NERC CIP Version 5

A Roadmap To Compliance

PATHMAKER GROUP

Table of Contents

Overview

The North American Electric Reliability Corp. Critical Infrastructure Protection (NERC CIP) standards Version 5 establishes extensive change to previous scope and requirements.

These complex standards and supplemental guidelines are defined in over 300 pages of documentation. While the Federal Energy Regulatory Commission (FERC) approved the CIP 5 standards, NERC maintains development and oversight authority.

The new risk based rating system, which categorizes bulk electric systems (BES) into High, Medium, and Low impact tiers, effectively results in all cyber assets that could impact BES facilities being brought into scope. Most North American energy producers and distributors previously exempt now need to comply with stringent NERC CIP 5 standards.

Entities determined to be Critical Assets are now responsible for security measures in four broad areas: Security Awareness, Physical Security, Remote Access Connections, and Incident Response.

CIP 5 covers 11 reliability standards covering various aspects of cyber security in the critical energy infrastructure, including establishing programs for managing access to cyber assets, documenting which personnel are authorized to access cyber assets, and creating plans and processes for electronic and physical security of assets, among other things.

Identity and access management is a critical component of the standards, because it allows organizations to carefully monitor and control access to assets that may be vulnerable to cyber attacks.

NERC CIP Version 5 Standards

CIP-002: BES Cyber System Asset Identification

Cyber Assets associated with the Critical Assets that support the reliable operation of the BES.

REQUIREMENTS:

1. Incorporates the "Bright Line Criteria" to classify BES Assets as Low, Medium, or High.
2. BES Cyber System Lists must be reviewed and approved every 15 calendar months.

CRITICAL SECURITY CONTROLS:

Control 1: Inventory of Authorized and Unauthorized Devices
Control 2: Inventory of Authorized and Unauthorized Software
Control 4: Continuous Vulnerability Assessment and Remediation

CIP-003: Security Management Controls

Requires Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

REQUIREMENTS:

1. Cyber Security Policies approved for Medium and High Impact BES Cyber Systems by CIP Senior Manager every 15 calendar months.
2. Cyber Security Policies approved for Low Impact Assets by CIP Senior Manager every 15 Calendar Months. Cyber Security Policies for low impact assets must include Cyber Security Awareness, Physical Security Controls, Electronic Access Controls for external routable protocol connections and dial-up connectivity and incident response to Cyber Security Incident.
3. Identify a CIP Senior Manager and document any change within 30 calendar days of the change.
4. CIP Senior Manager must document any delegates.

CRITICAL SECURITY CONTROLS:

Control 2: Continuous Vulnerability Assessment and Remediation (All Impact Tiers)
Control 3: Secure Configurations for hardware and software on mobile devices, laptops, workstations, and servers (High and Medium Impact)
Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (All Impact Tiers)
Control 13: Boundary Defense (Low Impact)
Control 15: Controlled Access based on need to know (All Impact Tiers)
Control 18: Incident Response and Management (All Impact Tiers)

NERC CIP VERSION 5 STANDARDS

CIP-004: Personnel and Training

Requires personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

REQUIREMENTS:
1. Security Awareness Program
2. Training Program
3. Personnel Risk Assessment Program
4. Access Management Program
5. Access Revocation Program

CRITICAL SECURITY CONTROLS:
Control 9: Security Skills Assessment and appropriate training to fill gaps.
Control 15: Controlled Access based on need to know

CIP-005: Electronic Security Perimeters

Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, including perimeter access points.

REQUIREMENTS:
1. Electronic Security Perimeters
2. Interactive Remote Access Management

CRITICAL SECURITY CONTROLS:
Control 9: Security Skills Assessment and appropriate training to fill gaps
Control 13: Boundary Defense
Control 14: Maintenance, Monitoring and Analysis of Audit Logs
Control 15: Controlled Access based on need to know

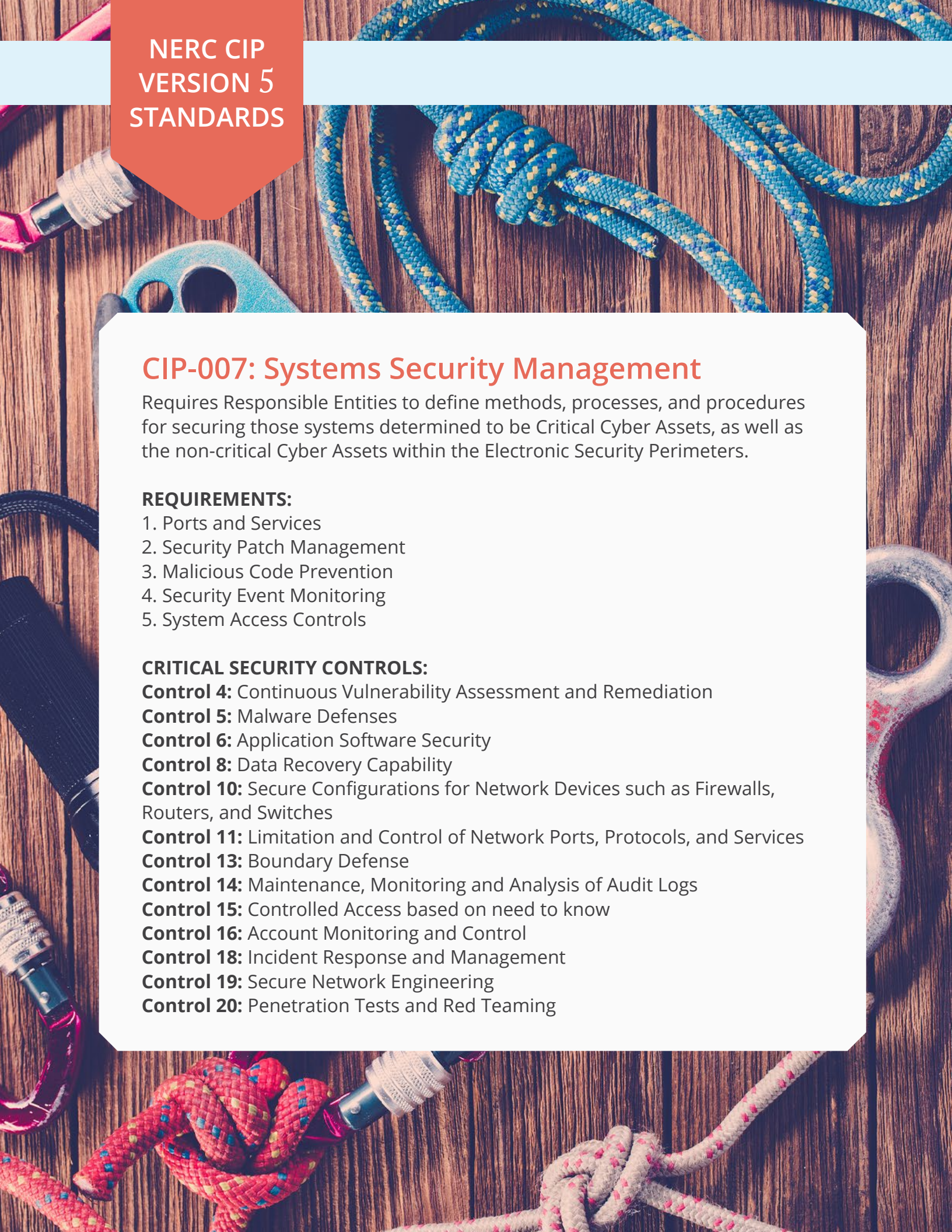
CIP-006: Physical Security of BES Cyber Systems

Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

REQUIREMENTS:
1. Physical Security Plan
2. Visitor Control Plan
3. Maintenance and Testing Program

CRITICAL SECURITY CONTROLS:
Control 9: Security Skills Assessment and appropriate training to fill gaps
Control 13: Boundary Defense
Control 14: Maintenance, Monitoring and Analysis of Audit Logs
Control 15: Controlled Access based on need to know

NERC CIP VERSION 5 STANDARDS



CIP-007: 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 non-critical Cyber Assets within the Electronic Security Perimeters.

REQUIREMENTS:

1. Ports and Services
2. Security Patch Management
3. Malicious Code Prevention
4. Security Event Monitoring
5. System Access Controls

CRITICAL SECURITY CONTROLS:

Control 4: Continuous Vulnerability Assessment and Remediation
Control 5: Malware Defenses
Control 6: Application Software Security
Control 8: Data Recovery Capability
Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Control 11: Limitation and Control of Network Ports, Protocols, and Services
Control 13: Boundary Defense
Control 14: Maintenance, Monitoring and Analysis of Audit Logs
Control 15: Controlled Access based on need to know
Control 16: Account Monitoring and Control
Control 18: Incident Response and Management
Control 19: Secure Network Engineering
Control 20: Penetration Tests and Red Teaming

NERC CIP VERSION 5 STANDARDS

CIP-008: Incident Reporting and Response Planning

Ensure the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

REQUIREMENTS:

1. Cyber Security Incident Response Plan.
2. Implementation and testing of Cyber Security Incident Response Plans.
3. Cyber Security Incident Response Plan Review, Update and Communication.

CRITICAL SECURITY CONTROLS:

Control 18: Incident Response and Management

CIP-009: Recovery Plans for Critical Cyber Assets

Ensures that recovery plans are implemented for Critical Cyber Assets and plans follow established business continuity and disaster recover techniques and practices.

REQUIREMENTS:

Recovery Plan review, update and communication.

CRITICAL SECURITY CONTROLS:

Control 1: Inventory of Authorized and Unauthorized Devices
Control 2: Inventory of Authorized and Unauthorized Software
Control 8: Data Recovery Capability
Control 17: Data Loss Prevention
Control 18: Incident Control and Management

Refer to CIP Reliability Standards for comprehensive explanation of requirements.

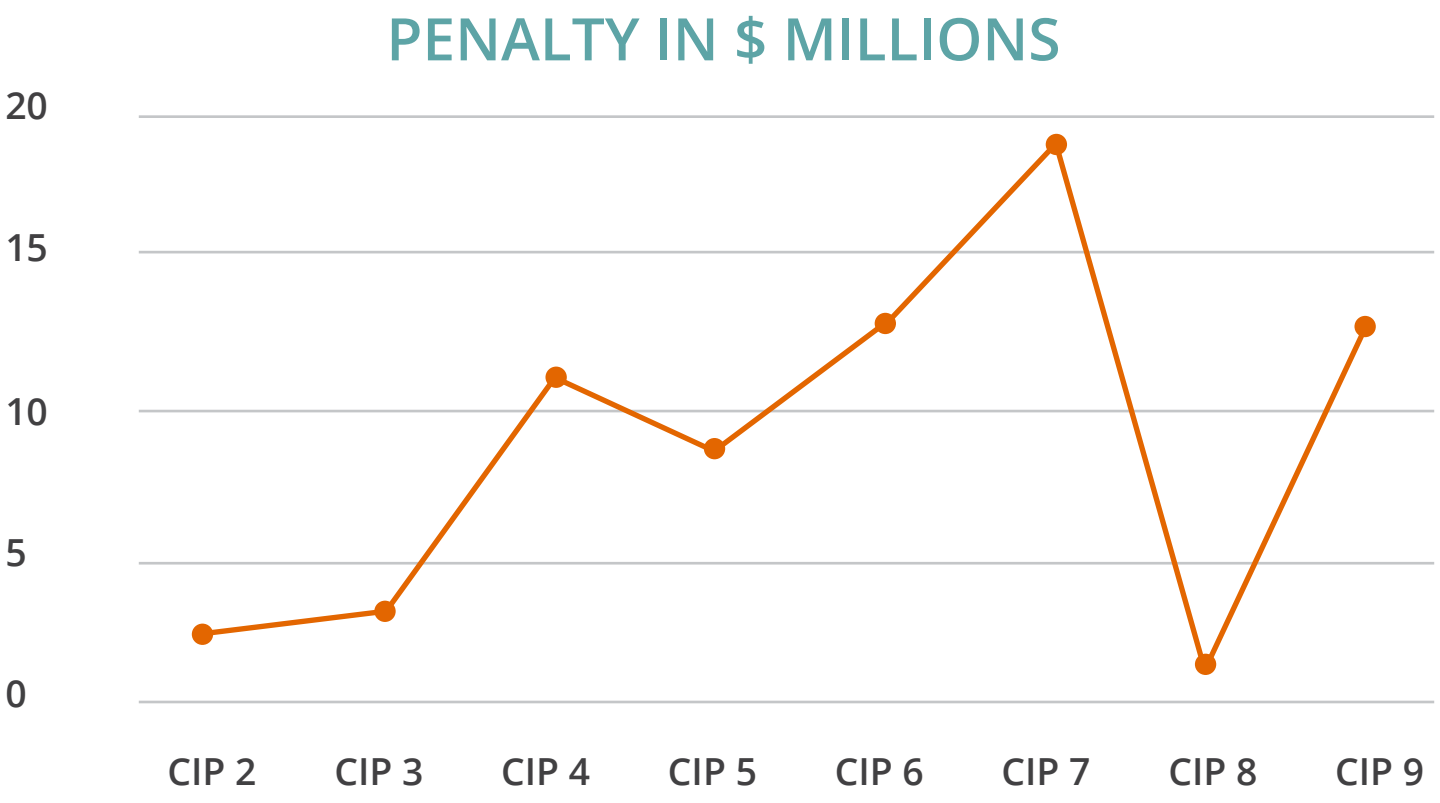
CIP 5 Violations and Trends

Firm policy enforcement is proving costly for energy companies. Penalty trends indicate top tier fines of $1.7M comprise majority of assessments.

CIP 5 enforcement began July 1, 2016

$68.4M in aggregate penalty dollars have been assessed YTD

Violations for 2016 are costly and expected to grow



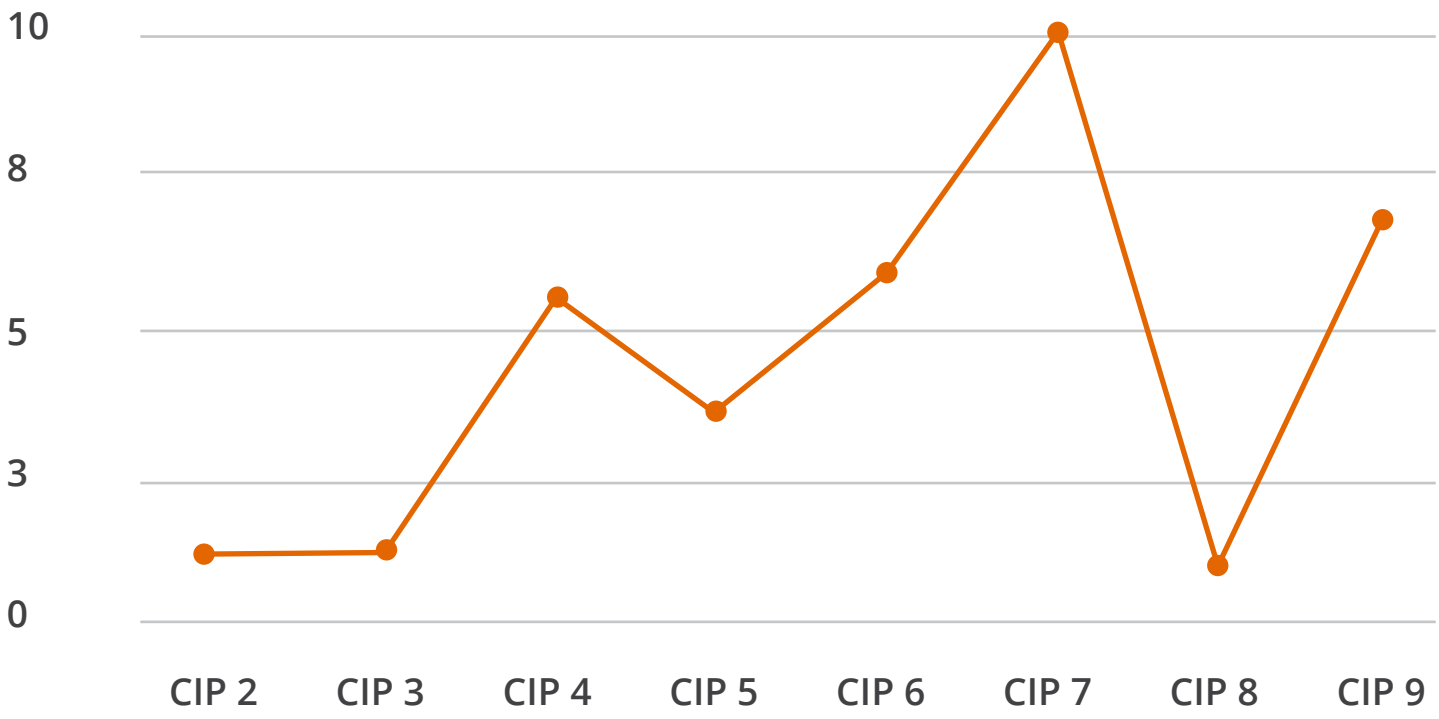
TRENDS

CIP 4, 5, 6, 7, and 9 comprise 85% of the number of violations.

Of the $68.4M in penalty dollars assessed $61.2M was in the maximum penalty tier of $1.7M assessment.

These same standards are responsible for 91.2% of the total penalty dollars assessed for violations.

NUMBER OF $1.7M MAXIMUM PENALTIES

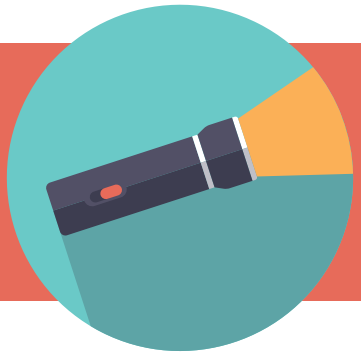


Future Enforcement Dates

OCTOBER 1, 2016
CIP-004-6 Requirement 4.2.

APRIL 1, 2017
CIP-003-5 Requirement 2.2.
CIP-003-5 Requirement 2.3.
CIP-003-5 Requirement 2.4.
CIP-003-6 Requirement 1.2.
CIP-003-6 Requirement 1.2.1
CIP-003-6 Requirement 1.2.2
CIP-003-6 Requirement 1.2.3
CIP-003-6 Requirement 1.2.4
CIP-003-6 Requirement 2

JULY 1, 2017
CIP-004-6 Requirement 2.3.
CIP-004-6 Requirement 4.3.
CIP-004-6 Requirement 4.4.
CIP-006-6 Requirement 3.1.
CIP-008-5 Requirement 2.1.
CIP-009-6 Requirement 2.1.
CIP-009-6 Requirement 2.2.
CIP-009-6 Requirement 2.3.



Common IAM Gaps

Weak Program Management

Successful IAM programs get sustained support from the top. We commonly see short-term or limited allocation of support and funding to achieve progress toward a specific, tactical problem. Sooner or later, support wains and the long-term strategic success of the IAM program is jeopardized.

Experienced Partners

IAM technical skills are in high demand and finding these resources is difficult. Successful organizations depend on experienced partners who possess the skills and expertise to handle any IAM need. Outside resources are key to bridging this gap.

No Long-Term Vision

Painting a long-term vision enables an organization to build a strategic IAM program. Many organizations have leveraged specific IAM capabilities in a way that limits long-term progress. Designing the program based on a long-term vision and prioritizing the right order for foundational capabilities, helps avoid future technical roadblocks.

Lack of Data Classification

Not understanding how important/valuable each data attribute is to your business prevents you from successfully designing appropriate protections. Understanding the value of your critical data will allow you to place a risk score and dollar value on the data to help with a cost vs. loss analysis when determining budgets.

Lack of Control over Privileged Accounts

Insufficient controls around the special requirements of powerful admin and systems accounts within the IT infrastructure of an enterprise exposes critical infrastructure to the most common means that hackers use to breach systems. Controlling the passwords and access rights for these critical accounts and auditing all of their activities allows for much tighter control of your important resources.

Limited Adoption of Key IAM Capabilities

Many companies haven't fully rolled out some of today's basic Identity and Access Management functions that are part of the products they have already purchased. Not fully deploying many easily adopted functions such as single sign-on, multi-factor authentication and step-up authentication means that companies are missing basic approaches to increasing security for their application portfolios.

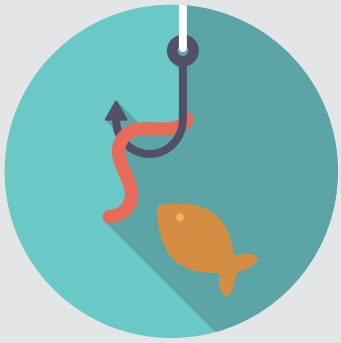
Energy Industry Pain Points

24-Hour Terminations Window

It is critical to have controls in place to ensure that physical and logical access is disabled within 24 hours of a user being terminated. Dormant accounts are a key vulnerability that can enable cybersecurity attacks.

24-Hour Recertification Window for on the Job Changes

When users change job responsibilities, prior access should be reviewed within 24 hours and removed if it is no longer needed for the new job responsibilities. Accrued access for long-time employees increases the risk of internal and external cybersecurity attacks using their credentials.



Enforced Approval Chain

The granting of access to NERC CIP assets requires that a specific approval chain is enforced many times by multiple approvers at different levels. This ensures that resource owners and managers are in control of the access granted to critical resources.

Physical and Logical Access

The inclusion of both physical and logical access in the NERC CIP controls is vital to properly protecting critical assets. Badge systems that control access to physical doors in key facilities and logical access granted via accounts in key systems and applications are important components of NERC CIP.

Auditing and Reporting

The ability to review audit records and generate reports on all activities surrounding physical and logical access is mandatory in proving that the appropriate controls are in place for protecting NERC CIP assets. Being able to show who was granted access to which resources during specific timeframes and trigger events is a must.

Background Checks (Personnel Risk Assessments)

Different levels of resources require varying degrees of background checks as a control to ensure risky individuals are not granted access to critical resources. The need to track background checks and use that information in the approval and authorization process is key.

Control Center / Corporate Network Air Gap

The need to separate the corporate network from the control center network is a fundamental requirement to prevent cybersecurity attacks on control center assets. This separation usually makes it harder to apply the same physical and logical access controls to resources in each network, but maintaining consistent controls across both “domains” is critical.

Training Checks

Industry-specific training is mandatory as a control to ensure individuals with access to NERC CIP assets are knowledgeable in following proper procedures pertaining to the use of those assets. The need to track training completion and use that information in the approval and authorization process is key.

How Do I Fix it?

Our unique IAM Maturity Advisory Program (MAP) measures 80 critical data points to show gaps against energy industry best practice.

The IAM MAP is a brief, value packed process that provides a comprehensive orientation to all the ways you can improve your security posture and plan for NERC CIP compliance. It is entirely focused on your people, process, environment and technologies.

As a process it is a NERC CIP expert led management level workshop utilizing a methodology called the Eight Levers of IAM Maturity. This is supported by an online performance benchmarking tool. You will come away with your big questions answered and an action plan tailored to your NERC CIP compliance needs.

At the strategic level, we will identify your gaps and prioritize closing actions. At the tactical level we will review immediate actions to drive short term compliance improvements over the next three to six months.

WORKSHOP DAY: PART ONE

Where we are now and what we will build on

In a room (or remote web conferencing session if you prefer) equipped with all the workshop logistics and online access, we'll begin an in-depth knowledge sharing session about the Eight Levers of IAM Maturity, so you can put them into strategic context for your business. This foundation enables you to extract greater value from the workshop, and embeds IAM maturity knowledge into the process going forward.

Then we'll gather around the Eight Levers of IAM Maturity online benchmark and progressively work our way through 80 measures, ranking your firm from poor to best practice. The questions are answered by you, but under our expert guidance and moderation. At the end of this section, you and your team will have a common and thorough understanding of the strengths and weaknesses in your IAM program.

WORKSHOP DAY: PART TWO

What's possible and how to get there

Armed with a comprehensive understanding of your objectives, current state and gaps, we can now model the future against your key goals. In this section we do scenario modeling to determine what you want your future to look like.

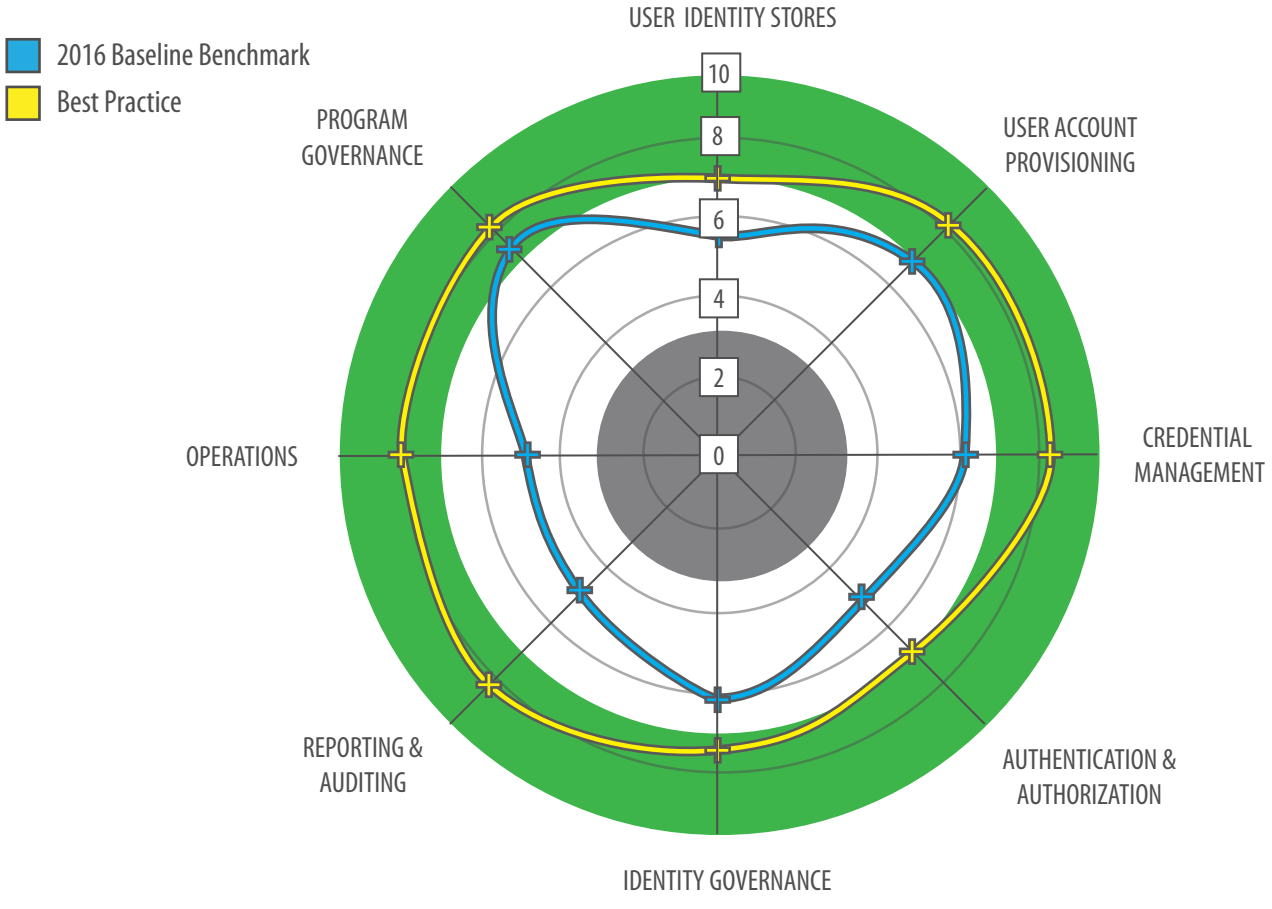
We'll factor in all of the outputs from the process so far and plan the most important next steps. We will offer guidance and recommendations on how moving forward with the next priorities can be achieved with synergy and maximum impact to your overall IAM maturity.

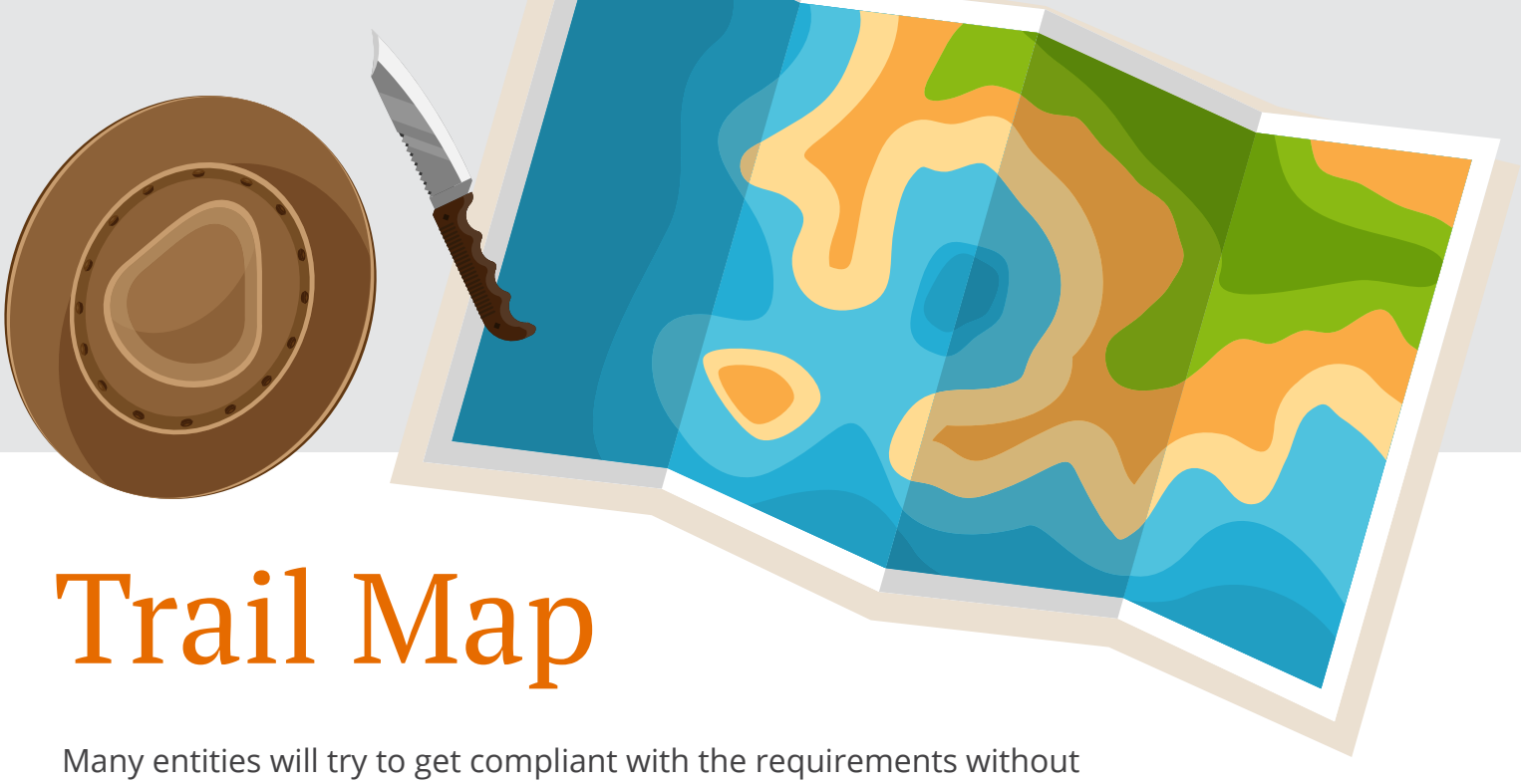
At a strategic level, we'll identify gaps and prioritize maturity improvement actions. At a tactical level, we'll look at the most immediate actions to drive short term improvements in the next three to six months.

POST WORKSHOP:

Taking action

Within a week we'll produce a summary presentation of our recommendations and provide you with any additional materials, tools or templates we think will be helpful to you. You'll also receive an implementation plan which prioritizes the sequence of events, in priority order, at a detailed level. You'll retain access to the online benchmark so you can remodel the value of your IAM program at any time and as often as you like. Our clients use this as their scorecard and progressively push maturity up by increasing their score across the Eight Levers and 80 Measures.





Trail Map

Many entities will try to get compliant with the requirements without the assistance of experienced consultants who are familiar with CIP v5 requirements.

This is one of the primary reasons …

The importance of the implementation requirement cannot be ignored. Simply creating policies will not be sufficient for compliance. Policies must be implemented through the deployment of processes, procedures, and controls that meet the objectives described in the written policies.

The concern over cybersecurity risks to critical infrastructure, of which power generation is a significant element, is unlikely to wane in the foreseeable future. In fact, the issue is receiving increasing scrutiny from the federal government and, recently, state utility commissions and legislatures. The expectation that critical infrastructure operators will proactively and effectively address cyber risks is increasing.

Additionally, with respect to the NERC CIP standards, there is an active effort to shift the focus of audit and enforcement away from a strict measurement against specific requirements toward a qualitative assessment of internal controls. This move will reinforce the need for holistic approaches that emphasize real security rather than mere compliance.

Compliance requirements can be an effective catalyst to kickstart cybersecurity efforts, but if they remain the only focus, long-term success is unlikely. Holistic efforts that view cybersecurity as a means to compliance, rather than assuming compliance is the basis for security, are the only effective way to address both concerns now and into the future.

Get In Touch

Contact us to learn more about the NERC / CIP Compliance Journey.

WHO WE ARE

Pathmaker Group is a specialized Security and Identity Management Consultancy, blending core technical and product expertise, consultative know-how, and extensive implementation experience.

WHAT WE DO

We provide complete solutions by merging software, hardware, managed service solutions, professional services, and customized training. We work to leverage your investments by integrating new solutions with your current products.

HOW WE DO IT

Our high-quality, formalized methodologies, grounded in PMI project management principles, have been refined through practical application and have gleaned best -practices from dozens of multi-million dollar projects.

www.pathmaker-group.com
info@pathmaker-group.com
(817) 704-3644