



ACHIEVING NERC CIP COMPLIANCE THROUGH IAM

A Roadmap to Compliance

Whitepaper



Table of Contents

Introduction

CIP-002-5.1a Critical cyber Asset Identification

CIP-003-8 Security Management Controls

CIP-004-6 Personnel and Training

CIP-005-6 Electronic Security Perimeters

CIP-007-6 Systems Security Management

CIP-008-6 Incident Reporting and Response Planning

CIP-009-6 Recovery Plans for Critical Cyber Assets

CIP-010-3 Configuration Change Management and
Vulnerability Assessments

CIP-012-1 – Communications between Control Centers

Conclusion

Introduction

Everyone needs electricity, and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is an attempt to make sure everyone gets it. Cybersecurity for this industry is of particular importance due to the nature of energy production.

Without power, computers have no “cyber” to secure. What’s more, power disruptions can produce staggering economic losses. A mere 6-hour blackout in France could cost an estimated 1.5 billion euros.

Protecting North America’s Bulk Electric System (BES) is considered a matter of the public welfare due to the number of crucial societal functions reliant upon the mammoth feat of engineering that is the electrical grid.

For this reason, the CIP regulations are mandatory within the US, with hefty penalties reserved for violators. Maximum fines for NERC violations can be as high as \$1,000,000 per day per violation. With such heavy costs on the line, investing in a NERC CIP compliance solution must be a top priority for energy producers.

Identity and Access Management (IAM) should be at the top of your list of considerations for tackling the challenge of NERC CIP compliance. While a standard compliance service will only focus on satisfying the dictates of the regulations, a managed IAM service looks to improve your whole identity fabric in the course of meeting compliance.

Consider the key criteria of NERC CIP and how IAM works to achieve each one.

CIP-002-5.1a Critical Cyber Asset Identification

Overview – Under this regulation, enterprises must identify the critical assets that could significantly damage the BES if their cybersecurity was compromised. These assets must be categorized into a comprehensive list of other potential at-risk assets. Once identified, these assets must be secured through appropriate safeguards and controls capable of mitigating disruptions to their performance.

How IAM Helps – An identity assessment identifies all aspects of your identity program which could be improved. An assessment by a skilled provider fulfills the need for an itemized list of potential risks, as well as advising on how best to plug up those gaps.

Additionally, an identity orchestration platform can institute those fixes and maintain safeguards. These include active monitoring and remediation through PAM and IGA. This accounts for unforeseen disruptions to daily activity while also enhancing efficiency through tailored AM and CIAM.

CIP-003-8 Security Management Controls

Overview – This mandate requires that enterprises establish a clear chain of accountability delineating who is responsible for each stage of BES security. This segment requires that authority be clearly delegated with a senior manager empowered to develop policies around consistent and sustainable security management controls. The standard also requires that the enterprise provide for remediation strategies in advance of emergency situations.



How IAM Helps – A robust PAM solution rolls out extensive role-based access controls, allowing your enterprise to provision, track, and deprovision all aspects of your identity fabric from a single trusted source.

The safety of your cloud must be a consideration for satisfying CIP-003 as well. Pairing an orchestrator with a secure CIEM solution ensures that your security controls are comprehensive and standardized regardless of which part of your enterprise they are in.



CIP-004-6 Personnel & Training

Overview – This rule concerns staff and contractor training for cybersecurity best practices. Recognizing that most cybersecurity incidents result from human elements, this provision is separated into two primary areas. The first is cybersecurity awareness, a ground-level training requirement which provides an easily digestible baseline of cybersecurity awareness and best practices. This training must be carried out a minimum of every 15 months. The second is command-level risk and access control management. This requires that administrators possess a strong knowledge of personnel risk assessment, access management, and revocation or removal of personnel access privileges.

How IAM Helps – A managed identity service's assessment will not neglect the human side of your identity needs. Beyond providing a personal point of contact with your enterprise, they will ensure that you are equipped with the best teaching tools and topics to impart to your staff. Thanks to the experience managed identity experts bring to your enterprise, they are uniquely equipped to establish an effective curriculum.

Additionally, the capabilities of PAM and IGA, especially when augmented by automatic controls, can go a long way towards guiding your users down the path of good identity hygiene. Real-time tracking of usage and automatic policy enforcement makes adherence to good practices much easier on users, reducing friction without compromising security.

CIP-005-6 Electronic Security Perimeters

Overview – This rule protects BES cyber systems by requiring the presence an Electronic Security Perimeter (ESP) and decisive controls over network access to critical assets. This includes data monitoring, encryption, record-keeping, and shutoff capability. Any assets located outside of the perimeter (such as off-site systems or clouds) are only allowed to connect to the network through a specific Electronic Access Point (EAP).

How IAM Helps – A managed identity service can plan, implement, and maintain the mandated ESP as well as institute the controls needed to comply with CIP-006. By bringing together the most suitable products into a unified package, your systems no longer need to worry about losing track of critical functions. The component IGA and CIEM of your orchestration tool ensures that no identity is provisioned more than it should be while enabling greater efficiency through role-based permissions. Whether in-house or on the cloud, your perimeter remains within your awareness and control.

With a properly structured orchestration tool, no third-party systems connected with your enterprise is truly outside your perimeter. Your PAM can be set up to automatically enforce security policies, track usage, and even auto-shutoff both internal and external applications and users.

CIP-007-6 Systems Security Management

Overview – This outlines the precise parameters that enterprise security systems must follow for safeguarding BES assets. These include disabling any logic ports which present security risks, disabling unnecessary physical or output ports connected to BES assets, fully installing security patches on all security systems, and evaluating those patches at least once every 35 calendar days. It also requires that any malicious code be immediately removed, security events must be logged, and security systems must raise alerts for critical incidents.

How IAM Helps – Not only can a managed IAM provider pin down the vulnerable ports of your enterprise and correct them, but they can also institute systems to prevent them from appearing again. By federating PAM and CIEM solutions into an orchestration tool, patches, assets, and evaluations can be expedited, catalogued, and unified across your entire identity fabric. While human oversight is still needed during the testing phase, the automation of your systems eases the process and shortens time to completion. Furthermore, thanks to the heightened security from your IGA, PAM, and CIEM solutions, incidences of compromised security are much less likely to come up in the first place.

"Managed IAM providers can automate the process of securing BES assets, reducing the time to completion and freeing up human resources for other tasks."

CIP-008-6 Incident Reporting and Response Planning

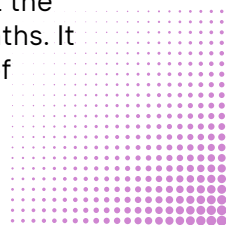
Overview – This standard puts down guidelines on the best ways to respond to cyber incidents with a cybersecurity incident response plan. It requires that enterprises have a clearly delineated remediation strategy for identifying, classifying, responding to, reporting, and documenting cybersecurity incidents. This mandate also requires the plan be tested at least once every 15 months as well as communicate any changes to the plan to the relevant stakeholders within 90 days of a security incident.

How IAM Helps – An IAM assessment will clearly lay out the best recommended practices for employee responses in the case of a cyber incident, instituting a clearly defined emergency action plan. When paired with the security features of an automation-enabled PAM, the dangers posed by breach incidents can be greatly reduced. Your systems cease to rely on flawed human reactions, catching suspicious activity as soon as it happens and clamping down on further infiltration.

Additionally, your enterprise won't have to worry about long hours spent evaluating or testing, as your identity service experts can implement systems to carry out these necessary functions with minimized oversight. For those functions which require human eyes, your managed identity service provider can work with you to keep you up to date and prepared.

CIP-009-6 Recovery Plans for Critical Cyber Assets

Overview – This requirement concerns recovery planning in the aftermath of breach incidents. This includes clearly outlining activation conditions, the roles and responsibilities of incident responders, the systems needed to carry out the recovery, and meaningful testing cycles every 15 months. It also deals with the backup, verification, and storage of information vital to restore BES functionality.



CIP-010-3 Configuration Change Management and Vulnerability Assessments

Overview – This NERC requirement covers a wide range of domains related to the management of configurations and vulnerability assessments. They require that enterprises develop change management configurations for non-independent OS or firmware, commercially sourced or open-source applications, custom software installations, logical network accessible ports, and security patches. They must also document changes, update baseline config within 30 days of making those changes, and verify that any changes conform to CIP-005 and CIP-007 standards. These changes must also be tested under specific conditions every 35 days and any software installed onto security systems must be tested prior to installation. Additionally, a vulnerability assessment must be carried out at least once every 15 days or whenever a new asset is integrated into the production environment.

How IAM Helps – It should go without saying that the assessments performed during the initial stages of a digital transformation serve to satisfy the above requirements, assuming of course that the recommendations are implemented. Rules about future change documentation can be provided for as well.

However, executing on those initiatives is where managed IAM really shines. A bespoke orchestration solution augmented with automated systems can regularly satisfy most of the testing requirements. Any tests which cannot be wholly performed by machines can still be expedited and eased. This is accomplished through purpose-built platforms created by your managed IAM service provider.

CIP-012-1 – Communications between Control Centers

Overview – This requires that organizations protect real-time communication of assessment or monitoring data during transmission between control centers. Recommendations include security risk mitigation, defined responsibilities, verifiable demonstration of compliance with secure data transmission protocols, and compliance with CIP-012.

How IAM Helps – Identity orchestration is one of the greatest tools ever devised for the purpose of unified identity control. It allows enterprises to observe usage in real time across the planet. An orchestration platform puts different locations in synchronous operation with each other. Orchestration also enforces (manually and automatically) policies that strengthen security and efficiency.

The orchestration platform, and satisfaction of CIP-12, are completed through the institution of a fully realized CIEM solution. This ensures that third party cloud platforms allow for distant collaboration without compromising security.

Conclusion

Major enterprises must consider their investments carefully, lest limited resources be squandered while necessary undertakings flounder. The necessary satisfaction of NERC CIP compliance is an opportunity for comprehensive improvement for both security and efficiency. By strategically deploying IAM solutions, your needs for compliance and desires for greater safety and performance can be accomplished in a single stroke.

When faced with mandates like NERC CIP, you must choose either to begrudgingly fulfill your obligation or else seize the chance to evolve. If your investment must be made, why not maximize its returns?