FORTRA™

WHITE PAPER (TRIPWIRE)

Achieving Resilience While Fulfilling NERC CIP Requirements

Compliance and Beyond with Tripwire

Some of our nation's most critical physical infrastructure is represented by the national Bulk Electric Systems (BES). Today's digital world relies upon this interconnected network of power generation and transmission systems more than ever. To ensure the reliability and resilience of that network, providers must continually manage threats to the infrastructure, including many that relate to cybersecurity. Meanwhile, providers must also continuously manage costs and other resources to meet customer demands and maintain reasonable utility rates for customers.

To keep the lights on, regional power providers have been collaborating and interoperating for almost a century. This cooperation introduces dependencies and heightens the need for consistent standards of practice. Each member has a responsibility to the joint network to follow those practices, thus supporting the safety and reliability of the entire system. Imbalance or failure in the system can have a devastating impact, as shown by the 2021 Texas power outages that impacted at least 4.5 million customers. Since 1968, the North American Electric Reliability Corporation (NERC)[1] has played an important part in governing resilience standards and practices for the network.

Risk management is a continual balance among benefits, risks, and resources. Convenient electrical power brings many benefits, but, of course, such power isn't free. In addition to the direct cost of generating and distributing power, providers must also account for various risks—from tree limbs to vandalism to cybersecurity attacks—that might jeopardize the availability of those functions. Providers and distributors continually work together, applying practical critical infrastructure protection from an evolving set of threats and vulnerabilities, natural and man-made.

Like that changing risk landscape, the methods for responding to that risk must continually evolve. Throughout the 21st century, NERC has coordinated that response through a set of reliability standards known as the Critical Infrastructure Protection (CIP) standards. These requirements demand a constant review of the risk balance described above. Providers know that personnel, processes, and technology are needed to manage risks; they also understand that market demands (and utility rate pressure) limit the resources available for risk management.

Similar trade-offs occur on the part of those providing oversight, seeking effective supervision without onerous micromanagement. Optimally, participants in the BES seek not to simply comply with the rules by doing the minimum necessary but rather to operate a safe and reliable system in light of both requirements and cost constraints. Such a system meets the needs of customers and other stakeholders while also complying with industry standards of practice.

Challenges of Meeting NERC CIP Requirements

NERC CIP includes 13 cybersecurity and physical infrastructure security standards, comprised of 44 management, administrative, and technical controls. Meeting this broad set of requirements is crucial yet challenging, especially with limited resources. In fact, at times, just documenting and explaining compliance can draw resources away from other activities, including risk management operations.

Other challenges include:

- **Manual processes are insufficient for meeting NERC CIP baselines.** Human solutions can't keep pace with today's high-speed digital environments. Manual procedures (unsupported by automated tools and processes) can be prone to errors.
- **Difficulty staying current with changes to the standards based on evolving risk landscape.** CIP processes change over time—each revision of the NERC CIP standard expands the scope of critical assets and the technical requirements to secure them.
- **Difficulty understanding requirements.** Clarity of standards has improved over time, but it can be challenging to understand specific compliance needs, expectations of each auditor, and means to demonstrate fulfillment. Providers specialize in energy production, not security risk management, and sometimes find it difficult to understand and achieve what's expected.
- **Challenges of securing a geographically dispersed BES infrastructure.** Many providers have hundreds of systems spread across broad regions, with many that

are often located in difficult terrain. Such a system depends upon sensors and interfaces for continual reporting, and those sensors represent both potential failure points and attack surfaces.

- **Difficulty maintaining situational awareness of a broad and varying set of cyber assets.** Manually collected data may be insufficient or out of date, a challenge that is accentuated by the many types of platforms that enable, control, and monitor this critical infrastructure. Out-of-date and inaccurate inventory and security posture information often leads to negative audit findings.
- **Change management challenges hinder protection, detection, and response activity.** Even the most comprehensive documentation and compliance across the full breadth of the organization must be continually updated for new/replacement assets, locations, facilities, and technologies.

While these challenges can be daunting, the need for cost-effective risk management has never been greater. Nation-state attacks on the Ukrainian power system, a terrorist attack on a Pacific Gas and Electric substation, and even a recent issue at a municipal water treatment plant in Florida all highlight the heightened need for vigilance and preparedness.[2] And this mounting pressure occurs at a time when providers are faced with increasingly limited personnel and resources.

A Cost-Effective Solution for Resilience and Compliance

For nearly ten years, Fortra's Tripwire NERC CIP Solution Suite has been enabling a risk-based approach for hundreds of members of the North American bulk power system. Our engineers stay current about changes to both technology and standards, helping you stay continually compliant and resilient. That ongoing intelligence enables Tripwire's automation solution—keeping you current about changes to industry practices, updates to NERC CIP policies, and methods to efficiently apply new controls to new asset classes when needed. These proven products are backed by the expertise of Tripwire's professional services, skilled practitioners who help you apply the proper controls, generate the appropriate documentation, and meet demanding deadlines for changing regulations.

Proven Automation Solutions Drive Reliability and Compliance

Tripwire's proven automation solutions ensure effective continuous cybersecurity monitoring and CIP compliance. Human-based protection, detection, and response processes are error-prone and often less efficient than automated methods. Automation is a force multiplier, consistently performing routine tasks and freeing valuable personnel to focus their attention on enterprise priorities.

Tripwire has been meeting the mission-critical network infrastructure needs of industrial enterprises for decades. Tripwire builds on this history with more than 25 years as a leader in cybersecurity. These solutions help you accomplish critical tasks such as:

Identifying and Managing Cyber Assets

For both network defense and compliance, your team needs to be continually aware of what's on the network—confirming availability of trusted devices, ensuring that critical cyber assets haven't gone missing, and verifying that rogue devices have not appeared on the scene. That challenge is amplified for those in the energy sector where assets include industrial control system (ICS) technology. Tripwire brings extensive ICS experience to enable continuous discovery, threat monitoring, and real-time change management on a broad array of SCADA (Supervisory Control and Data Acquisition) components, Human-Machine Interface (HMI) systems, Remote Terminal Units (RTUs), and Programmable Logic Controllers (PLCs). Industrial operators count on Tripwire to decipher over 40 of the most common industrial communication protocols—more than any other ICS visibility solution.

Managing Security Configuration Management

Change and file integrity monitoring (FIM) are Tripwire's DNA. We help you continually monitor for anomalies and changes that might be suspicious (or that might lead to non-compliance) and provide alerts and other actions so that you can rapidly respond. For example, Tripwire® Enterprise is trusted by thousands of organizations to provide sophisticated security configuration management (SCM) and FIM. The only constant in cybersecurity is change, and Tripwire has been the proven leader in security change management since 1997.

Documenting Ports and Services

CIP requires that your organization be able to record, track, and justify every one of the hundreds of ports, protocols, and services on your hosts and traversing your networks. Auditors tell us this is one of the biggest challenges they see in the field, so Tripwire provides the tools to provide the evidence you need and the confidence your managers expect. Those same tools provide a proactive approach through detailed "allow lists" of ports, services, users, applications, and other elements, enabling your security managers to decide what's permitted on your platforms. Our profiler continuously monitors these characteristics and immediately detects anomalies, providing detailed reporting about unauthorized changes.

Continuous Monitoring and Incident Response

CIP requirements demand sophisticated security event monitoring, configuration monitoring, vulnerability assessment, and log review. These same processes are foundational to vigilant network defense. Tripwire provides holistic visibility that continuously collects and reports what's happening throughout your critical information technology (IT) and operational technology (OT) infrastructures. In addition to real-time collection to detect and respond to suspicious activities, Tripwire provides an integrated workflow to respond to events of interest. Whether by creating a work ticket, sending a notification email, or running a command, Tripwire's solutions work together to both support real-time security situational awareness and effective service management to prioritize and address changes and vulnerabilities.

Trusted Advisors Enable Trustworthy and Compliant Infrastructure

Automation itself will not fulfill the objectives, but is very powerful when combined with our NERC CIP-specific rulesets, templates, custom reports, dashboards, and utility extensions. We understand best practices for BES providers—as we bring the experience of hundreds of practitioners to help you comply, we learn from our discussions with auditors. As we learn, we pass that intelligence along through our baselines, product updates, and professional services.

Proven Success for Internal Reviews and External Audits

One of the most critical questions that our customers are asked is, "You claim to have effective processes and procedures for managing cybersecurity risk and NERC CIP compliance, but how do you know?" Not knowing can be costly. Violations of CIP Reliability Standards can result in significant penalties; some have said as much as $1 million per day. Yet, like many standards, the broad applicability of CIP requirements means that the standards are non-specific about exactly how to comply and exactly how to demonstrate conformance.

The road to accountability and performance can be tough to find, but Tripwire's solutions provide a clear pathway for customer success. Auditors and regulators trust Tripwire's automation, baselines, and reports. They recognize that the NERC CIP Solution Suite covers 23 of NERC CIP's 44 requirements. While every audit is subject to the findings of individual reviewers, Tripwire's engineers understand what such auditors have previously expected to see, how they expect it to be documented, and how to use Tripwire's built-in system understanding to support evidence and conformance.

Tripwire's suite brings relevant information together to produce reports that are directly aligned with updated requirements. Consider **CIP-007, Cyber Security – Systems Security Management**, which includes a requirement that only necessary ports and services may be enabled on applicable assets. Tripwire Enterprise provides a detailed report, by asset, that lists each port or service discovered, the justification for each, and date/timestamp information for the discovery. The report also lists any ports that have changed or lack justification, enabling immediate follow-up. This example of audit-ready evidence illustrates that Tripwire's suite helps an entity stay vigilant against adversaries and remain prepared to demonstrate compliance with the reliability standards.

Another control that is frequently flagged by auditors is **CIP-010, Configuration Change Management and Vulnerability Assessments**. Compliance with these requirements includes the need for asset management, understanding of baseline configuration for each Cyber Asset, and documentation of changes to the baseline. Each CIP requirement has specific

and stringent evidentiary criteria—evidence that Tripwire has built into Tripwire Enterprise's comprehensive reports that reviewers have come to know and trust.

While CIP compliance is critical, Tripwire Enterprise also allows you to conform, without additional burden, with a broad array of other standards. The same out-of-the-box solution applies Tripwire Enterprise's intelligence to report enterprise alignment with guidelines from the National Institute of Standards and Technology (NIST) guidelines and with controls such as those from Center for Internet Security (CIS), Sarbanes-Oxley (SOX), and Payment Card Industry Data Security Standard (PCI DSS). Flexible reports based on automated evidence collection enable the entity to always be ready to prove compliance, whether for the boardroom, internal audit, or an external regulator.

Tripwire's professional services staff are experts in NERC CIP compliance and can help apply the proper controls, generate appropriate documentation, and meet demanding deadlines for changing regulations. Tripwire's reliable automated tools and experienced professionals combine to help you stay prepared to defend against skilled cyber adversaries while always ready for compliance reviews.

Beyond Compliance: Secure, Reliable, Resilient Systems

While compliance with mandatory requirements, such as those in NERC CIP, is crucial, the safety and reliability of an entity's information and technology are paramount. The Tripwire NERC CIP Solution Suite provides enterprise security staff with continual awareness of what's on the networks: what assets are expected to be reporting, which might be missing, and what activity is suspicious.

Our host-based intrusion detection and continuous monitoring/system hardening reports quickly highlight changes and help separate the good changes from the bad changes. Tripwire's correlation engines apply the MITRE ATT&CK framework to provide context to observations, helping operators quickly recognize adversaries' tactics, techniques, and procedures (TTPs). Many advisories, such as those from the FBI and the U.S. CISA (an entity of the Department of Homeland Security), often use ATT&CK references to provide warnings or after-action analysis, so this Tripwire correlation helps providers put such alerts in context.

TRIPWIRE COVERAGE OF NERC CIP REQUIREMENTS

13 Standards & 44 Requirements – Tripwire Covers 23

	CIP-002 BES Cyber System Identification and Categorization	CIP-003 Security Management Controls	CIP-004 Training and Personnel Security	CIP-005 Electronic Security Perimeter	CIP-006 Physical Security of BES Cyber Systems	CIP-007 Systems Security Management	CIP-008 Incident Reporting and Response Planning	CIP-009 Recovery Plans for BES Cyber Systems	CIP-010 Configuration Change Management and Vulnerability Assessments	CIP-011 Information Protection	CIP-012 Control Center Communica-tion Network	CIP-013 Supply Chain Management	CIP-014 Physical Security
1	BES Cyber System Identification	Cyber Security Policy for High/ Medium Systems	Awareness	Electronic Security Perimeter	Physical Security Plan	Ports and Services	Cyber Security Incident Response Plan	Recovery Plan Specifications	Configuration Change Management	Information Protection	Physical & Logical Risk Mitigation for Data	Risk Management Plan	Transmission Station Physical Security
2	Regular Approval	Cyber Security Policy for Low Systems	Training	Interactive Remote Access Management	Visitor Control Program	Security Patch Management	Cyber Security Incident Response Plan Implemen-tation and Testing	Recovery Plan Implemen-tation and Testing	Configuration Monitoring	BES Cyber Asset Reuse and Disposal	Proof of Implemen-tation	Proof of Implemen-tation	Third Party Verification of Physical Security
3		Identification of Senior Manager	Personnel Risk Assessment Program		Maintenance and Testing Program	Malicious Code Prevention	Cyber Security Incident Response Plan Review, Update, Communi-cation	Recovery Plan Review, Update and Communi-cation	Vulnerability Assessments			CIP Senior Manager Approval	Primary Control Center
4		Delegation of Authority	Access Management Program			Security Event Monitoring			Transient Cyber Assets and Remov-able Media				Evaluate Potential Threats & Vulnerabilities
5			Access Revocation Program			System Access Controls							Physical Security Plan
6													Third Party Review of Plans

Conclusion

Those responsible for power generation and distribution face a broader set of risks than ever before. In addition to the forces of nature that have historically challenged the electric grid, such providers must prepare for and thwart increasing threats from hackers, terrorists, and even nation-states. Many organizations have limited personnel for addressing these risks—in some cases a single individual. Requirements such as the NERC Critical Infrastructure Protection standard provide the necessary oversight to ensure that, in this interdependent system, all are fulfilling that responsibility, but providers may find it difficult to understand, conform, and document compliance with such standards. Tripwire's NERC CIP Solution Suite, paired with specialized engineering expertise in the electrical reliability field, will help ensure that organizations can meet their consumers' needs for a safe and reliable infrastructure that fulfills the evolving expectations of industry regulators.

Schedule Your Demo Today

Let us take you through a demo of the Tripwire NERC CIP Solution Suite and answer any of your questions.
Visit tripwire.com/demo

References

1 A brief history of the North American Electric Reliability Corporation is available from https://www.nerc.com/news/Documents/HistoryofNERC01JUL19.pdf (retrieved Feb 1, 2021, login required)
2 For information about similar issues, please see "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations" Congressional Research Service. July 02, 2015.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.