FORTRESS
Information Security

White Paper

NERC CIP COMPLIANCE

Updates, Enforcement and Practical Implementation

Date: 4/25/2019
http://www.fortressinfosec.com

Fortress Information Security, LLC
Email: sales@fortrssinfosec.com
Phone: 855.FORTRESS
189 S. Orange Ave., Orlando, FL 32801

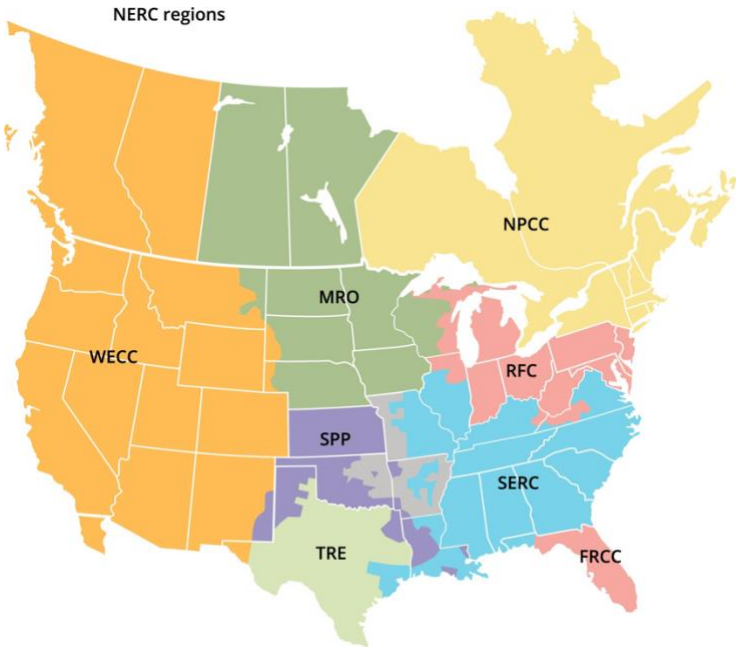
Introduction

The North American Electric Reliability Corporation (NERC) is a non-profit organization tasked by the Federal Energy Regulatory Commission (part of the US Department of Energy) with ensuring the reliability of the North American electric power grid. Among its tasks are drafting and auditing standards for cyber security of the systems that monitor and control the grid. This set of standards is known as NERC CIP (Critical Infrastructure Protection). Compliance with the NERC CIP Reliability Standards requires NERC entities to adopt precise procedures and to verify their implementation. This white paper describes recent CIP requirements updates and illustrates how a NERC entity can utilize technological solutions to save time and resources assessing and managing its compliance with the primary parts of CIP.

Important NERC CIP Concepts

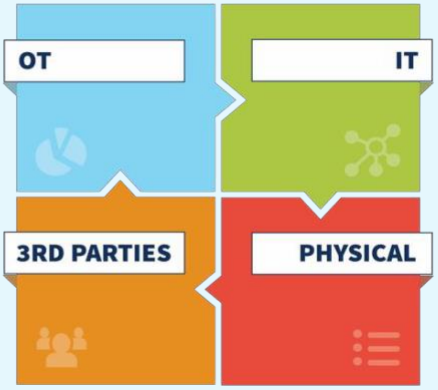
NERC – The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.

As illustrated above, FERC has oversight over NERC and its development and enforcement of reliability standards. In turn, RTOs support resiliency of members and cyber security advancement. The companies themselves are ultimately responsible for implementation of NERC CIP requirements. However, Fortress has observed that a company's IT and OT managers are not always on same page as to how to implement and comply with CIP requirements. This potential disconnect poses an important compliance challenge due to the interconnected IT/OT cyber, TPRM and physical asset ecosystem.



Interconnected IT/OT Cyber, TPRM & Physical Asset Ecosystem

- The stakes are even higher when these emerging risks converge.
- **The intersection of these areas:**
  - Drastically increases the attack surface
  - Where the biggest challenges, powerful transformations and boldest solutions emerge
- **The urgency stems from:**
  - increasing nation-state threats
  - and the societal consequences of failure
  - heightened regulatory pressures and compliance hurdles



NERC CIP Standards – The NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements (Standards) designed to secure the assets required for operating North America's bulk electric system. There are currently thirteen CIP standards either in effect, awaiting approval by FERC, or under development. These standards are numbered CIP-002 through CIP-014. See Appendix for more information about the standards and timelines associated with each.

Bulk Electric System (BES) – The North American power grid consists of a huge network of fixed assets linked by transmission lines. The primary types of assets include:

- Control centers , where trained and experienced operators monitor and control electric power flows, using many types of computer systems;
- Generating assets , including traditional nuclear, coal, natural gas and other power plants, as well as "renewable" power assets such as wind and solar farms and hydroelectric dams;
- Low-power renewable generating assets , primarily solar panels, installed at homes and businesses; and
- Substations, where devices like transformers and circuit breakers and control electric power flows, usually under the supervision and direction of a control center.

The BES is monitored and controlled by many types of computing systems. The NERC CIP standards were developed to secure these systems against cyberattacks, whether targeted (as in individual hacking attempts), broadcast (e.g. computer viruses and worms), or inadvertent (a user clicks on a phishing email that installs ransomware and renders his system unusable).

Cyber Asset – There are many types of systems that monitor and control the Bulk Electric System. Some of them are computers like those all of us are familiar with. Others are devices that look very different, and operate very differently, from "normal" computers. Since both

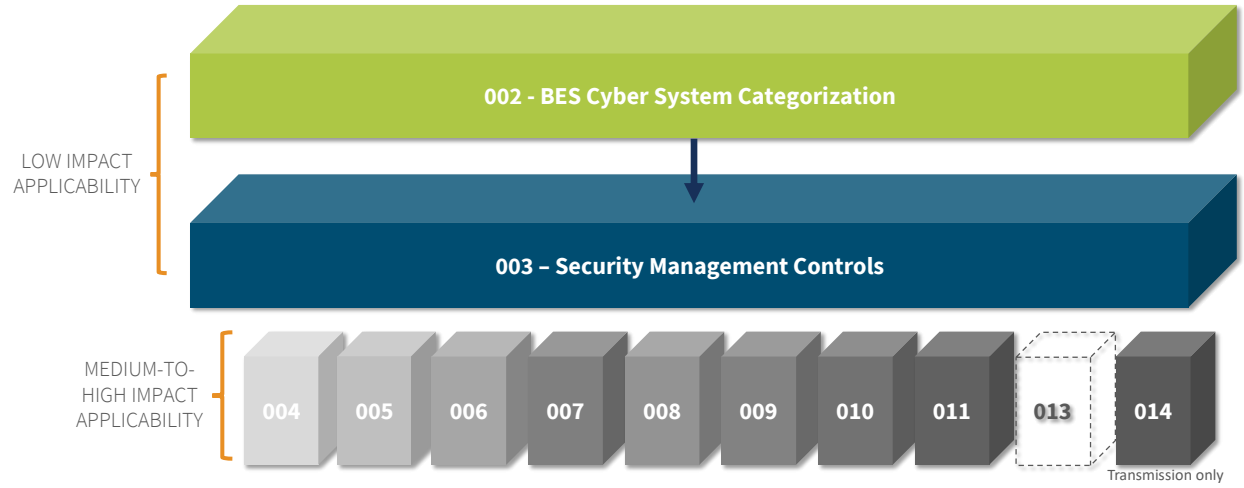
types of devices have roles in controlling the BES, the NERC CIP standards introduced the fundamental concept of a Cyber Asset, defined as a "programmable electronic device". This means an electronic device whose operation can be controlled through a program, which can be revised or replaced in some way.

BES Cyber System (BCS) – While there are many Cyber Assets involved in monitoring and controlling the BES, not all of these are in scope for NERC CIP. There is a subset of these Cyber Assets whose loss or mis-operation (perhaps under the control of a virus or a hacker) could cause an "impact" on the BES within 15 minutes. These are called BES Cyber Systems. Most of the requirements in the CIP standards apply to BES Cyber Systems, although these are divided into three groups based on their degree of impact on the BES: High, Medium and Low impact.

Applicability – All bulk power system owners, operators, and users must comply with NERC-approved Reliability Standards. These entities are required to register with NERC through the appropriate Regional Entity. All industry participants responsible for or intending to be responsible for, the following functions must register with NERC through the Organization Registration process.

	Entities that Must Register	Entities that Must be Certified
Reliability Coordinator (RC)	✓	✓
Transmission Operator (TOP)	✓	✓
Balancing Authority (BA)	✓	✓
Planning Authority (PA)	✓	
Transmission Planner (TP)	✓	
Transmission Service Provider (TSP)	✓	
Transmission Owner (TO)	✓	
Resource Planner (RP)	✓	
Distribution Provider (DP)	✓	
Generator Owner (GOP)	✓	
Reserve Sharing Group (RSG)	✓	
Frequency Response Sharing Group (FRSG)	✓	
Regulation Reserve Sharing Group	✓	

The following illustration shows which standards apply based on different levels of applicability.



Enforcement – NERC has authority to assess fines against non-compliant utilities in amounts up to $1,000,000 per violation and per day, retroactive to the effective date of the standard.

What Does NERC CIP Compliance Mean to Utilities?

Due to the increasing risk of power outages and vulnerabilities to our critical infrastructure federal regulators have tighten their monitoring of utility companies regardless of size. Therefore, utility companies must plan and budget resources to facilitate minimum NERC CIP compliance. The failure to conduct due diligence and due care in regards to NERC CIP compliance could lead to cascading vulnerabilities and risk throughout the industry. The non-compliance with mandatory NERC CIP standards will result in penalties and monetary fines.

NERC recently assessed a record $10 million fine for compliance failures at Duke Energy. The NERC filing, referring to an "unidentified registered entity," includes 127 violations of safety rules, such as a "configuration error" lasting six months that would have prevented system engineers from being alerted to a potential cyber security incident (i.e. hacking attempt), among numerous other violations. Given that such a major company with significant resources was in breach of NERC compliance — including "repeated failures to implement physical and cyber security protections" according to NERC — this raises the question of how well small- and medium-sized utilities are faring in their own compliance requirements. Further, all of this is happening against the backdrop of recent attempts by foreign adversaries who are known to be seeking ways to penetrate the defenses of utilities, according to the 2019 Worldwide Threat Assessment of the US Intelligence Community, released on January 29. Therefore, compliance with NERC and the protection of our nation's critical infrastructure from attack is more important than ever.

WHAT IS NERC COMPLIANCE ENFORCEMENT?

The process by which NERC issues sanctions and ensures mitigation of confirmed violations of mandatory NERC Reliability Standards.

Enforcement utilizes the following methods:

- **Directives:** NERC can also issue directives to immediately address and deter new or further violations, irrespective of their presence or status (i.e., confirmed or alleged).
- **Sanctions:** Sanctioning of confirmed violations is determined pursuant to the NERC Sanction Guidelines and is based heavily upon the Violation Risk Factors and Violation Severity Levels of the standards requirements violated and the violations' duration. NOTE: Entities found in violation of any standard must submit a mitigation plan for approval by NERC and, once approved, must execute this plan as submitted.
- **Fines:** NERC has authority to assess fines against non-compliant utilities in amounts up to $1,000,000 per violation and per day.

HIGHLIGHTS OF RECORDED NERC VIOLATIONS / FINES (2017-PRESENT)

NERC has authority to assess fines against non-compliant utilities in amounts up to $1,000,000 per violation and per day.

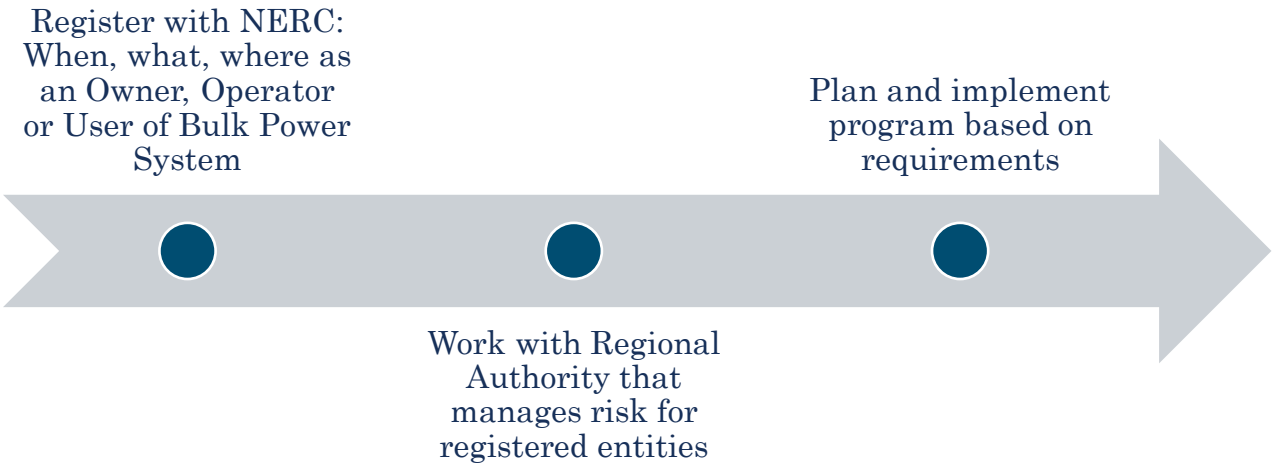
Year	2017	2018	2019
Assessed Fine	$1,721,000	$3,273,000	$10,000,000
CIP Standards Violated	CIP-02; CIP-03; CIP-04; CIP-05; CIP-06; CIP-07; CIP-08; CIP-09; CIP-10	CIP-03; CIP-05; CIP-07; CIP-10	CIP-03; CIP-04; CIP-05; CIP-06; CIP-07; CIP-14

The following table contains additional information about recent fines.

CIP-2: Identification and protection of Assets • Failure to identify assets and protect sensitive information regarding critical cyber assets. and allowed employees without proper	**CIP-003-3 Cyber Security Management Controls** **CIP-011-2 Information Protection** • Failure to safeguard "protected utility information" data from being publicly available online. • Failure of vendor to comply with electronic access controls
CIP-004-6 Personnel & Training • Failure to provide formal system operator training for its transmission operations center (TOC) staff and key employees.	**CIP-007-6 System Security Management** **CIP-010-3 Config Change Management and Vulnerability Assessments** • Failure to safeguard passwords for critical systems.

• Failure to perform background checks on employees before allowing access to networks and systems. • Failure to follow access control procedures for uncleared contractors, employees and former employees.	• Failure to implement password policy • Failure to implement patch management program • Failure to comply with change monitoring and remediation plans
CIP-006-6 Physical Security of BES Cyber Systems • Failure to maintain physical security perimeters of a six-wall border. • Failure to provide all the protections specified for cyber assets that authorize and log access to the physical security parameter. • Failure to provide continuous escorted access of visitors within the physical security perimeter.	**CIP-005-5 Electronic Security Perimeter(s)** • Failure to secure remote, computer access to some sensitive systems without requiring • No use of multi-factor authentication. • No encryption tools • Failure to properly configure network firewalls • No monitoring of traffic for malicious communications.

Practical Approaches to Achieve Compliance

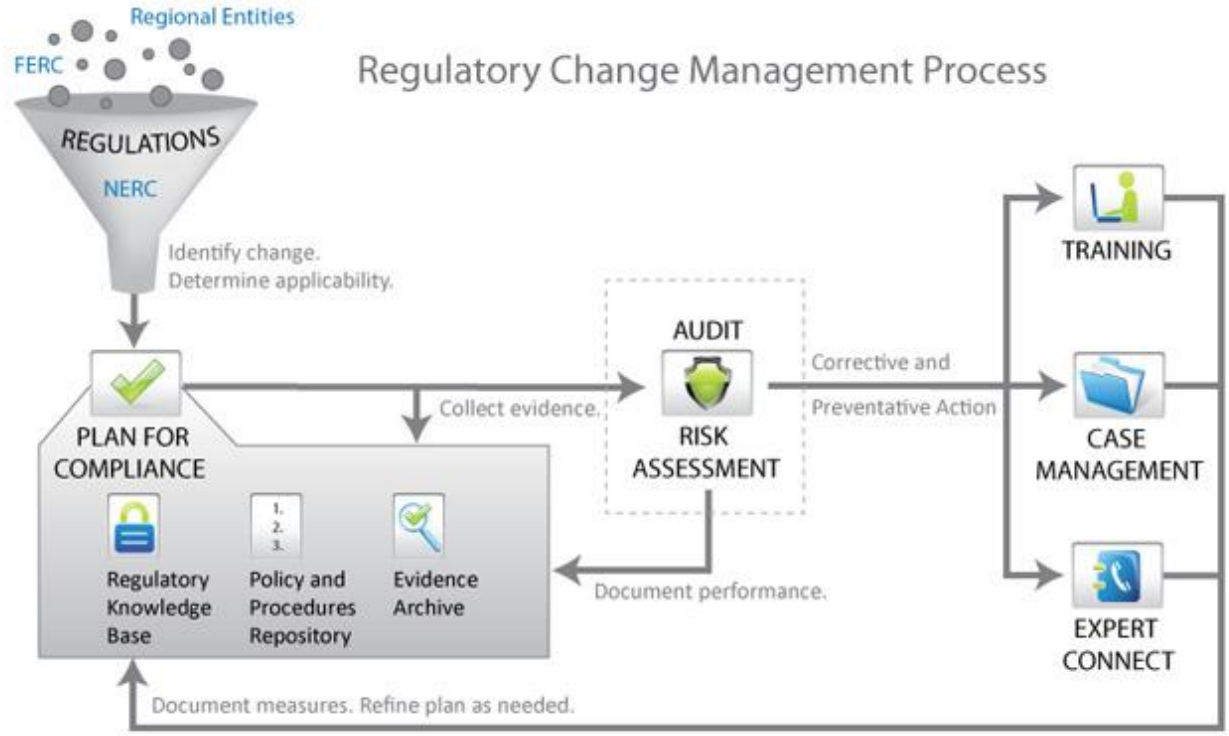


APPROACHES THAT HAVE PROVEN TO BE SUCCESSFUL

- Know what you have.
- Fail. A lot. Get better.
- The key is progress, forward movement. A Plan of Action and Milestones
  - Get HELP! (Partners, Consultants, NERC, anyone who will pick up the phone)
- Corrective Action Plans in a continuous improvement cycle
- Stay informed on changes to NERC standards. As the changes are promulgated, consider adopting the following analytical model:

- Identify and Determine Applicability
- Plan (Policy, Knowledge, and Procedures)
- Collect Evidence and documentation
- Conduct Internal Assessments and Audits
- Correct, Prevent and Monitor

The following diagram illustrates our recommended Regulatory Change Management Process.



UPCOMING NERC CHANGES

NERC CIP 13-01 (Effective, July 1, 2020)

CIP-013/Cybersecurity—supply chain risk management:

- Requires registered entities to develop documented C-SCRM plans to identify and assess risks related to vendor products, installing vendor products and software, and even transitioning from one vendor to another.
- In addition to having an overarching plan, the requirements also explicitly cover six key required process areas—but do not specify how to implement them.
- The six covered areas are vendor security incident notification, coordinated vendor incident response, vendor personnel termination notification, vendor vulnerability disclosures with respect to products and services, verification of vendor software integrity and authenticity, and coordination of vendor remote access controls.
- What's Different:
    - CIP-013-1 is the first CIP Standard that requires you to manage risk.
    - Compliance Requirements: You are required to develop (R1), implement (R2), and maintain (R3) a plan to manage supply chain cyber security risk. You should already be familiar with the needs of plan-based Standards, as many of the existing CIP Standards are
    - Development Requirements: Require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.

CIP 13-01 Standard Focus:

- Software integrity and authenticity;
- Vendor remote access protections;
- Information system planning; and
- Vendor risk management and procurement controls

CIP-005/Cybersecurity:

- Updated CIP-005/Cybersecurity—electronic security perimeters Standards:
    - Requirement for registered entities to comply with two new standards identifying active vendor remote access sessions and establishing methods to disable active vendor remote access sessions.

Updated CIP-010/Cybersecurity:

- Updated CIP-010/Cybersecurity—configuration change management and vulnerability assessments Standards:

- Requirement for entities to verify where its software originates as well as the integrity of the software it has obtained from its source. The intent is to make it increasingly difficult for attackers to take advantage of vendor patch and software distribution practice to introduce compromises into a system.

WHERE SHOULD YOU BE FOCUSING YOUR RESOURCES?

CIP-002-5.1a – BES Cyber System Categorization

The effective categorization of bulk-power system components according to how detrimentally the failure of a component or asset would affect the bulk-power system.

CIP-004-6 Personnel & Training

The training of personnel that work for, or have access to, the cyber systems of functional entities.

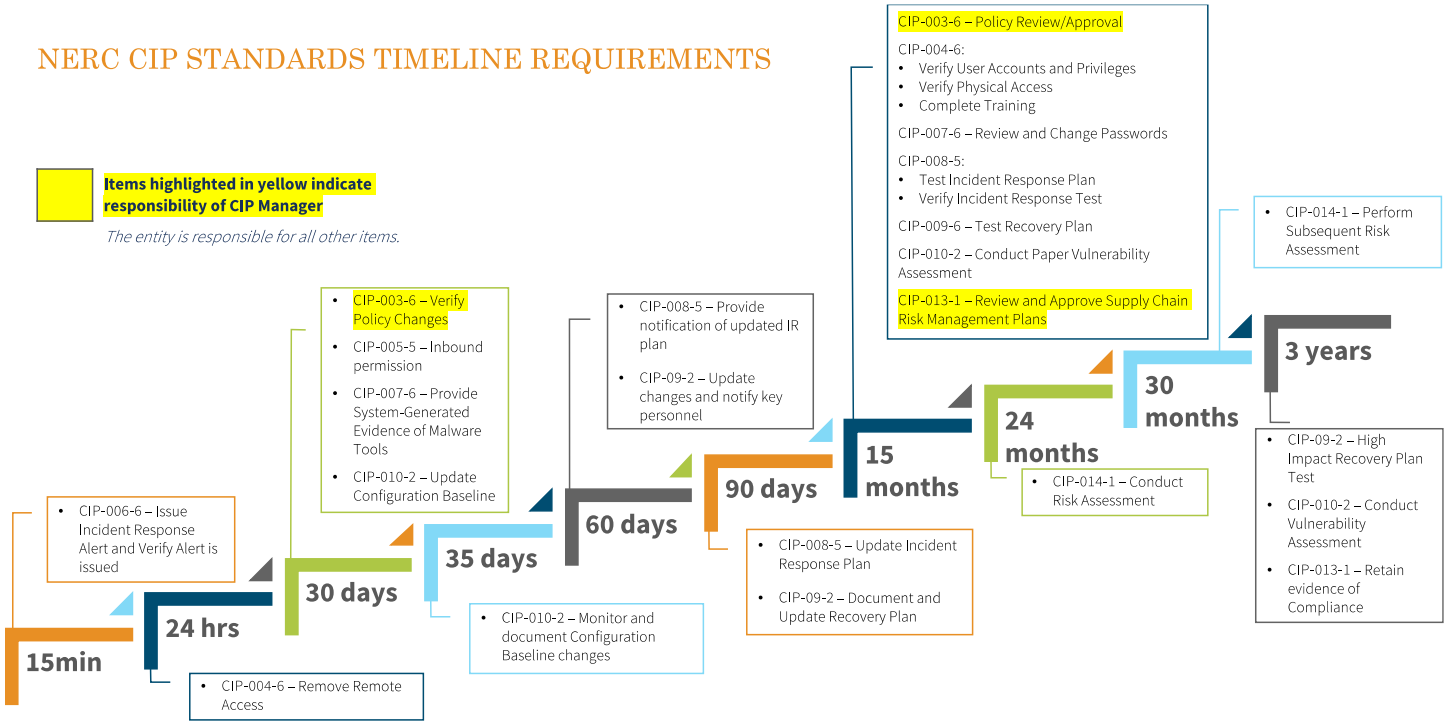
CIP-005-5 Electronic Security Perimeter(s)

The implementation of an electronic security perimeter to guard against cyber threats and external intrusion.

CIP-006-6 Physical Security of BES Cyber Systems

The requirements include policies meant to restrict access to physical assets, implement physical access controls, monitor unauthorized access, implement an alert system, continually monitor physical access controls, keep extensive logs of physical access, and maintain the physical access control systems over time.

NERC CIP STANDARDS TIMELINE REQUIREMENTS



CIP-011-2 Information Protection

The requirement for organizations to put procedure into place that enable them to identify BES Cyber System Information.

CIP-007-6 System Security Management
The creation and implementation of operational, technical, and procedural requirements for all entities covered by NERC regulations. In particular, CIP-007 covers things like how input and output ports are configured and can be accessed, the implementation of a patch management system, the use of malicious code detection software, and a variety of password requirements.

CIP-010-2 Configuration Change Management & Vulnerability Assessments
The Objective of CIP 10 is to ensure Change Management to prevent unauthorized modifications to Bulk Electric Systems (BES) Cyber Systems as well as Monitoring processes to detect unauthorized modifications to Bulk Electric Systems (BES) Cyber Systems and finally to conduct Vulnerability assessment to ensure proper implementation of cyber security controls and improve security posture of Bulk Electric Systems (BES) Cyber Systems

The Need for a Holistic Platform Management System

The best solution to these compliance challenges is a blend of **technology, analytics and services** – all of which can be leveraged by using a holistic platform management system that achieves all these outcomes (in other words, a "TOTAL" solution):

- Capture Cyber asset inventory and monitor configuration changes
- Standardize Access control for all physical, electronic and other critical assets
- Track and mitigate results from Vulnerability assessments
- Sustain Incident reporting and response requirements
- Remediation plans and reporting
- Manage and Controls changes and/or revisions on Policies and Procedures
- Maintain and track recurring training needs and gaps
- Facilitate approval, review and submission processes

The Fortress Total Solution

The Fortress Total Solution is the blueprint for a safe digital transformation and NERC compliance in a world of the "Small City" Integrated Asset Ecosystem and emerging cyber risks

THE KEY VALUE IS AN INTEGRATED APPROACH:

Holistic approach across organizational and technology silos

A single source of truth and unified view of risk and compliance challenges

All tied directly to your business impacts and strategic decision making

WHY FORTRESS?

Fortress is the #1 choice for **NERC-registered,** generation entities

Trusted Partner

- To **10%** of US power generation
- Managing over 300,000 BES and non-BES assets
- Over 40,000 vendors monitored

Operations Friendly

- CapEx versus O&M structures
- **Reverse cost** with assessment library
- Concierge-style services

The Right Platform

- Bridge vendor and IT/OT/IoT/IIoT risk management
- Eliminate waste through analytics
- Integrate existing tools and unlock value

HOW QUICKLY ARE TYPICAL PROGRAMS STOOD-UP?

WHAT ARE THE OUTCOMES WITH OUR PARTNERSHIP?

300% Faster Program Maturity

100% More Vendor & Asset Coverage In The Same Time Period

30-45 Days To Implement

40% Effort Reduction Through Automation

MORE ABOUT FORTRESS

Fortress Information Security helps companies stop emerging cyber threats that pose the biggest risk to their business. Our clients benefit from a unique "Technology, Analytics and Services" (TAS) approach to protecting their connected assets. Fortress has deep, combined expertise in both cyber security and specific industry sectors – like manufacturing, finance and energy – to provide solutions that specifically tie into the business processes of our clients. The centerpiece of our technology, the Fortress Platform, gives clients a "single source of truth" on emerging risk.

The Fortress Platform derives its power from a unique bundling of innovative technology, human analysts and managed services designed to help both large and small companies wherever they are in their cyber risk management journey. The Fortress Platform leverages automation, alerting, escalation and a variety of other advanced functions – with service levels assigned whenever appropriate to ensure and measure execution and compliance. Unlike siloed point tools that only look at one part of the problem, we take a holistic view of risks across our clients' entire digital ecosystem of IT, operational technology (OT), third parties and the extended supply chain to better prioritize and unlock value of existing technology investments.

By leveraging everything from risk assessments and security scoring models, to continuous monitoring of third parties and system reviews from elite analyst teams, Fortress connects traditionally disparate sources of information to help clients uncover not just emerging cyber risks, but every ripple of business impact that flows from those risks. Fortress delivers all our clients need to enable their process and be on path to security and excellence and regulatory compliance within 60 days – a fraction of the time it would take the enterprise to learn about, compare, select and purchase new tools.

Our NERC Foundations Solutions are tailored to address all CIP standards:

Foundations	**CIP 002—BES Cyber System Categorization** · Identify and Certify BES Assets · Impact Ratings	**CIP 003—Security Management Controls** · Security Awareness · Physical · Electronic Access · CSIRT	**CIP 004—Personnel & Training** · Security Awareness · Identity Confirmation · Min. Access	
Cyber Security Protection	**CIP 005—Electronic Security Perimeter** · Perimeter Isolation · Remote Access · Monitoring	**CIP 007—System Security Management** · Network Access · Patch Management · Malware Prevention · Event Monitoring · Access Control	**CIP 010—Config. Change Mgmt. and Vuln. Assessments** · Configuration Baseline · Change Monitoring · Vuln. Assessments	
Incident Response	**CIP 008—Incident Reporting & Response Planning** · Processes to Identify, Classify & Respond · Incident Response Group Roles		**CIP 009—Recovery Plans for BES Cyber Systems** · Conditions for Activation of Recovery Plans · Responder Responsibilities	
Physical and Supply Chain	**CIP 006—Physical Security BES Cyber Systems** · Define Controls · Monitor access · Controls for Authorized, Unescorted Physical Access · Alert System	**CIP 011—Information Protection** · Identify BES Cyber System Information · Procedures to Protect Information Storage, Transit & Use	**CIP 013—Supply Chain Risk Management** · Vendor Risk Mgmt. Plans · Remote Access · Software Integrity · Known Vulns · Security Incidents & Exposures	**CIP 014—Physical Security** · Risk Assessments of Transmission Stations · Third Party Verification · Threats & Vuln Analysis

Appendix

Requirement	Evidence Requirements Timeline	Reference Summary
CIP-003-6	**Policy Review/Approval EVERY 15 Calendar months.**	• High impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies. • Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months.
CIP-003-6	**Verify Policy Changes within 30 Days of the Change**	• Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of Change.
CIP-004-6	Verify User Accounts and Privileges **EVERY 15 months.**	For each BES Cyber System, EACMS, and PACS Provide: • Evidence that the authorization records for each enabled user of each Cyber Asset of the BES Cyber System, EACMS, or PACS match the actual implemented permissions. • Evidence that evaluations of authorization records against actual account privileges were performed at least once every 15 calendar months for the audit period.
CIP-004-6	Verify Physical Access **EVERY 15 months.**	For each BCSI storage location provide: • Evidence that the authorization records for each individual with access, either electronic or physical, to the BCSI storage location match the actual implemented permissions. • Evidence that evaluations of authorization records against actual privileges were performed at least once every 15 calendar months for the audit period.
CIP-004-6	Remove Remote Access **Within 24 Hours of Termination**	• Provide evidence of removal of remote access to system within 24 hours of termination
CIP-004-6	Complete Training once **Every 15 months.**	• Require completion of training at least once every 15 calendar months.
CIP-005-5	Inbound permission with in **30 Days of request**	• Provide evidence of inbound and outbound access permissions (generated no more than 30 days prior to the date of this request), including the reason for granting access for each permission.
CIP-006-6	Issue Incident Response **Alert within 15 Mins of Detection.**	• 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.
CIP-006-6	Issue Incident Response Alert **within 15 Mins of Detection.**	• Verify the Responsible Entity has documented one or more physical security plans to 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.
CIP-006-6	Verify Incident Response Alert is issued **within 15 Mins of Detection**	• Verify that an alarm or alert is issued 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 detection.
CIP-007-6	Provide System Genate Evidence of **Malware Tools within 30 Days**	• For each Cyber Asset, provide system-generated evidence (generated no more than 30 days prior to the date of this request) demonstrating that malware deterrent, detection or prevention tools are deployed.

CIP-007-6	Review and Change **Passwords EVERY 15 months**	For each Cyber Asset, provide the following evidence: 1. The type of authentication used for interactive user access (e.g., username/password, two factor with password and token, etc. 2. For interactive user access which uses password-only authentication, provide evidence of how password changes at least once every 15 calendar months are enforced (i.e., technical or procedural). 3. For password changes enforced by technical means, provide evidence that the Cyber Asset requires a password change at least once every 15 calendar months. 4. For password changes enforced by procedural means, provide evidence of the applicable procedure. 5. Provide evidence that passwords for all accounts have been changed within the preceding 15 calendar months. 6. For accounts whose password has not been changed in the previous 15 calendar months, provide evidence of an approved TFE for this device.
CIP-008-5	Test Incident Response Plan **EVERY 15 months.**	• Test each Cyber Security Incident response plan(s) at least once every 15 calendar months
CIP-008-5	Verify Incident Response **Test EVERY 15 months.**	• Verify the Responsible Entity has tested each Cyber Security Incident response plan(s) at least once every 15 calendar months
CIP-008-5	Update Incident Response Plan **within 90 Days**	• No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response document, update or notify agencies on results.
CIP-008-5	Provide notification of updated **NLT 60 days after changes to IR Plan.**	• No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan
CIP-009-6	Test Recovery Plan **EVERY 15 months.**	• Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months
CIP-09-2	High Impact Recovery Plan Test **EVERY 36 months.**	• High Impact must test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.
CIP-09-2	Document and Update Recovery Plan **EVERY 90 days.**	• No later than 90 calendar days after completion of a recovery plan test or actual recovery document lessons learned and update plans.
CIP-09-2	Update changes and notify key personnel **within 60 days of making changes.**	• No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan document changes and notify key personnel of changes.
CIP-010-2	Update Configuration Baseline **within 30 days of change.**	• For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.
CIP-010-2	Monitor and document changes **EVERY 35 days.**	• Monitor at least once every 35 calendar days for changes to the baseline configuration
CIP-010-2	Conduct Paper Vulnerability Assessment **Once EVERY 15 calendar months.**	• At least once every 15 calendar months, conduct a paper or active vulnerability assessment.
CIP-010-2	Conduct Vulnerability Assessment **Once EVERY 36 calendar months.**	Where technically feasible, at least once every 36 calendar months: • 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
CIP-011-2	Identify and Verify Information Protection Programs.	• Identify and verify the Responsible Entity has documented one or more information protection programs that have method(s) to identify information that meets the definition of BES Cyber System Information.
CIP-013-1	Review and Approve Supply Chain Risk Management Plans Once **EVERY 15 calendar months.**	• Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months
CIP-013-1	Retain evidence of Compliance for **3 calendar years.**	• Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years
CIP-014-1	Conduct Risk Assessment **within 24 months of initial service**	• Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months)
CIP-014-1	Perform Subsequent Risk Assessment **within 30 calendar months** of previous assessment.	• Subsequent risk assessments shall be performed at least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection;