White Paper

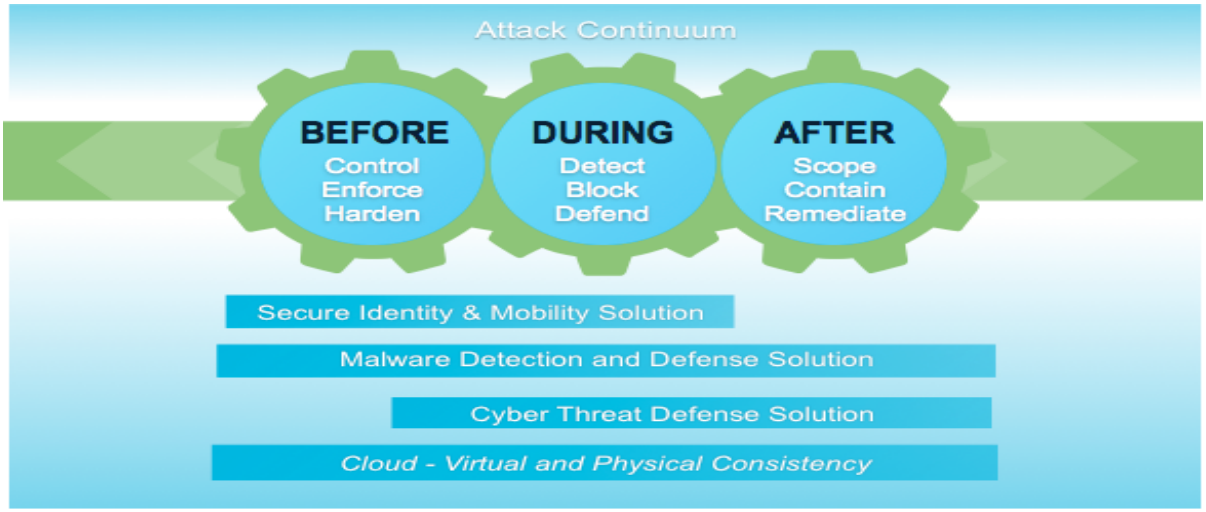
Cisco NERC CIP v5 Compliance Solutions

Cisco's Cybersecurity Solutions offer organizations a framework for protecting critical infrastructures and information from theft, corruption, or disruption from external threats as well as internal threats. The framework also protects network hardware and software from compromise, disruption, or destruction.

This paper outlines how the Cisco Cybersecurity Solutions can help Power Utilities comply with North American Electric Reliability Corporation reliability standards for Critical Infrastructures, otherwise known as ***NERC-CIPv5 Standards***. NERC's compliance program is designed to improve the reliability of the bulk power system in North America by fairly and consistently enforcing compliance with NERC standards. The program is designed to ensure that the right practices are in place so that the likelihood and severity of future system disturbances are substantially reduced, while recognizing that no standards or enforcement process can fully prevent all such disturbances from occurring.

The Cisco Cybersecurity Framework

The core of the Cisco Cybersecurity Framework is an in-depth, pervasive, systematic security that runs throughout the fabric of the network, which we refer to as the Secure Network Fabric. This Secure Network Fabric is the anchor of our framework of following the threat attack continuum of Before, During, and After a threat event.



The Cisco Cybersecurity Solutions

Secure Identity & Mobility

Cisco's Secure Identity & Mobility Solution is based on architecture which integrates the Cisco Identity Services Engine with a Cisco network infrastructure that features Cisco's TrustSec® capabilities. These combined capabilities allow the overall Identification and Authentication control for Organizational users by performing authentication and authorization of users attempting to access the organization's information system at the network layer. The solution can be configured to grant network access to entities that successfully pass the identification and authentication phase, allowing only trusted users and devices on the network, and allow access to specified applications.

Secure Internal Monitoring

Cisco's Secure Internal Monitoring is based on an architecture that integrates Lancope's StealthWatch, Cisco AMP, the Cisco Identity Services Engine, and the Cisco's NetFlow capabilities enabled by Cisco networking infrastructure. This solution allows for full visibility into the network by first base-lining the network, then monitoring network flow for anomalies. Once an anomaly is detected, the solution is contextually aware of who is involved, what device they are on, the application being used, and the type of connection they are using. The

Solution is built upon the following components: Unique interior network traffic telemetry (NETFLOW) capabilities of Cisco Catalyst® switches, Cisco routers and Cisco adaptive security appliances. Network traffic analysis capabilities provided by the StealthWatch System from Lancope. identity, reputation, and application-type contextual information for discerning the target and severity of the threat. These context points are delivered by the Cisco Identity Services Engine, Cisco Security Intelligence Operations (SIO), and NBAR on Cisco routers, respectively, and are presented via the StealthWatch Management Console. Cisco AMP uses cloud intelligence to identify threats entering the network and uniquely tracks all files through the network to remove them retrospectively should they later be determined to be malicious.

Malware Detection and Defense

The Cisco Malware Detection & Defense solution is a comprehensive framework of in-depth products and services used to identify and defend against the multiple types of malware that can wreak havoc on your network. Using a multi-tiered approach, near real time intelligence is fed to devices via our Security Intelligence Operation (SIO) and Vulnerability Research Team (VRT), which monitors and gathers web data from Cisco security products globally. Cisco ASA firewalls with botnet filtering, Cisco Intrusion Prevention System (IPS), and Web and E-mail Security Devices use this intelligence, along with their own internal technology to detect and block malware attempting to access your perimeter as well and provide multiple layers of security for your network.

Cloud – Virtual and Physical Consistency

Although NERC CIP does not yet address virtualization, Cisco has developed virtual security solutions that protect the virtual layer as we do the physical network.

Cisco Cybersecurity Product Overview

Cisco Identity Services Engine

The Cisco Identity Services Engine is a next-generation identity and access control policy platform that enables enterprises to enable new business services, enhance infrastructure security, enforce compliance, and streamline service operations. Its unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure - wired, wireless, and remote. The Cisco Identity Services Engine is an integral component of the Cisco TrustSec® solution and SecureX architecture.

The Cisco Identity Services Engine provides a single policy plane across the entire organization that combines multiple services, including authentication, authorization, and accounting (AAA), posture, profiling, device on-boarding, and guest management, on a common platform. This reduces complexity and provides consistency across the enterprise. Using the Cisco Identity Services Engine, administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion and gain end-to-end visibility into everything that is connected to the network. The following features are key points of the Cisco Identity Services Engine:

- Allows enterprises to authenticate and authorize users and endpoints via wired, wireless, and virtual private networks with consistent policy throughout the enterprise

- Prevents unauthorized network access to protect corporate assets
- Provides complete guest lifecycle management by empowering sponsors to on-board guests, reducing IT's workload
- Offers comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint
- Addresses vulnerabilities on user machines through periodic evaluation and remediation to help proactively mitigate network threats such as viruses, worms, and spyware
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention
- Offers a built-in monitoring, reporting, and troubleshooting console to assist help-desk operators and administrators in streamlining operations
- Allows finer granularity while identifying devices on the network with Active Endpoint Scanning
- Augments network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on the network
- Manages endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VAN, return to the original VAN, or isolate the endpoint from the network entirely - all in a simple interface

Cisco TrustSec® Enabled Infrastructure

Cisco TrustSec®, the security component of the Cisco Borderless Network Architecture, provides visibility into and control of who and what is connected to the network. Cisco TrustSec allows organizations to embrace the rapidly changing business environment of mobility, virtualization, and collaboration while enforcing compliance, maintaining data integrity and confidentiality, and establishing a consistent global access policy. Cisco TrustSec integrates with the Cisco SecureX Architecture™ to allow the Cisco security portfolio to take advantage of the network-based identity context for full context-aware firewalling and policy enforcement.

Lancope StealthWatch

StealthWatch by Lancope is the leading solution for flow-based security and network performance monitoring across physical and virtual environments. By leveraging NetFlow, IPFIX, sFlow and other flow data from existing routers and switches, StealthWatch provides in-depth, borderless network visibility. With StealthWatch, network operations and security teams can obtain actionable insight into who is using the network, what applications and services are in use, and how well they are performing. StealthWatch combines behavioral-based network performance and security monitoring with application and identity awareness at a fraction of the cost of conventional monitoring solutions. The system empowers IT teams to make faster, more informed decisions across mission-critical areas including troubleshooting, incident response, compliance, resource allocation, capacity planning and change management.

Cisco Prime

Cisco Prime Assurance Manager uses embedded technologies and standards such as NetFlow, Medianet, Performance Agent and Simple Network Management Protocol (SNMP) to provide network-wide end-to-end application visibility, WAN optimization visibility, troubleshooting, and quality of experience workflows, abstracting the complexity involved in setting up and collecting data. Integration with Cisco Prime Network Analysis Module provides visibility, analytics, and advanced packet-level troubleshooting for fast time to resolution and granular analysis of performance data.

Cisco AnyConnect VPN

The Cisco AnyConnect Secure Mobility Solution gives organizations the connectivity and cost benefits of Internet transport, without compromising the integrity of corporate security policies. By converging Secure Sockets Layer (SSL) and IP Security (IPsec) VPN services with comprehensive threat defense technologies. AnyConnect enforces security policy in every transaction independent of where the user is located, whether it is an enterprise, in-house owned or a SaaS application. Secure Mobility allows the administrator to require always-on secure network connectivity with a policy to permit or deny network connectivity if access is unavailable. These services are optimized for use with Cisco Web Security, and require an AnyConnect Premium license or a Secure Mobility license.

Cisco NetFlow

Cisco NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing. Cisco invented NetFlow and is the leader in IP traffic flow technology.

Cisco Sourcefire Next-Gen Intrusion Prevention System (IPS)

The Sourcefire Next-Generation Intrusion Prevention System (NGIPS) was built from the ground up to arm security teams with the protection they need in today's rapidly changing environments. Based on core competencies of contextual awareness and automation— the Sourcefire NGIPS stands apart, offering:

Real-time Contextual Awareness—See and correlate extensive amounts of event data related to IT environments, applications, users, devices, operating systems, vulnerabilities, services, processes, network behaviors, files and threats.

Advanced Threat Protection—Protect against the latest threats with the best threat prevention that money can buy as validated by independent third-party testing and thousands of satisfied customers around the world.

Intelligent Security Automation— Significantly lower the total cost of ownership and enhance the ability to keep pace
with changing environments with automated event impact assessment, IPS policy tuning, policy management, network
behavior analysis and user identification.

Cisco Sourcefire Advanced Malware Protection (AMP)

AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum. Features include:

- File Reputation captures a fingerprint of each file as it traverses the Cisco Web Security gateway and sends it to AMP's cloud-based intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policies. The Cisco Web security user interface is the same and the policy-reporting frameworks are similar to the ones you already know.
- File Sandboxing provides you with the ability to analyze unknown files that are traversing the Cisco Web Security gateway. A highly secure sandbox environment enables AMP to glean precise details about a file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP's cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection.
- File Retrospection solves the problem of malicious files that pass through perimeter defenses but are subsequently deemed a threat. In doing so, it addresses the inherent weakness of most perimeter defenses: They are effective only at a single point in time. Even the most advanced techniques may fail to identify malware at the perimeter because polymorphism, obfuscation, sleep timers, and other tactics are highly effective at avoiding detection as they cross the wire. Malicious files simply wait until they are inside the network to do their dirty work.

That's where File Retrospection comes in. Rather than operating at a point in time, File Retrospection provides a continuous analysis of files that have traversed the security gateway, using real-time updates from AMP's cloud-based intelligence network to stay abreast of changing threat levels. Once a malicious file is identified as a threat, the administrator is alerted by AMP and given visibility into who on the network may have been infected and when. As a result, customers are able to identify and address an attack quickly, before it has a chance to spread.

Cisco Adaptive Security Appliance (ASA) with Botnet Filter

The Cisco ASA 5500 Series integrates multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN, IPS with Global Correlation, antivirus, anti-spam, anti-phishing, and web filtering services. Combined with real-time reputation technology, these technologies deliver highly effective network- and application-layer security, user-based access control, worm mitigation, malware protection, improved employee productivity, instant messaging and peer-to-peer control, and secure remote user and site connectivity. The Cisco ASA Botnet Traffic Filter complements existing

endpoint security solutions by monitoring network ports for rogue activity and detecting infected internal endpoints sending command and control traffic back to a host on the Internet. The Botnet Traffic Filter database accurately and reliably identifies command and control traffic, as well as the domains or hosts receiving the information.

CyberSecurity Architecture Assessment

Cisco will assess the technical controls of the Customer's CyberSecurity Architecture against the Control Framework based on the Customer's operational requirements, recommended security practices and the Cisco Security Control Framework (SCF). The SCF, based on fundamental security architecture principles derived from industry best practices, international and industry standards, and government regulations, defines Cisco recommended technical security controls for Cisco and non-Cisco equipment. Based on the analysis of Customer's security architecture, Cisco will provide a report describing the strengths and weaknesses of the Customer's security architecture, Cisco recommendations and the gaps between the Customer's security architecture technical controls and the technical controls based on the Control Framework.

CyberSecurity Posture Assessment

Cisco can provide a point in time assessment of how effectively the Customer's CyberSecurity controls have been implemented and are being operated against the Control Framework based on operational requirements, recommended security practices and the Cisco Security Control Framework (SCF). The SCF, based on fundamental security architecture principles derived from industry best practices, international and industry standards, and government regulations, defines Cisco recommended technical security controls for Cisco and non-Cisco equipment. By emulating typical malicious activities using nondestructive means, Cisco will identify the presence of vulnerabilities in the Customer's IP, wireless, and physical infrastructure. Cisco will assess, prioritize and make recommendations regarding the identified vulnerabilities and the risks they present to the Customer's infrastructure and business. A final report documenting the assessment results will be delivered to the Customer.

Cisco Cybersecurity Solutions and NERC CIP v5 Mapping

NERC CIP 005-5 Cyber Security – Electronic Security Perimeter(s)

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
Cisco Solution: *Cisco core infrastructure products with TrustSec features will provide a network with routable protocol within a defined Electronic Security Perimeter.*			
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Cisco Solution: *See next section, 1.3*			

1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
Cisco Solution: *ASA Next Generation Firewall, a proven, stateful inspection firewall with next-generation capabilities and a host of additional network-based security controls for end-to-end network intelligence and streamlined security operations. Cisco ASA Next-Generation Firewall Services enable organizations to rapidly adapt to dynamic business needs while maintaining the highest levels of security. Cisco ASA Next-Generation Firewall Services deliver application and user ID awareness capabilities for enhanced visibility and control of network traffic.* *Cisco Identity Services Engine (ISE) can deny access by default. ISE offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use*			
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: · PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: · PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
Cisco Solution: *The Cisco AS5400 Series Universal Gateway is a secure, reliable, scalable data and voice gateway utilizing several authentication methods to include Radius.*			

1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
Cisco Solution: *The Cisco ASA Botnet Traffic Filter is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance to detect rogue traffic in the network. When internal clients are infected with malware and attempt to phone home across the network, the Botnet Traffic Filter alerts the system administrator of this though the regular logging process for manual intervention. This is an effective way to combat botnets and other malware that shares the same phone-home communications pattern.* *Cisco's network-based intrusion prevention identifies, classifies, and stops known and unknown threats with the Cisco Intrusion Prevention System (IPS). Cisco IPS is one of the most widely deployed intrusion prevention systems, providing: Protection against more than 30,000 known threats, along with signatures produced specifically for the SCADA / ICS market.* *Timely signature updates and Cisco Global Correlation to dynamically recognize, evaluate, and stop emerging Internet threats is provided by Cisco Security Intelligence Operations (SIO) and the SourceFire Vulnerability Research Team (VRT).*			

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].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP- 005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R5 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
Cisco Solution: *Cisco ASA Next-Generation Firewall Services work with Cisco AnyConnect to provide highly secure mobility, regardless of user's location. When the user is located outside the firewall, Cisco AnyConnect will recognize that the user is in an untrusted network and will establish a connection to the most optimal network scanning element (that is, the most optimal Cisco ASA Next-Generation Firewall Services). As a result, consistent access rules can be applied to the user's traffic, even when the user is located outside the office.*			
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Cisco Solution: *The Cisco AnyConnect Secure Mobility Solution gives organizations the connectivity and cost benefits of Internet transport, without compromising the integrity of corporate security policies. By converging Secure Sockets Layer (SSL) and IP Security (IPsec) VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series delivers highly customizable network access tailored to the requirements of diverse deployment environments, while providing advanced endpoint and network-level security. Supports strong encryption, including AES-256 and 3DES-168 (Security gateway device must have a strong crypto license enabled). Next-generation encryption, including NSA Suite B algorithms, ESPv3 with IKEv2, 4096-bit RSA keys, Diffie-Hellman Group 24, and enhanced SHA2 (SHA-256 and SHA-384) (only applies to IPsec IKEv2 connections; Premium ASA license required)*			

2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to: · Something the individual knows such as passwords or PINs. This does not include User ID · Something the individual has such as tokens, digital certificates, or smart cards; or · Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
Cisco Solution: *Cisco products work with industry leading authentication systems such as Radius, TACACS and others to enforce access controls.*			

CIP-007-5 Table R1 – Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to: · Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. · Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or · Configuration files of host based firewalls or other device level mechanisms that only allow needed ports and deny all others.
Cisco Solution: *The Cisco ASA provides firewall services that, by default, all ports are blocked on the outside interface. Needed ports and services can be enabled based on requirements needed for normal and emergency operations*			

1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Cisco Solution: *Cisco devices allow for unused network or console ports to be logically shut down, or be controlled utilizing tools such as TACACS or RADIUS to log and control access.*			

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more
documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R2 – Security
Patch Management. [Violation Risk Factor: Medium] [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-007-5 Table R2 – Security Patch Management and additional evidence to demonstrate
implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

Cisco Solution: *Security is part of Cisco culture. Cisco's Framework follows the attack continuum by determining what is required **Before, During,** and **After** an attack. Cisco Secure Design Lifecycle (CSDL) is our first step in the fight against malicious code. Our development teams are required to implement secure practices from the beginning of development to product rollout. Our current solutions include Malware Detection and Defense, which included the Cisco ASA Botnet Traffic Filter, which is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance to detect rogue traffic in the network. When internal clients are infected with malware and attempt to phone home across the network, the Botnet Traffic Filter alerts the system administrator of this though the regular logging process for manual intervention. This is an effective way to combat botnets and other malware that shares the same phone-home communications pattern. Another important piece of this solution is the ability to identify, classify, and stop known and unknown threats with the Cisco Sourcefire Next Generation Intrusion Prevention System (IPS). IPS Advanced Malware Protection protects against known threats by utilizing sandboxing and other techniques, and unknown threats by using retrospective methods and protects against more than 30,000 known threats with signatures produced specifically for the SCADA / ICS market.*

The Cisco Cyber Threat Defense Solution focuses on threats that have already made their way into your networks and steal vital information and/or disrupt vital operations. Cisco provides visibility into these threats and context to decipher their targets and potential damage. Security analysts gain visibility into advanced cyber threats such as: Network reconnaissance, Network interior malware proliferation, Command and control traffic, and Data exfiltration. The Solution uses interior network traffic telemetry (NETFLOW) capabilities of Cisco Infrastructure products, Identity, reputation, and application-type contextual information delivered by the Cisco Identity Services Engine, and NBAR on Cisco routers, respectively. This information is presented via the StealthWatch Management Console.

3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.
Cisco Solution: *Cisco's Security Intelligence Operations (SIO) is a cloud-based service that connects global threat information, reputation-based services, and sophisticated analysis to Cisco network security devices to provide stronger protection with faster response times. Cisco has designed Security Intelligence Operations (SIO) to cope with the constantly evolving malware environment and provide comprehensive protection. Cisco SIO also updates devices with timely signature updates and Cisco Global Correlation to dynamically recognize, evaluate, and stop emerging Internet threats*			

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more
documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R4 – Security
Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]
M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement
parts in CIP-007-5 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as
described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
Cisco Solution: *The Cisco Cyber Threat Defense Solution provides visibility into threats and provides context to decipher their targets and potential damage. Security analysts gain visibility into advanced cyber threats such as: Network reconnaissance, Network interior malware proliferation, Command and control traffic, and Data exfiltration. The Solution uses interior network traffic telemetry (NETFLOW) capabilities of Cisco Infrastructure products, Identity, reputation, and application-type contextual information delivered by the Cisco Identity Services Engine, and NBAR on Cisco routers, respectively. This information is presented via the StealthWatch Management Console. Data is retained for after the fact investigations and logging purposes. This solution includes Cisco Sourcefire AMP, which allows for data retention and for retrospective identification and tracking of Malicious files. We also support the use of SEIM products such as SPLUNK by automatically sharing contextual information associated with an attack and adding that information to the SPLUNK information.*			

4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to, paper or system generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.
Cisco Solution: *Log monitoring for troubleshooting and longer-term security analysis is also critical for security administrators. Cisco Prime Security Manager provides intuitive access to raw events from the reporting dashboard to support administrators in scenarios that require deeper analysis. A view of the policies that have been deployed provides more information on the effects of various policy rules. Cisco Prime Security Manager Event Monitor supports real-time and historical event analysis, as well as intuitive filtering capabilities.* *Lancope StealthWatch System and the IPS Manager Express, which is part of the IPS solution, will alert on Cyber Security anomalies via email alerts. The IPS Manager feeds can be personalized to your needs and can provide recommendations for securing your network.* *Alerts can also be sent via Email notification in order to keep you informed about threats when you are away. You can specify email notification intervals and events. Events can be filtered based on severity and Risk Rating.*			
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater

Cisco Solution: Cisco, SourceFire and Lancope StealthWatch logs can be kept to any set number of days depending upon available storage space.			
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	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.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.
Customer: *Required to create procedures to review logs at intervals no greater than 15 days*			

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more
documented processes that collectively include each of the applicable requirement parts in CIP-007-5 Table R5 – System
Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].
M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable
requirement parts in CIP-007-5 Table 5 – System Access Controls and additional evidence to demonstrate implementation
as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
Cisco Solution: *ISE offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use. The Cisco AnyConnect VPN capabilities protect the integrity of the corporate network by restricting VPN access based on an endpoint's security posture. Prior to establishing connectivity, a system may be validated for compliance with various antivirus, personal firewall, or antispyware products, and may undergo additional system checks with a premium license. In addition to industry-leading VPN capabilities, the Cisco AnyConnect Secure Mobility Client enables IEEE 802.1X capability, providing a single authentication framework to manage user and device identity. Consistent with its VPN functionality, the Cisco AnyConnect Secure Mobility Client supports IEEE 802.1AE (MACsec) for data confidentiality, data integrity, and data origin authentication on wired networks, safeguarding communication between trusted components of the network.]*			

5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
Cisco Solution: *The Cisco Secure Identity Solution provides valuable audit information regarding network authentication, authorization, accountability and enforcement for incorporation into an organization overall audit and accountability policy and procedures. All components of this solution, including ISE, and network device produce valuable audit information to support the organizations audit and accountability policy and procedures. While each component provides logging information, each component also provides the ability to upload this information into an organizational auditing system via the syslog protocol*			
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.
Customer: *Required to create process to identify both shared accounts and individuals utilizing such accounts.*			

5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: · Records of a procedure that passwords are changed when new devices are in production; or · Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
Customer: *Required to create procedure that mandates the changing of default passwords.*			
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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	Examples of evidence may include, but are not limited to: · System-generated reports or screen-shots of the system forced password parameters, including length and complexity; or · Attestations that include a reference to the documented procedures that were followed.
Customer: *Required to create procedure to mandate minimum password length and complexity requirements.*			

5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	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.	Examples of evidence may include, but are not limited to: · System-generated reports or screen-shots of the system forced periodicity of changing passwords; or · Attestations that include a reference to the documented procedures that were followed
Customer: *Create procedures to enforce password changes every 15 months at a minimum.*			
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: · Limit the number of unsuccessful authentication attempts; or · Generate alerts after a threshold of unsuccessful authentication attempts	Examples of evidence may include, but are not limited to: · Documentation of the account lockout parameters; or · Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.
Cisco Solution: *The Cisco Secure Identity Solution provides valuable audit information regarding network authentication, authorization, accountability and enforcement for incorporation into an organization overall audit and accountability policy and procedures. All components of this solution, including ISE, and network device produce valuable audit information to support the organizations audit and accountability policy and procedures. While each component provides logging information, each component also provides the ability to upload this information into an organizational auditing system via the syslog protocol*			

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

CXX-XXXXXX-XX 10/11