The bridge to possible

NERC CIP Compliance

A Solutions-Based Approach to Network and Cybersecurity for Power Utilities

Overview

The focus of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) reporting and audit compliance program is achieving system-level cybersecurity from each utility operator connected to the bulk electric systems (BES) in United States and adjacent domains. Each utility operator contributing to the BES is subject to these compliance mandates. The NERC CIP compliance program has been in place for many years and most utilities have some level of adherence, but as both technology and cybersecurity concerns advance, the requirements are also becoming more prescriptive with frequent updates.

A Reliability Standard Audit Worksheet (RSAW) is a critical component of the compliance process and is taken seriously by NERC. Significant preparation and planning contributes to this set of documents. This plan provides operations teams a worksheet to meet the compliance specifications and is also used by the auditors to evaluate the level of compliance. The worksheet serves as evidence of that compliance.

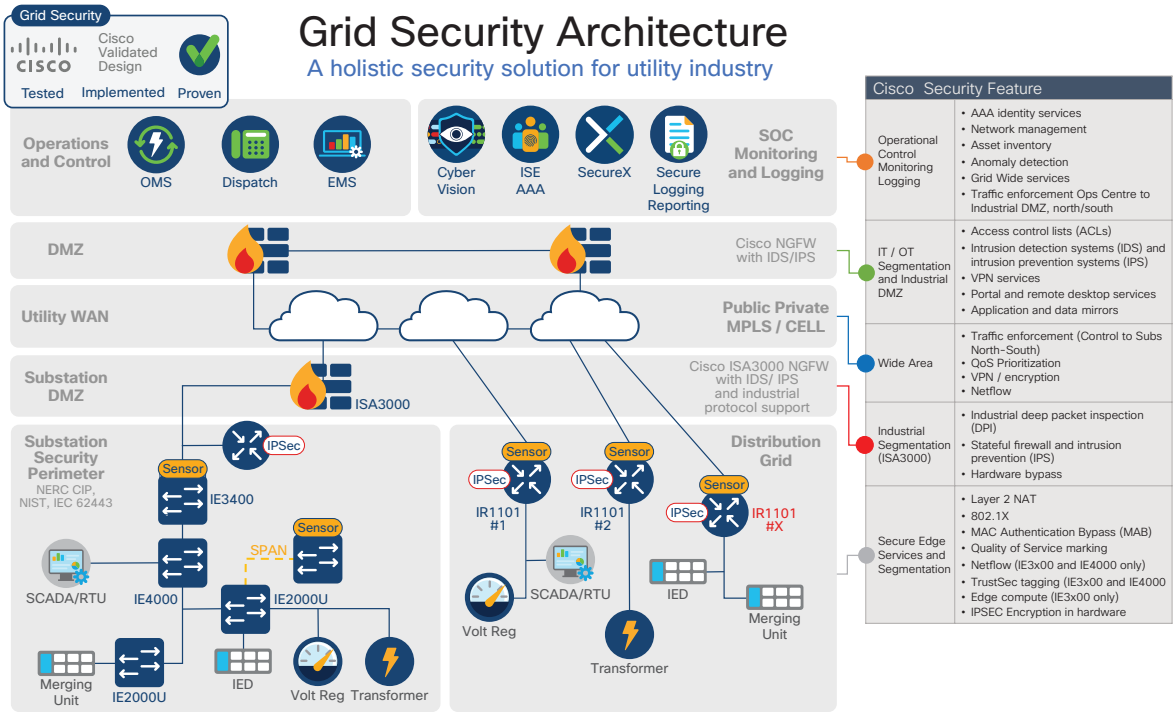
The prospect of a NERC CIP audit can be intimidating, time consuming, and costly. Auditors require standard reports, and may also request additional proof of compliance while on site. Last minute or ad-hoc requests demonstrate the utility's process and practices in action and further confirm that the plan and documentation is comprehensive and aligned.

Cisco's goal is to assist and support our utility customers with a comprehensive security architecture that addresses cybersecurity at the core of the solution. Additionally, the solution compliance requirements are layered with reliability improvements for the grid. The solution is cost effective and sensitive to both capital expenditure (CapEx) and operational expenditure (OpEx) concerns of a utility operator. This white paper addresses the applicability of the Cisco Grid Security solution in response to NERC CIP mandates.

The bridge to possible

Cisco Grid Security Architecture

The Grid Security Architecture is based on industry-leading innovations in Cisco Internet of Things (IoT) security and networking technologies that are built into Cisco products and solutions.



Cisco Cyber Vison greatly enhances industrial control system (ICS) visibility, operational insights, and threat detection. The Cisco Grid Security Architecture provides comprehensive cybersecurity protection at a lower security operational cost with a validated blueprint to accelerate implementation.

Cisco Cyber Vison greatly enhances industrial control system (ICS) visibility, operational insights, and threat detection. The Cisco Grid Security Architecture provides comprehensive cybersecurity protection at a lower security operational cost with a validated blueprint to accelerate implementation.

This comprehensive security architecture with proven integration is a more operational and cost-effective answer. The integration of IT and OT around security, and leveraging the experience of IT when building to accommodate the protocols and performance requirements of the operations network, is the right approach. A well designed, implemented, and operationally-effective security posture requires a partnership between IT and OT and starts at the foundation – the physical network.

The Grid Security Cisco Validated Design (CVD) provides a holistic cybersecurity architecture to protect utility networks and processes while addressing the key security and compliance concerns of the utility grid operators. Cisco product development is based on Cisco Secure Development Lifecycle (CSDL) to ensure validity in development. This is an important baseline for any product development and a cornerstone for a robust system and security architecture that integrates, manages, and orchestrates communication and security products. Cisco IoT product development process achieved certification based on IEC 62443-4-1: Secure product development lifecycle requirements. This ensures that product development is addressing the needs of an industrial automation and control system (IACS).

The bridge to possible

Remote workers use Cisco AnyConnect from their device to connect through intermediate systems and then onto the trusted network based on well-defined policies and layers of authentication.

Address Security Challenges of Utility Grid Operators

Identify: Unknown and Unpatched Assets

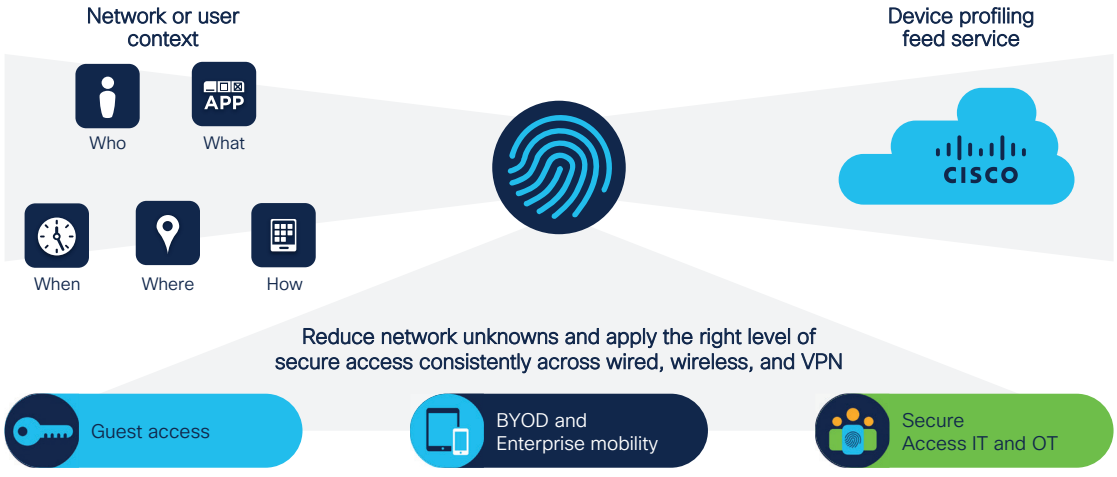
The utility grid has gone virtually unchanged for many years with assets operating in place for decades. Asset discovery often requires time consuming, costly, and even hazardous manual inspections that are error prone and may be obsolete in just days. This is a security risk and a compliance issue. Cisco Cyber Vision automatically discovers these devices, providing significant levels of device detail, patch information, security posture assessments and communications flow information. Grid modernization efforts are underway for the successful transition from legacy and often unmanageable equipment making the mapping of these devices and their communication flows more important than ever.

Protect: Lack of Separation and Segmentation

Separation and segmentation are at the heart of security best practices providing numerous points of inspection. Separation and control of the flow of operational data and critical applications is best accomplished at the network level. Many regulatory bodies such as NERC-CIP, IEC, NIST, EU NIS and others are dictating the separation and segmentation of operational and monitoring, control traffic, physical security, and the wider IT traffic from each other throughout the network. The Cisco Industrial Security Appliance ISA 3000 and next generation firewall (NGFW), TrustSec, and encryption techniques are part of the Cisco Secure architecture that leverages these tools to achieve the system-wide segmentation required.

Protect: Secure Remote Access

Remote access security starts by establishing validity of the device and the device user before secure access to the network is granted. Secure access allows a utility to reduce costly manual intervention and the ability to leverage trusted third-parties. The Cisco ISA 3000 firewalls establish a secure DMZ and inspection points within the substation. Remote workers use Cisco AnyConnect from their device to connect through intermediate systems and then onto the trusted network based on well-defined policies and layers of authentication. The Cisco Identity Service Engine (ISE) uses standards-based tools like 802.1x and MAC profiling for each edge port. All features are supported on the Cisco Catalyst Industrial Ethernet switching portfolio including the Catalyst IE3x00, IE4000, IE5000 families.

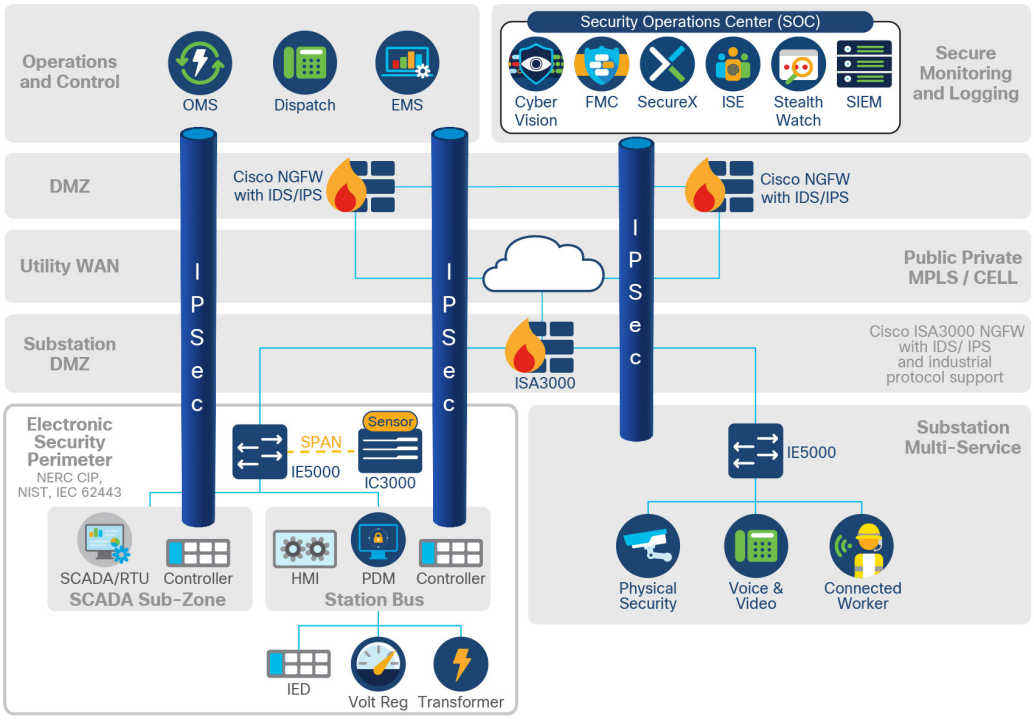


The bridge to possible

Port security on Cisco Catalyst Industrial Ethernet switches and a wide variety of encryption technologies on the ISA 3000 or any of the Cisco Industrial Routers contribute to the design.

Protect: Data Availability, Integrity and Confidentiality

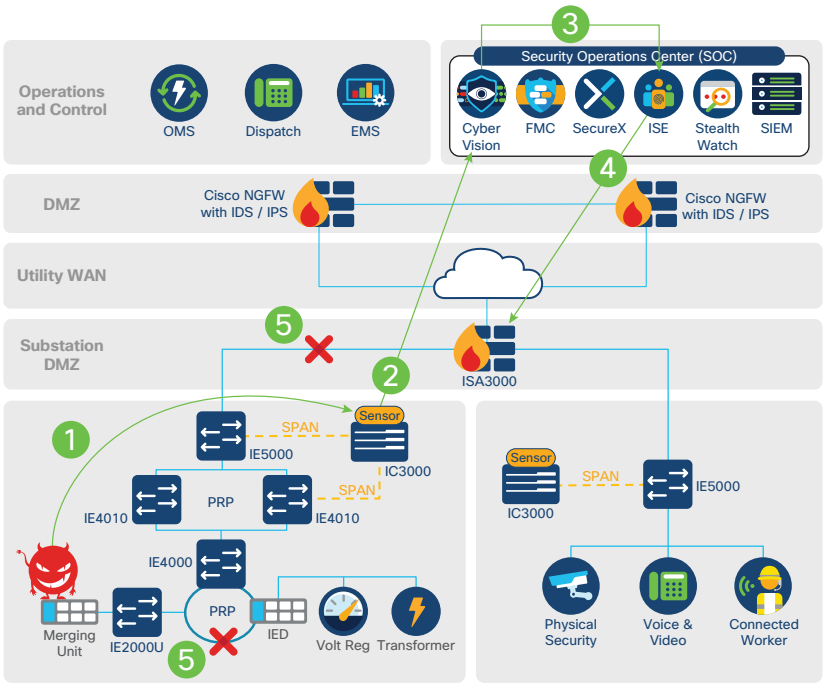
Grid operators depend on secure and reliable data transport for real-time control and monitoring of data as well as remote operational modifications and results. Compliance mandates separation of critical data and encryption of all data exiting a physical perimeter. Logging information must also be securely delivered and maintained. Access control based on strong authentication and data confidentiality on a highly-available network infrastructure are foundational. Port security on Catalyst Industrial Ethernet switches and a wide variety of encryption technologies on the ISA 3000 or any of the Cisco Industrial Routers IR1101, IR807, and CGR-2010 contribute to the design.



Detect and Respond

Utilities face several challenges when it comes to detecting and responding to cybersecurity attacks. The first is a lack of visibility. Operators can only stop malicious activities they can see. Another is a lack of reliable mitigation. A methodology to stop cyberattacks requires a variety of cybersecurity technologies working together seamlessly. A fully integrated security architecture that can discover threats and provide the information necessary for mitigation is required. The solution includes Cyber Vision, Stealthwatch, SecureX, and the ISA 3000 industrial firewall.

The bridge to possible



Detection & Remediation :

1. Bad Actor / Compromised device
2. Passive monitoring and detection
3. Alert to ISE / SIEM
4. Policy push to ISA3000 / IE switch
5. Bad actor blocked

A fully integrated security architecture that can discover threats and provide the information necessary for mitigation is required. The solution includes Cyber Vision, Stealthwatch, SecureX, and the ISA 3000 industrial firewall.

Compliance Requirements

A well-architected and comprehensive security solution can provide a secure, compliant, and operationally efficient OT network. A single system is easier to maintain, more reliable and trusted, with fewer integration costs and ongoing operational costs, thus reducing both CapEx and OpEx over the life of the system.

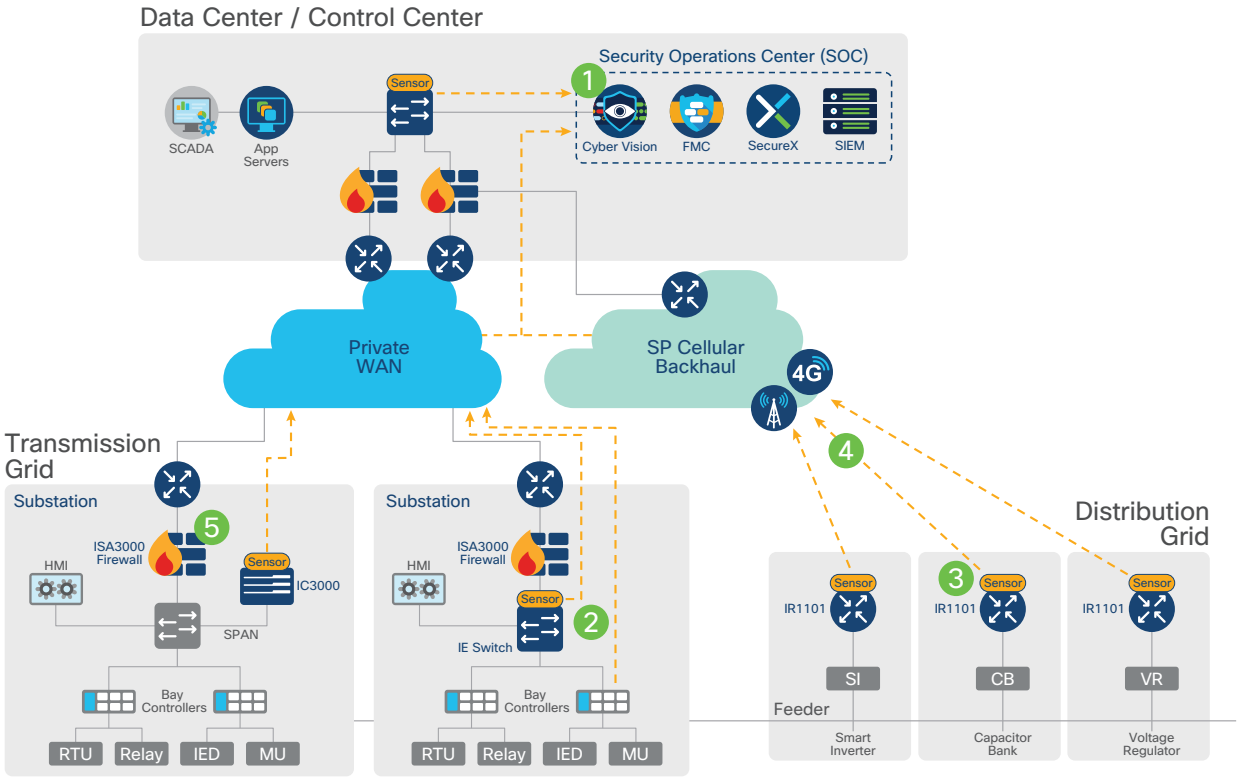
A matrix mapping NERC-CIP mandates to Cisco solutions is located at the end of this document.

Defense-in-Depth

A solid security architecture leverages a defense-in-depth approach. The Cisco Grid Security CVD details the integration of multiple security tools and devices to accomplish this in an OT environment. This holistic security solution addresses the unique requirements of the utility network with best practices and compliance requirements like those found in NERC CIP and IEC 62443 and the NIST framework.

The bridge to possible

Foundational Security Architecture in Electric Utilities



1. Cyber Vision Center, Firepower Management Center and SecureX deployed at Control Center.
2. Cyber Vision Sensor embedded in IE3400 switches or deployed via one-hop SPAN on IC3000 in transmission substations.
3. Cyber Vision Sensor embedded in IR1101 gateways in the distribution grid.
4. Application-flow metadata streamed from sensors to center over utility private WAN with little network impact.
5. Industrial Security Appliance (ISA3000) provides the access control and IPS capability - in a simplistic form, it is a DMZ.

Cisco is a leader in securing enterprise networks. Cisco is also a leader in industrial networking.

A Validated Security Solution

Cisco's team of validation engineers design and build these solutions based on detailed use cases from real-world environments and scenarios. We test the full solution to the limit of its capabilities and document the results in a Cisco Validated Design (CVD). These documents can be found here: www.cisco.com/go/iotcvd

Cisco is a leader in securing enterprise networks. Cisco is also a leader in industrial networking. We are leveraging these unique portfolios of products and solutions, together with threat intelligence from Talos®, one of the world's largest security research teams, to make security inherent and embedded in the industrial network.

Cisco is not only "IT approved" but is "IT preferred", helping you streamline and accelerate security deployments in the utility industry.

The bridge to possible

Product Mapping and Alignment to NERC CIP

Requirements	Summary	Explanation/Purpose	Solution Mapping
CIP-002-5.1a	Cybersecurity – Critical Cyber Asset Identification	To identify and categorize Bulk Electric System (BES) cyber systems and their associated BES cyber assets for the application of cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES cyber systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.	Cisco Cyber Vision
CIP-003-8	Cybersecurity – Security Management Controls	Requires that responsible entities have minimum security management controls in place to protect critical cyber assets.	Cisco ISA 3000 and Firepower firewalls
CIP-005-5	Cybersecurity – Electronic Security Perimeter(s)	Requires the identification and protection of the electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter.	Cisco Duo, ISA 3000
CIP-006-6	Cybersecurity – Physical Security of Critical Cyber Assets	Addresses implementation of a physical security program for the protection of critical cyber assets.	IoT Grid Security Architecture
CIP-007-6	Cybersecurity – Systems Security Management	Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be critical cyber assets, as well as the other (non-critical) cyber assets within the electronic security perimeters.	FMC, ISA 3000, Firepower, SecureX, ISE
CIP-008-5	Cybersecurity – Incident Reporting and Response Plan	To mitigate the risk to the reliable operation of the BES as the result of a cybersecurity incident by specifying incident response requirements.	Cyber Vision, ISE, FMC SecureX, AMP for Endpoints, AMP for Networks, ThreatGrid
CIP-010-2	Cybersecurity – Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to Bulk Electric System (BES) cyber systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES cyber systems from compromise that could lead to mis-operation or instability in the BES.	Cisco FMC, Cyber Vision, Stealthwatch, ISE
CIP-011-2	Cybersecurity – Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).	Segmentation with ISA 3000, encryption, TrustSec
CIP-13-1	Supply Chain Management	To mitigate cybersecurity risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES cyber systems.	Cisco has been awarded IEC 61443-4-1 and 4-2 certifications. https://www.cisco.com/c/en/us/about/trust-center.html
CIP-014-2	Physical Security	To identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability.	Meraki MV72 outdoor camera and analytics

Identification and categorization of BES cyber systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.

Appendix A

Current NERC CIP Mandates and Detailed Solution Mappings

CIP-002-5 requires the initial identification and categorization of BES cyber systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES cyber systems. This suite of CIP standards is referred to as the Version 5 CIP cybersecurity standards.

CIP-002-5.1a Cybersecurity – Critical Cyber Asset Identification. To identify and categorize BES cyber systems and their associated BES cyber assets for the application of cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES cyber systems could have on the reliable operation of the BES. Identification and categorization of BES cyber systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.

CIP-002-5.1a is in place to determine the level of risk associated with the utility under audit and is predominantly a procedure and documentation effort. However, it is necessary to understand the level of exposure and the key components in the grid.

The requirements section R1 lists the following:

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning]

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

The Cisco architecture described in this paper identifies several mechanisms to support secure and up-to-date equipment inventory, configuration change and the authenticity of the reporting.

The measures associated with R1 are:

M1: Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

As cited above this mandate is predominantly a documentation and classification requirement. However, manual data gathering is time consuming and often difficult to control, confirm and keep updated.

The Cisco architecture described in this paper identifies several mechanisms to support secure and up-to-date equipment inventory, configuration change and the authenticity of the reporting. With technologies like dynamic multipoint virtual private network (DMVPN) a Cisco firewall or industrial gateway can establish secure encrypted tunnels to multiple locations from a substation or any grid location. Tunnel termination in a secure logging and monitoring zone in a data center or control center establishes a virtual "chain of evidence" for any changes occurring in the substation. The audit responder now has a single source of truth with time stamps of logs and inventory in a single location.

The solution would include Cisco Cyber Vision and Stealthwatch as well as the ISA 3000 or one of the Cisco Industrial Routers to establish and terminate the encryption. Authentication servers such as Cisco Identity Service Engine and switching infrastructure to support port access, assist with edge device identity, and additional security features to control access and prevent probes or threats.

CIP-003-8 Cybersecurity – Security Management Controls. Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets.

Section B describes the "Requirements and Measures" which are documentation based. This is where the reliability standard audit worksheet (RSAW) is a critical piece of the compliance response. Record keeping and document retention is critical with CIP-003 as well as workflow process and procedures and adherence to those process and procedures as detailed in the RSAW.

CIP-004-6 Cybersecurity – Personnel and Training. The objective is to minimize the risk against compromise that could lead to mis-operation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

This is a utility-specific process and procedures mandate. All of the detailed "Requirements and Measures" are very specific to cybersecurity training for utility personnel. Cisco and the Grid Security architecture have no bearing on the specifications for CIP-004. The RSAW and the preparation put into its completion will play a key role in the utility's success on this mandate.

CIP-005-5 Cybersecurity – Electronic Security Perimeter(s). Requires the identification and protection of the electronic security perimeters (ESP) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

The "Requirements and Measures" dictate the following electronic security perimeter (ESP):

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

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts and additional evidence to demonstrate implementation.

1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.

1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

1.4 Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.

1.5 Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

2.1 Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.

2.3 Require multi-factor authentication for all Interactive Remote Access sessions.

The Cisco Grid Security Architecture clearly defines and establishes an electronic security perimeter (ESP)

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP- 005-5.*

The Cisco Grid Security Architecture clearly defines and establishes an electronic security perimeter (ESP). The compliance requirements for CIP-005-5 are focused on the documentation of the established ESP and the communications and flow of data into and out of the ESP. This can be achieved in numerous ways including the manual or automated gathering of dated and time stamped log files from the ESP gateway and the encryption tunnel terminations at both ends.

The secure centralized logging and monitoring as defined in our architecture consolidates and automates the collection of this data easing the compliance and audit response burden. This architecture also includes a best practice approach for IT/OT interconnection that includes back to back firewalls and intermediate systems aka jump-hosts or jump-servers.

This can be deployed in a DMZ that includes AAA services and Cisco's IoT Signature base for intrusion detection. This signature base is continuously enhanced by our Talos research team in the form of updated Snort rule sets. This same model can be leveraged in the substation for additional levels of protection with the firewall rule set and IoT signature base with deep packet inspection on the ISA 3000 industrial firewall.

CIP-006-6 Cybersecurity – Physical Security of Critical Cyber Assets. Addresses implementation of a physical security program for the protection of Critical Cyber Assets.

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan.*

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

1.1 Define operational or procedural controls to restrict physical access.

1.2 Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.

Monitor for unauthorized access through a physical access point into a physical security perimeter.

1.3 Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

1.4 Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

1.5 Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

1.6 Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.

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.

1.8 Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.

1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.

1.10 Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- encryption of data that transits such cabling and components; or
- monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- an equally effective logical protection.

The Grid Security Architecture defines a variety of encryption options to and from the PSP and from various zones inside the substation including the electronic security perimeter (ESP) and a defined zone for cameras and badge readers and other physical security devices.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures.

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-6 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.

Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.

Retain visitor logs for at least ninety calendar days.

CIP-006-6 is primarily a documentation-specific exercise and is significantly dependent on the planning and completion of the RSAW. However, the establishment of a physical perimeter, access controls and the monitoring and logging of access are necessary. There are 3 sections where Cisco can assist a utility's compliance to this mandate: sections R1-1.4, R1-1.8 and R1-1.10. Cisco can leverage security cameras and advanced onboard analytics to help define entry, access and exit to the physical security perimeter (PSP). The Grid Security architecture established a secure portion of the data network for the purposes of camera controls access and the ability to securely deliver critical event information to the NOC/SOC as well as provide secure logging.

CIP-006-6 R1-1.10 discusses the delivery of data to and from PSPs. The rich set of access control and encryption features on the Cisco well-established suite of secure gateways, routers, and firewalls are both standards based and fully interoperable with numerous vendors.

The Grid Security Architecture defines a variety of encryption options to and from the PSP and from various zones inside the substation including the electronic security perimeter (ESP) and a defined zone for cameras and badge readers and other physical security devices.

The bridge to possible

The Cisco industrial switching portfolio supports secure group tags or TrustSec for micro-segmentation.

The Cisco industrial switching portfolio supports secure group tags or TrustSec for micro-segmentation. This tagging separates and identifies specific flows between devices, switching infrastructure, and gateways. This secure mapping can be continued and placed into specific encrypted tunnels for transport across a public network. The ISA 3000 and or any of the IR-800 or the IR-1101 or CGR-1000 or 2000 series routers support access controls and mappings into/and out of IPSEC tunnels. Segmentation and protection of data is available at the edge and deep inside the various security zones of substation, network operations center (NOC), security operations center (SOC), and control center.

CIP-007-6 Cybersecurity – Systems Security Management. Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services.*

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES cyber systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a responsible entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the responsible entity's control (i.e. as part of the telecommunication carrier's network).

The bridge to possible

Cisco routers, gateways, switches, and firewalls can be used to significantly minimize the attack surface of a utility.

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP- 007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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.

1.2 Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

Cisco routers, gateways, switches, and firewalls can be used to significantly minimize the attack surface of a utility. Cisco integrated access controls are robust and exceed the mandates for NERC CIP-007-6. The Industrial Security Appliance (ISA 3000) with deep packet inspection capabilities coupled with a robust IoT protocol aware signature-base enhanced by Snort and Talos to provide an enhanced protection level at the port and protocol level.

The ISA 3000 and all Cisco firewalls support IDS/IPS with Firepower services and the widest range of access, threat, and application controls for the harshest and most demanding industrial environments. Additionally, Cyber Vision provides asset and device discovery with deep protocol awareness and data flow mapping between peers and communications partners and paths. This gives a level of both L2 and L3 visibility previously unavailable thus eliminating unknown or undocumented devices and potential vulnerabilities with visibility and reporting of critical software patches and updates required.

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

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Cisco publishes the Cisco Product Security Incident Response Team (PSIRT) software or hardware defects identified or discovered on its public facing webpage here: https://www.cisco.com/c/en/us/support/index.html

Patch administration and/or workaround and any network configuration are also defined and can be deployed by a wide variety of network management systems such as Prime Infrastructure in an automated, manual, or phased roll out.

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable cyber assets of a BES cyber system.

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.

2.2 At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

2.3 For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches
- Create a dated mitigation plan;

or

- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

2.4 For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention.*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable cyber assets of a BES cyber system. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES cyber system.

The Cisco Grid Security Architecture uses a defense-in-depth layered methodology to seperate, segment, and isolate critical resources to prevent the spread of malicious code and to ease the remediation efforts.

The prevention, detection, and remediation of malicious code and the detection of attempted propagation of such code is best addressed by a fully integrated layered approach. The Cisco Grid Security Architecture uses a defense in depth layered methodology to seperate, segment, and isolate critical resources to prevent the spread of malicious code and to ease the remediation efforts. The same approach is useful in the detection process and is accomplished with multiple layers of strategically placed firewalls performing IoT specific deep packet inspections.

Cyber Vision passively monitors edge devices and equipment to identify code changes and operational changes and/or anomalies of devices in the OT environment. Furthermore, application level performance and the inspection and monitoring of "data in flight" at the higher layers is supported by Cisco Stealthwatch. These products can provide separate reporting or be integrated with Cisco SecureX for advanced level of threat detection and mitigation support. All products are also proven to integrate well with standards-based security information and event management (SIEM) products for correlation and post-event forensics and remediation.

3.1 Deploy method(s) to deter, detect, or prevent malicious code.

3.2 Mitigate the threat of detected malicious code.

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.

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

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES cyber systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Cisco networking equipment includes a robust logging facility and supports integration to a secure and protected facility for centralized logging collection and retention, such as Secure Logging and Monitoring.

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;

4.1.2. Detected failed access attempts and failed login attempts;

4.1.3. Detected malicious code.

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.

4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances

4.4 Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

Cisco networking equipment includes a robust logging facility and supports integration to a secure and protected facility for centralized logging collection and retention, such as Secure Logging and Monitoring. This may be a SOC that also includes SecureX integrations or a SIEM. Login attempts both successful and unsuccessful are logged on the box and can be logged via terminal access controller access control system (TACACS+) to include operational or configuration changes with detailed time stamps and user ids. AAA services of both Cisco and third-party devices or port connections can be authenticated because the Cisco Identity Services Engine provides AAA services.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls.*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

The logon facilities on Cisco networking equipment supports encrypted passwords of various lengths and supports user id specific integrations to LDAP via TACACS+ and AAA services on the Identity Services Engine (ISE).

5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.

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).

5.3 Identify individuals who have authorized access to shared accounts.

5.4 Change known default passwords, per Cyber Asset capability

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, non- alphanumeric) or the maximum complexity supported by the Cyber Asset.

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.

5.7 Where technically feasible, either:

- Limit the number of unsuccessful authentication attempts; or
- Generate alerts after a threshold of unsuccessful authentication attempts.

The logon facilities on Cisco networking equipment supports encrypted passwords of various lengths and supports user id specific integrations to LDAP via TACACS+ and AAA services on the Identity Services Engine (ISE).

CIP-008-5 Cyber Security – Incident Reporting and Response Plan. To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan*

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

CIP-008-5 is predominantly a process and procedure only mandate requiring detailed planning and completion of the RSAW. SecureX and SIEM integration from switches routers, Cyber Vision, Stealthwatch, ISA 3000 firewalls and FMC may play a part of the evidence collection and determination of the severity of an incident but these are not specifically applicable to CIP-008-5.

CIP-009-6 Cyber Security – Recovery Plans for BES Cyber Systems. To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications.*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP- 009-6 Table R1 – Recovery Plan Specifications.*

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES cyber system functionality occurs.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-65 Table R2 – Recovery Plan Implementation and Testing.*

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

The bridge to possible

Cisco Grid Security Architecture enables improved procedures and operational effectiveness.

CIP-009-5 is a planning, process and procedural mandate. Cisco Grid Security Architecture enables improved procedures and operational effectiveness. It may have no direct impact on this mandate as it is really focused on the planning and response to a cyber incident and the documentation of the procedures the utility intends to follow in such an event.

CIP-010-2 Cyber Security – Configuration Change Management and Vulnerability Assessments. To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

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.

1.2 Authorize and document changes that deviate from the existing baseline configuration.

1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

Change management of network equipment and edge devices will be monitored and reported upon as part of the defense-in-depth approach. Configuration changes should only come from well know entities within the bounds of the utility, from the control center.

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.

1.5 Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Change management of network equipment and edge devices will be monitored and reported upon as part of the defense-in-depth approach. Configuration changes should only come from well know entities within the bounds of the utility, from the control center. The ability to secure this is well within the capabilities of the Grid Security Architecture and the services and equipment comprising that architecture.

This approach is useful in the detection process and is accomplished with multiple layers of strategically placed firewalls performing IoT specific deep packet inspections. Cyber Vision monitors edge devices and equipment to identify code changes and operational changes and/or anomalies of devices in the OT environment. Furthermore, application level performance and the inspection and monitoring of “data in flight” at the higher layers is supported by Cisco Stealthwatch. All three products can provide sperate reporting or be integrated Cisco SecureX for advanced level of threat detection and mitigation support. All products are also proven to integrate well with standards based SIEM products for correlation and post event forensics and remediation.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring.*

Cisco Cyber Vision has been validated to identify edge device, state and operational behavior changes.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

2.1 Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

Cisco networking equipment and devices, when properly configured, will log any and all changes. TACACS+ can identify the user credentials and changes made. It is highly recommended that these logs be sent via an encrypted facility to a central logging server or collector in a secured section of a control center or data center for centralized reporting and to ease audit response. Furthermore, devices entering and exiting the network can be identified at the switch port level if changes in MAC address occur or logging of just the port changing state (up/down). Cisco Cyber Vision has been validated to identify edge device, state and operational behavior changes. These changes are also logged in the manner identified above.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3– Vulnerability Assessments*.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

3.1 At least once every 15 calendar months, conduct a paper or active vulnerability assessment.

3.2 Where technically feasible, at least once every 36 calendar months:

3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and

3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Cisco Cyber Vision provides detailed mapping of edge devices and flows between these devices and head end facilities to assist with this requirement.

The Cisco Grid Security architecture includes devices and systems to simplify and enhance the assessment process for a utility.

3.3 Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.

3.4 Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

The Cisco Grid Security architecture includes devices and systems to simplify and enhance the assessment process for a utility. Cisco Cyber Vision, Stealthwatch, ISA 3000 and SecureX are valuable tools for a utility to identify edge devices, mappings of traffic flows to/from and between devices as well as perform anomaly detection and deep packet protocol analysis. Detailed information on IoT edge devices software versions, patch status, and reporting of known vulnerabilities via a detailed knowledge base of IEDs, PLCs and other IoT devices are included with Cyber Vision. Furthermore, Cisco has the ability to perform this evaluation as a service.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

CIP-011-2 Cyber Security – Information Protection. To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).

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

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES cyber system information.

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-2 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

1.1 Method(s) to identify information that meets the definition of BES Cyber System Information.

1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

CIP-012-1 Cyber Security – Configuration Change Management and Vulnerability Assessments. The objective is to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan.

The Grid Security Architecture defines separate layers of security along the commination's path including micro-segmentation at both the operations center and field networks or substation ESPs.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Protection of the endpoints authorizing the change and the communications infrastructure between the edge device and the control center must be tightly controlled. The Grid Security Architecture defines separate layers of security along the commination's path including micro-segmentation at both the operations center and field networks or substation ESPs. Segmentation for the ESP leveraging MPLS and IPSEC VPNs with firewalls and Security Group Tags controlling access to and from the network or networks being traversed.

1.1 Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

CIP-013-1 Supply Chain Management – 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.

IEC 61443-4-1 & 62443-4-2.

Cisco has long maintained a robust Security and Trust Program which focuses on building security into the foundation of everything we do and make.

The bridge to possible

Cisco products and services meet numerous security standards and are frequently certified or audited according to international accreditation schemes.

This commitment to security cuts across our secure development life cycle, product security incident response team, trustworthy technologies, data protection program, and value chain security. We recognize the criticality of value chain security and continually assess, monitor, and improve the security of the third parties who are part of our solutions' life cycles. Cisco's layered approach to value chain security is core to our business, and part of what helps us earn a place as a trusted partner that assesses risk and effectively addresses security while enabling our customers' business. We invite you to learn more about Cisco's commitment to security & trust by visiting the Trust Center.

Cisco products and services meet numerous security standards and are frequently certified or audited according to international accreditation schemes. These include Common Criteria, FIPS 140-2, ISO 27001, ISO 27017/27018, SOC-2, C5, and FedRAMP, among others. Details regarding specific certifications and audit reports for particular products and services can be found on the Cisco Trust Portal. Additionally, Cisco has obtained certification for IEC 62443-4-1, Product Security Development Life Cycle requirements, for all IoT and industrial IoT products in our portfolio. Lastly, Cisco's quality management system is certified to ISO 9001.

CIP-014-2 Physical Security – To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability.

Physical security and specifically CIP -014 will be addressed in following documents and Cisco Validated Designs. Cisco has current offerings for physical security involving Meraki cameras and end points that include edge intelligence and analytics to assist and support customers with advanced detection and false positive elimination.

The bridge to possible

Links and References

CIPC Page:

https://www.nerc.com/comm/CIPC/Pages/default.aspx

One-Stop-Shop Spreadsheet:

https://www.nerc.com/pa/Stand/Standard%20Purpose%20Statement%20DL/US_Standard_One-Stop-Shop.xlsx

US Effective Data Page:

http://www.nerc.net/standardsreports/standardssummary.aspx

Standards, Compliance, and Enforcement Bulletin Aug 2020:

https://www.nerc.com/pa/comp/news/Documents/2020_08_17_StandardsCompliance_Bulletin.pdf

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

https://www.nerc.com/files/cip-005-5.pdf