship between the NERC CIP standards and the ISA/IEC 62443 standards, industry can leverage the certifications offered for the ISA/IEC 62443 family of standards to help ensure compliance to NERC CIP standards. Additionally, the ISA/IEC 62443 series includes a variety of internationally recognized requirements that are evaluated and verified. Through certifications obtained during the project planning or procurement process, CIP-applicable assets can largely be validated to meet the asset owner/operator's regulatory mandates prior to the implementation of the technology. ISA/IEC 62443 can be a catalyst for reducing the security burden of asset owners while enabling a clear path for suppliers to demonstrate effective, globally recognized and independently verified cybersecurity best practices.

Further Reading

To learn more about the ISA Global Cybersecurity Alliance (ISAGCA) and its work on adoption and advocacy for the ISA/IEC 62443 series of standards, visit www.isagca.org.

To learn more about conformance certifications to the ISA/IEC 62443 series of standards through ISASecure, visit www.isasecure.org.

For more information about the ISA/IEC 62443 series of standards, visit www.isa.org/62443standards.

Summary Figures

95%

ISA/IEC 62443-4-2 product security requirements support 59 of 62 or 95% of the technical system capabilities required to achieve NERC CIP compliance

100%

100% of the CIP-013-2 controls are supported and independently validated by 21 related ISA/IEC 62443-4-1 product security lifecycle requirements

Figure 1

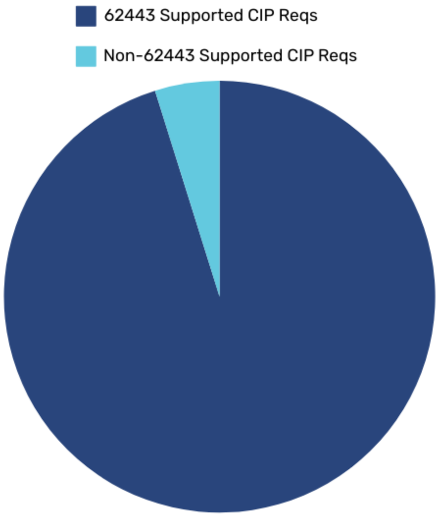


Figure 2

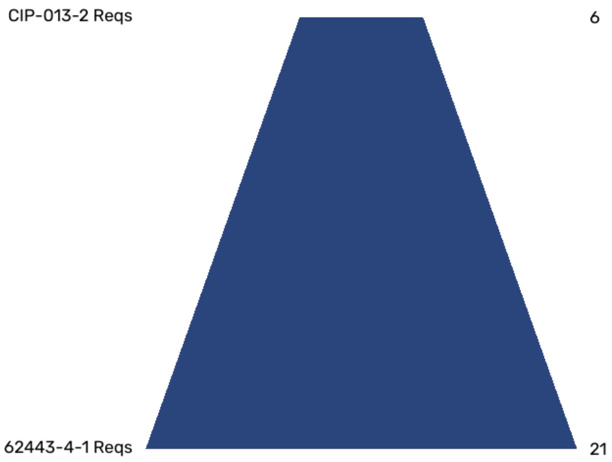
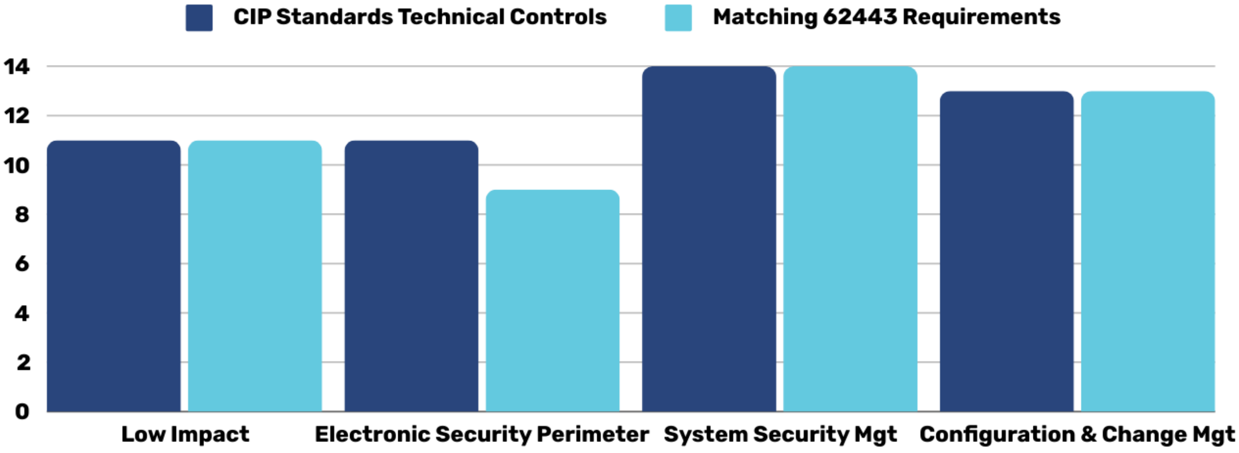


Figure 3



Detailed Analysis

Table 1 – CIP-013-2 Analysis

CIP-013-2 controls independently validated by ISA/IEC 62443-4-1 Certifications of Suppliers

Part 1.2	CIP-013-2	ISA/IEC 62443 4-1 Related Requirement
1.2.1.	Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity	DM-1 - Receiving Notifications of Security-Related Issues DM-5 - Disclosing Security-Related Issues
1.2.2.	Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity	SI-1 - Security Implementation Review DM-1 - Receiving Notifications of Security-Related Issues DM-2 - Reviewing Security-Related Issues DM-4 Addressing Security-Related Issues DM-5 - Disclosing Security-Related Issues SUM-1 – Security Update Qualification SUM-2 - Security Update Documentation SUM-3 - Dependent Component or OS Security Update Documentation SUM-5 - Timely Delivery of Security Patches
1.2.3	Notification by vendors when remote or onsite access should no longer be granted to vendor representatives	SG-2 - Defense in Depth Measures Expected in the Environment SG-6 - Account Management Guidelines
1.2.4	Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity	SVV-2 - Threat Mitigation Testing SVV-3 - Vulnerability Testing SVV-4 - Penetration Testing DM-1 - Receiving Notifications of Security-Related Issues DM-5 - Disclosing Security-Related Issues
1.2.5	Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES	SM-6 - File Integrity SM-7 - Development Environment Security SUM-4 - Security Update Delivery
1.2.6	Coordination of controls for vendor-initiated remote access	SR-1 - Product Security Context SD-1 - Secure Design Principles SG-1 - Product Defense in Depth SG-2 - Defense in Depth Measures Expected in the Environment

Table 2 – Highlighting Key ISA/IEC 62443 Requirements

Highlighting Key ISA/IEC 62443-4-2 Component Requirements that Exceed the NERC CIP Requirements

Req #	ISA/IEC 62443-4-2 Req Name	Req Description
CR 1.2	Software process and device identification and authentication	Component shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA/IEC 62443-3-3 [11] SR1.2. If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to ISA/IEC 62443-3-3 [11] SR1.1 may be part of the component identification and authentication process towards the other components.
EDR 3.12 **HDR 3.12** **NDR 3.12**	Provisioning product supplier roots of trust - protection	Embedded device, host or network system shall provide the capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.
NDR 5.2 RE(2)	Island mode	The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode)
CR 7.1	Denial of Service (DoS) Protection	Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.
CR 7.2	Resource management	Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

Table 3 – Exceeding the NERC CIP Standards

Highlighting ISA/IEC 62443-4-2 Component Requirements that Exceed the NERC CIP Requirements

Req #	ISA/IEC 62443-4-2 Req Name
CR 1.2 RE(1)	Unique identification and authentication
CR 1.8	Public key infrastructure (PKI) certificates
CR 1.9A-F	Strength of public key-based authentication - check validity of signature of a given certificate
CR 1.9 RE(1)	Hardware security for public key-based authentication
CR 1.10	Authenticator feedback
CR 1.11B	Unsuccessful login attempts - response
CR 1.14A	Strength of symmetric key-based authentication - establish trust
CR 1.14B-D	Strength of symmetric key-based authentication - secure storage for shared secret
CR 1.14 RE(1)	Hardware security for symmetric key-based authentication
CR 2.1 RE(3)	Supervisor override
CR 2.1 RE(4)	Dual approval
CR 2.5B	Session lock - removal
CR 2.7	Concurrent session control
CR 2.10A	Response to audit processing failures - maintain essential functions
CR 2.10B	Response to audit processing failures - actions taken
CR 2.11 RE(1)	Time synchronization
CR 2.11 RE(2)	Protection of time source integrity
CR 2.12	Non-repudiation
CR 2.12 RE(1)	Non-repudiation for all users
CR 3.5	Input validation
CR 3.6	Deterministic output
CR 3.7	Error handling
CR 3.9 RE(1)	Audit records on write-once media
EDR 3.12 **HDR 3.12** **NDR 3.12**	Provisioning product supplier roots of trust - protection
HDR 3.13A	Provisioning asset owner roots of trust - protection
HDR 3.13B	Provisioning asset owner roots of trust - inside zone
HDR 3.14	Integrity of the boot process
HDR 3.14 RE(1)	Authenticity of the boot process
NDR 5.2 RE(2)	Island mode
NDR 5.2 RE(3)	Fail close
NDR 5.3	General purpose, person-to-person communication restrictions
NDR 5.4	Application partitioning
CR 7.1	Network and security configuration settings
CR 7.1 RE(1)	Manage communication load from component
CR 7.2	Resource management
CR 7.6 RE(1)	Machine-readable reporting of current security settings

Table 4 – CIP Requirements Not Met by ISA/IEC 62443

Technical Requirements Within NERC CIP Standards Not Supported by ISA/IEC 62443

Standard	Requirement or Part	Applicability
CIP-005-7	Part 2.1 For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA
CIP-005-7	Part 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA
CIP-012-2	Part 1.2 Identification of method(s) used to mitigate the risk(s) posed by the loss of the ability to communicate Real-time Assessment and Real-time monitoring data between Control Centers; • Identification of alternative communication paths or methods between Control Centers • Procedures explaining the use of alternative systems or methods for providing for the availability of the data • Service level agreements with carriers containing high availability provisions • Availability or uptime reports for equipment supporting the transmission of Real-time Assessment and Real-time monitoring data	Control Centers

Table 5 – Technical Requirements Comparison

Technical Requirements within NERC CIP Standards Supported by ISA/IEC 62443-3-3 (System) and ISA/IEC 62443-4-2 (Component) Standards

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-003-9	Attachment 1, Section 3: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and iii. not used for time-sensitive protection or control functions between intelligent electronic devices (*e.g.*, communications using protocol IECTR-61850-90-5 R-GOOSE).	**System:** SR 1.13 - Access via untrusted networks SR 5.1 RE(1) - Physical network segmentation SR 5.1 RE(3) - Logical and physical isolation of critical networks **Embedded device, network device, host device, software application:** NDR 1.13 RE(1) - Access via untrusted networks NDR 5.2 RE(1) - Zone boundary protection
CIP-003-9	Attachment 1, Section 3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.	**System:** SR 1.13 - Access via untrusted networks SR 1.1 Human user identification and authentication SR 1.2 RE(1) - Unique identification and authentication **Embedded device, network device, host device, software application:** CR 1.1 - Human user identification and authentication CR 1.2 RE(1) - Unique identification and authentication

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-003-9	Attachment 1 Part 5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability): • Antivirus software, including manual or managed updates of signatures or patterns; • Application whitelisting; or • Other method(s) to mitigate the introduction of malicious code.	**System:** SR 3.2 - Malicious Code Protection SR 2.3(a) - Preventing the use of portable and mobile devices SR 2.3(b) - Requiring context specific authorization SR 2.4 (b) - Requiring proper authentication and authorization for origin of the code **Embedded device, network device, host device, software application:** CR 2.2 - Wireless use control (Components) NDR 2.4 RE(1) - Mobile code authenticity check HDR 3.2 RE1 - Report version of code protection

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-003-9	Attachment 1 5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any: 5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability): • Review of antivirus update level; • Review of antivirus update process used by the party; • Review of application whitelisting used by the party; • Review use of live operating system and software executable only from read-only media; • Review of system hardening used by the party; or • Other method(s) to mitigate the introduction of malicious code 5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.	**System:** SR 3.2 - Malicious Code Protection SR 2.3 - Use control for portable and mobile devices SR 2.3 (a) - Preventing the use of portable and mobile devices SR 2.3 (b) - Requiring context specific authorization SR 2.4 - Mobile code SR 2.4 (b) - Requiring proper authentication and authorization for origin of the code **Embedded device, network device, host device, software application:** CR 2.2 - Wireless use control (Components) NDR 2.4 RE(1) - Mobile code authenticity check SAR/EDR/HDR/NDR 3.2 - Protection from malicious code HDR 3.2 RE1 - Report version of code protection
CIP-003-9	Attachment 1 5.3 For Removable Media, the use of each of the following: 5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and 5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System	**System:** SR 3.2 - Malicious Code Protection SR 2.3 - Use control for portable and mobile devices SR 2.3 (a) - Preventing the use of portable and mobile devices SR 2.3 (b) - Requiring context specific authorization **Embedded device, network device, host device, software application:** CR 2.2 - Wireless use control (Components)

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
		NDR 2.4 RE(1) - Mobile code authenticity check SAR/EDR/HDR/NDR 3.2 - Protection from malicious code HDR 3.2 RE1 - Report version of code protection
CIP-003-9	Attachment 1 Part 6: Vendor Electronic Remote Access Security Controls 6.1 One or more method(s) for determining vendor electronic remote access	**System:** SR 1.13 - Access via untrusted networks SR 2.3 RE (1) - Enforcement of security status of portable and mobile devices SR 2.7 - Concurrent session control
CIP-003-9	Attachment 1 Part 6: Vendor Electronic Remote Access Security Controls 6.2 One or more method(s) for disabling vendor electronic remote access;	**System:** SR 2.6 - Remote session termination SR 5.2 - RE 2 Island mode SR 5.2 - RE3 Fail close
CIP-003-9	Attachment 1 Part 6: Vendor Electronic Remote Access Security Controls 6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access	**System:** SR 5.2 - Zone boundary protection **Embedded device, network device, host device, software application:** NDR 5.2 - Zone boundary protection
CIP-003-9	Attachment 2 Section 3.1: Electronic Access Controls: Documentation…or lists of implemented electronic access controls (*e.g.*, access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways)	**System:** SR 5.1 - Network segmentation SR 5.2 - Zone Boundary protection **Embedded device, network device, host device, software application:** NDR 5.2 - Zone boundary protection CR 5.1 - Network segmentation

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-003-9	Attachment 2 Section 3.2: Documentation of authentication for Dial-up Connectivity (*e.g.*, dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System)	**System:** SR 1.13 - Access via untrusted networks **Embedded device, network device, host device, software application:** CR 1.1 - Human user identification and authentication CR 1.2 - Unique identification and authentication NDR 1.13 - Access via untrusted networks
CIP-004-7	Part 4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access	**System:** SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5A - Authenticator management SR 2.1 - Authorization enforcement SR 2.1 RE(1) - Authorization enforcement for all users **Embedded device, network device, host device, software application:** CR 1.3 - Account management CR 1.4 - Identifier management CR 1.5A - Identifier management CR 2.1 - Authorization enforcement CR 2.1 RE(1) - Authorization enforcement for all users
CIP-004-7	Part 6.1 Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI	**System:** SR 1.3 - Account management SR 1.4 - Identifier management SR 1.5A - Authenticator management SR 2.1 - Authorization enforcement SR 2.1 RE(1) - Authorization enforcement for all users **Embedded device, network device, host device, software application:** CR 1.3 - Account management CR 1.4 - Identifier management CR 1.5A - Identifier management CR 2.1 - Authorization enforcement CR 2.1 RE(1) - Authorization enforcement for all users

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-005-7	Part 1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined Electronic Security Perimeter (ESP).	**System:** SR 5.1 - Network segmentation SR 5.4 - Application partitioning **Embedded device, network device, host device, software application:** CR 5.1 - Network segmentation
CIP-005-7	Part 1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	**System:** SR 5.2 - Zone boundary protection **Embedded device, network device, host device, software application:** NDR 5.2 - Zone boundary protection
CIP-005-7	Part 1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	**System:** SR 5.2 RE(1) - Deny by default, allow by exception **Embedded device, network device, host device, software application:** NDR 5.2 RE(1) - Deny all, permit by exception
CIP-005-7	Part 1.4 Where technically feasible, perform authentication when establishing Dialup Connectivity with applicable Cyber Assets.	**System:** S-IAC-13 - Access via untrusted networks **Embedded device, network device, host device, software application:** CR 1.1 - Human user identification and authentication CR 1.1 RE(1) - Unique identification and authentication
CIP-005-7	Part 1.5 Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	**System:** SR 1.13 - Access via untrusted networks SR 5.3 - General purpose, person-to-person communication restrictions SR 6.2 - Continuous monitoring **Embedded device, network device, host device, software application:** CR 6.2 - Continuous monitoring NDR 1.13 - Access via untrusted networks NDR 5.3 - General purpose, person-to-person communication restrictions

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-005-7	Part 2.1 For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	n/a
CIP-005-7	Part 2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	n/a
CIP-005-7	Part 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.	**System:** SR 1.1 - Multifactor authentication for untrusted networks **Embedded device, network device, host device, software application:** CR 1.1 RE(2) - Multifactor authentication for all interfaces
CIP-005-7	Part 2.4 Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	**System:** SR 1.13 - Access via untrusted networks SR 2.5 - Session Lock **Embedded device, network device, host device, software application:** CR 2.5A - Session lock – initiation
CIP-005-7	Part 2.5 Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	**System:** SR 3.8 RE (1) - Invalidation of session IDs after session termination SR 2.6 - Remote session termination **Embedded device, network device, host device, software application:** CR 2.6 - Remote session termination CR 3.8A - Session integrity

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-005-7	Part 3.1 Have one or more method(s) to determine authenticated vendor initiated remote connections.	**System:** SR 1.1 RE(1) - Unique identification and authentication SR 3.8 - Unique session ID generation and recognition SR 2.6 - Remote session termination
CIP-005-7	Part 3.2 Have one or more method(s) to terminate authenticated vendor initiated remote connections and control the ability to reconnect.	**System:** SR-3.8 RE(1) - Invalidation of session IDs after session termination SR 2.6 - Remote session termination **Embedded device, network device, host device, software application:** CR 2.5A - Session lock - initiation CR 2.6 - Remote session termination CR 3.8A - Session integrity
CIP-006-6	Part 1.6 Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	**Embedded device, network device, host device, software application:** EDR 3.11 - Physical tamper resistance and detection HDR 3.11 - Physical tamper resistance and detection NDR 3.11 - Physical tamper resistance and detection EDR 3.13 - Use of physical diagnostic and test interfaces HDR 3.13 - Use of physical diagnostic and test interfaces HDR 3.13 - Use of physical diagnostic and test interfaces EDR 3.13 RE(1) - Active monitoring HDR 3.13 RE(1) - Active monitoring NDR 3.13 RE(1) - Active monitoring
CIP-006-6	Part 1.7 Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	**Embedded device, network device, host device, software application:** EDR 3.11 RE(1) - Notification of a tampering attempt HDR 3.11 RE(1) - Notification of a tampering attempt NDR 3.11 RE(1) - Notification of a tampering attempt

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-007-6	Part 1.1 Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed.	**System:** SR 7.7 - Least functionality **Embedded device, network device, host device, software application:** EDR 2.13 - Use of physical diagnostic and test interfaces HDR 2.13 - Use of physical diagnostic and test interfaces NDR 2.13 - Use of physical diagnostic and test interfaces EDR 2.13 RE(1) - Active monitoring HDR 2.13 RE(1) - Active monitoring NDR 2.13 RE(1) - Active monitoring CR 7.7 - Least functionality
CIP-007-6	Part 1.2 Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	**System:** SR 7.7 - Least functionality **Embedded device, network device, host device, software application:** EDR 2.13 - Use of physical diagnostic and test interfaces HDR 2.13 - Use of physical diagnostic and test interfaces NDR 2.13 - Use of physical diagnostic and test interfaces EDR 2.13 RE(1) - Active monitoring HDR 2.13 RE(1) - Active monitoring NDR 2.13 RE(1) - Active monitoring CR 7.7 - Least functionality

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-007-6	Part 2.1 A patch management process for tracking, evaluating and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	**62443-4-1** Product security development lifecycle requirements SM-2 - Security update documentation SUM-3 - Dependent component or operating system security update documentation **System:** Section 0.3 - Using 62443-4-1 ISA/EC 62443-3-3) **Embedded device, network device, host device, software application:** CCSC 4 Software development process (ISA/IEC 62443-4-2)
CIP-007-6	Part 3.1 Deploy method(s) to deter, detect or prevent malicious code.	**System:** SR 3.2 - Malicious Code Protection SR 3.2 RE(1) - Malicious code protection at entry and exit points **Embedded device, network device, host device, software application:** SAR 3.2 - Protection from malicious code EDR 3.2 - Protection from malicious code HDR 3.2 - Protection from malicious code NDR 3.2 - Protection from malicious code
CIP-007-6	Part 3.2 Mitigate the threat of detected malicious code	**System:** SR 3.2 - Malicious Code Protection SR 3.2 RE(1) - Malicious code protection at entry and exit points **Embedded device, network device, host device, software application:** SAR 3.2 - Protection from malicious code EDR 3.2 - Protection from malicious code HDR 3.2 - Protection from malicious code NDR 3.2 - Protection from malicious code

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-007-6	Part 3.3 For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	**System:** SR 3.2 Malicious code protection
CIP-007-6	Part 4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code	**System:** SR 1.11 - Unsuccessful login attempts SR 2.8 - Auditable events SR 2.8 RE1 - Centrally managed system wide audit trail **Embedded device, network device, host device, software application:** CR 1.11A - Unsuccessful login attempts - limit number CR 2.8 - Auditable events - categories
CIP-007-6	Part 4.2 Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	**System:** SR 1.11 - Unsuccessful login attempts SR 2.8 - Auditable events SR 2.8 RE(1) - Centrally managed system wide audit trail SR 2.9 RE(1) - Audit storage capacity - warn when threshold reached SR 2.10 - Response to audit processing failures SR 3.4 RE(2) - Automated notification of integrity violations SR 6.2 – Continuous monitoring **Embedded device, network device, host device, software application:** CR 2.8 - Auditable events – categories CR 2.9 RE(1) - Audit storage capacity - warn when threshold reached CR 6.2 - Continuous monitoring

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
		CR 2.10 - Response to audit processing failures CR 3.4 RE2 - Automated notification of integrity violations EDR 3.11 - Notification of a tampering attempt HDR 3.11 - Notification of a tampering attempt NDR 3.11 - Notification of a tampering attempt
CIP-007-6	Part 5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.	**System:** SR 1.1 - Human user identification and authentication SR 1.1 RE(1) - Unique identification and authentication SR 1.1 RE(3) - Multifactor authentication for all networks SR 1.5 - Authenticator management **Embedded device, network device, host device, software application:** CR 1.1 - Human user identification and authentication CR 1.1 RE(1) - Unique identification and authentication CR 1.5 - Authenticator management
CIP-007-6	Part 5.2 Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location or by system type(s).	**System:** SR 1.5 - Change default authenticators SR 1.3 RE(1) - Unified account management **Embedded device, network device, host device, software application:** CR 1.5B - Authenticator management - change default authenticators

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-007-6	Part 5.4 Change known default passwords, per Cyber Asset capability	**System:** SR 1.5 - Change default authenticators **Embedded device, network device, host device, software application:** CR 1.5B - Authenticator management - change default authenticators
CIP-007-6	Part 5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters *(e.g.*, uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.	**System:** SR 1.7 - Strength of password-based authentication **Embedded device, network device, host device, software application:** CR 1.7 - Strength of password-based authentication
CIP-007-6	Part 5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	**System:** SR 1.7 RE(1) - Password generation and lifetime restrictions for human users **Embedded device, network device, host device, software application:** CR 1.7 RE(1) - Password generation and lifetime restrictions for human users
CIP-007-6	Part 5.7 Where technically feasible, either: - Limit the number of unsuccessful authentication attempts; or - Generate alerts after a threshold of unsuccessful authentication attempts.	**System:** SR 1.11 - Unsuccessful login attempts **Embedded device, network device, host device, software application:** CR 1.11A - Unsuccessful login attempts - limit number

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-009-6	Part 1.3 One or more processes for the backup and storage of information required to recover BES Cyber System functionality	**System:** SR 7.3 – Control System Backup SR 7.3 RE(1) - Backup verification SR 7.4 - SUT recovery and reconstitution **Embedded device, network device, host device, software application:** CR 7.3 - Control system backup CR 7.3 RE(1) - Backup integrity verification CR 7.4 - Control system recovery and reconstitution
CIP-009-6	Part 1.4 One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	**System:** SR 7.3 - Backup verification **Embedded device, network device, host device, software application:** CR 7.3 RE(1) - Backup integrity verification
CIP-009-6	Part 1.5 One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	**System:** SR 7.3 - Control system backup **Embedded device, network device, host device, software application:** CR 7.3 - Control system backup
CIP-010-4	Part 1.1 Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	**62443-4-1**-SG-3 - Security Hardening Guidelines **System:** SR 7.6 - Network and security configuration settings SR 7.8 - SUT component inventory **Embedded device, network device, host device, software application:** CR 7.6 - Network and security configuration settings CR 7.8 - Control system component inventory

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-010-4	Part 1.4 For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	**62443-4-1**- 5.2.1 SM-1 - Development Processes **System:** SR 3.3 - Security functionality verification SR 7.8 - SUT component inventory **Embedded device, network device, host device, software application:** CR 3.3 Security functionality verification
CIP-010-4	Part 1.6 Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	**Embedded device, network device, host device, software application:** EDR 3.10 - Support for updates EDR 3.10 RE(1) - Update authenticity and integrity HDR 3.10 - Support for updates HDR 3.10 RE(1) - Update authenticity and integrity NDR 3.10 - Support for updates NDR 3.10 RE(1) - Update authenticity and integrity
CIP-010-4	Attachment 1 1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.	**System:** SR 2.3 - Use control for portable and mobile devices SR 2.3 RE(1) - Enforcement of security status of portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-010-4	Attachment 1 1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize: 1.2.1. Users, either individually or by group or role; 1.2.2. Locations, either individually or by group; and 1.2.3. Uses, which shall be limited to what is necessary to perform business functions.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-010-4	Attachment 1 1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability): • Security patching, including manual or managed updates; • Live operating system and software executable only from read-only media; • System hardening; or • Other method(s) to mitigate software vulnerabilities.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-010-4	Attachment 1 1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability): • Antivirus software, including manual or managed updates of signatures or patterns; • Application whitelisting; or • Other method(s) to mitigate the introduction of malicious code.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-010-4	Attachment 1 1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s): • Restrict physical access; • Full-disk encryption with authentication; • Multi-factor authentication; or • Other method(s) to mitigate the risk of unauthorized use	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-010-4	Attachment 1 2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability): • Review of installed security patch(es); • Review of security patching process used by the party; • Review of other vulnerability mitigation performed by the party; or • Other method(s) to mitigate software vulnerabilities.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-010-4	Attachment 1 2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability): • Review of antivirus update level; • Review of antivirus update process used by the party; • Review of application whitelisting used by the party; • Review use of live operating system and software executable only from read-only media; • Review of system hardening used by the party; or • Other method(s) to mitigate malicious code.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-010-4	Attachment 1 2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-010-4	Attachment 1 3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize: 3.1.1. Users, either individually or by group or role; and 3.1.2. Locations, either individually or by group.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-010-4	Attachment 1 3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall: 3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and 3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.	**System:** SR 2.3 - Use control for portable and mobile devices **Embedded device, network device, host device, software application:** SAR 2.4A-C - Mobile code - control execution EDR 2.4A-C - Mobile code - control transfer by user HDR 2.4A-C - Mobile code - integrity check NDR 2.4 RE(1) - Mobile code authenticity check
CIP-011-3	Part 1.2 Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality	**System:** SR 4.1 - Information confidentiality SR 4.1 RE(1) - Protection of confidentiality at rest or in transit via untrusted networks SR 4.2 - Information persistence SR 4.2 RE(1) - Purging of shared memory resources **Embedded device, network device, host device, software application:** CR 4.1A - Information confidentiality - at rest CR 4.1B - Information confidentiality - in transit CR 4.2 - Information persistence
CIP-011-3	Part 2.1 Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	**System:** SR 4.2 - Information persistence **Embedded device, network device, host device, software application:** CR 4.2 - Information persistence CR 4.2 RE(1) - Erase of shared memory resources

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-011-3	Part 2.2 Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	**System:** SR 4.2 - Information persistence **Embedded device, network device, host device, software application:** CR 4.2 - Information persistence CR 4.2 RE(1) - Erase of shared memory resources
CIP-012-2	Part 1.1 - Identification of method(s) used to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers; 1.1. Identification of method(s) used to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers; • Methods of mitigation used to protect against the unauthorized disclosure and unauthorized modification of the data (*e.g.*, data masking, encryption/decryption) while such data is being transmitted between Control Centers • Physical access restrictions to unencrypted portions of the network	**System:** SR 3.1 - Communication integrity SR 3.1 RE(1) - Cryptographic integrity protection SR 4.1 - Information confidentiality SR 4.1 RE(1) - Protection of confidentiality at rest or in transit via untrusted networks SR 4.2 RE(2) - Protection of confidentiality across zone boundaries **Embedded device, network device, host device, software application:** CR 3.1 - Communication integrity CR 4.1 B - Information confidentiality CR 4.2 RE(1) - Erase of shared memory resources

Standard	Requirement Part or Attachment Reference	Applicable ISA/IEC 62443 System and Component and Security Requirements
CIP-012-2	Part 1.2 Identification of method(s) used to mitigate the risk(s) posed by the loss of the ability to communicate Real-time Assessment and Real-time monitoring data between Control Centers; • Identification of alternative communication paths or methods between Control Centers • Procedures explaining the use of alternative systems or methods for providing for the availability of the data • Service level agreements with carriers containing high availability provisions • Availability or uptime reports for equipment supporting the transmission of Real-time Assessment and Real-time monitoring data	n/a
CIP-012-2	Part 1.3 Identification of method(s) used to initiate the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers; • Contract, memorandum of understanding, meeting minutes, agreement or other information outlining the methods used for recovery • Methods for the recovery of links such as standard operating procedures, applicable sections of CIP-009 recovery plan(s), or similar technical recovery plans • Documentation of the process to restore assets and systems that provide communications • Process or procedure to contact a communications link vendor to initiate and or verify restoration of service	**System:** SR 7.4 - Control system recovery and reconstitution