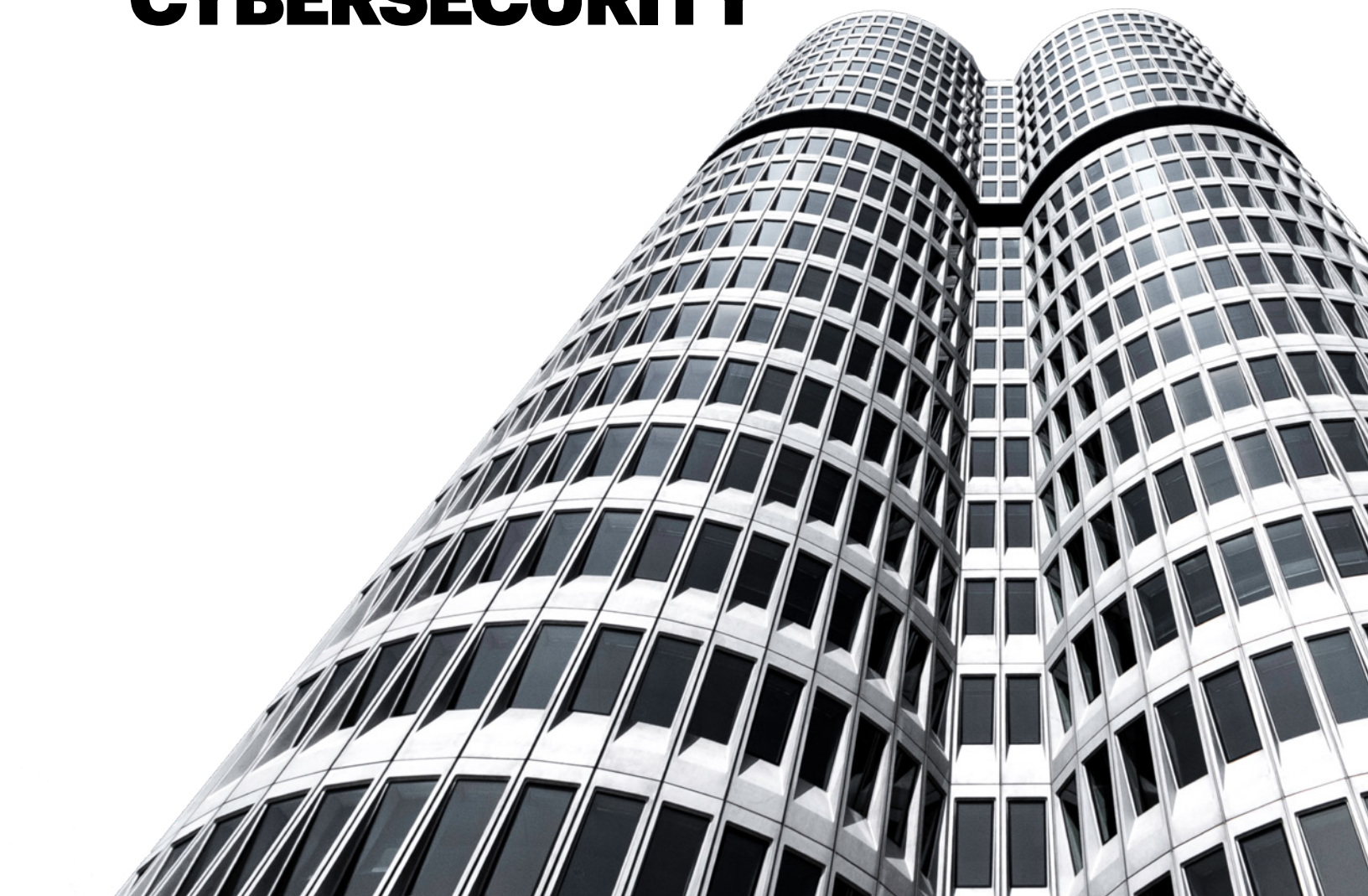
accenture

BEING BETTER PROTECTED:

NERC CIP CONTROL CENTER CYBERSECURITY



NERC'S CIP-012-1 STANDARD IS VITAL TO SAFEGUARD UTILITIES' CONTROL CENTER COMMUNICATIONS

As recent research shows, the good news is that cyber defenses continue to improve. The bad news is that cyber threats continue to advance as well. To that end, the North American Electric Reliability Corporation (NERC) has issued a critical infrastructure protection (CIP) standard in draft form that requires utilities to devise cybersecurity protections for control center communications.

The standard focuses specifically on the common ground where control rooms interact. The goals for CIP-012-1[i] ("Cyber Security—Communications between Control Centers") include mitigating the risk of unauthorized disclosures and responding to attempts to modify the real-time assessment and monitoring data transmitted between control centers. Achieving CIP-012-1 compliance is important for utilities seeking to protect their control centers.

Independent Service Operators (ISOs), which coordinate, control, and monitor the operation of the electrical power system, have multiple data links to many utility control centers within their regions and are likely to play a key role in CIP-012-1 compliance. For example, to comply with CIP-012-1, the ISOs will require utilities with applicable data connections to establish secure communications between control centers. If a utility cannot implement the necessary data link security controls, the ISO in the worst case could disable or delete the data link with that utility. Typically, these data links make it possible for a utility to participate in the marketplace. Therefore, a utility that does not implement CIP-012-1 according to the ISO's design specifications could, ultimately, find itself unable to participate in the energy market; a thought that is impossible to imagine and unacceptable to regulators, customers and shareholders.

While it is important to get ahead of all NERC CIP requirements, doing so with CIP-012-1 should be a mandate, given what is at stake. Three specific forward-looking actions should top the list: Start planning all system and application changes with an eye toward CIP-012-1 compliance; compel vendors to ensure that their solutions mesh with your CIP-012-1 requirements; and coordinate with neighboring utilities and ISOs.

Understanding the impact

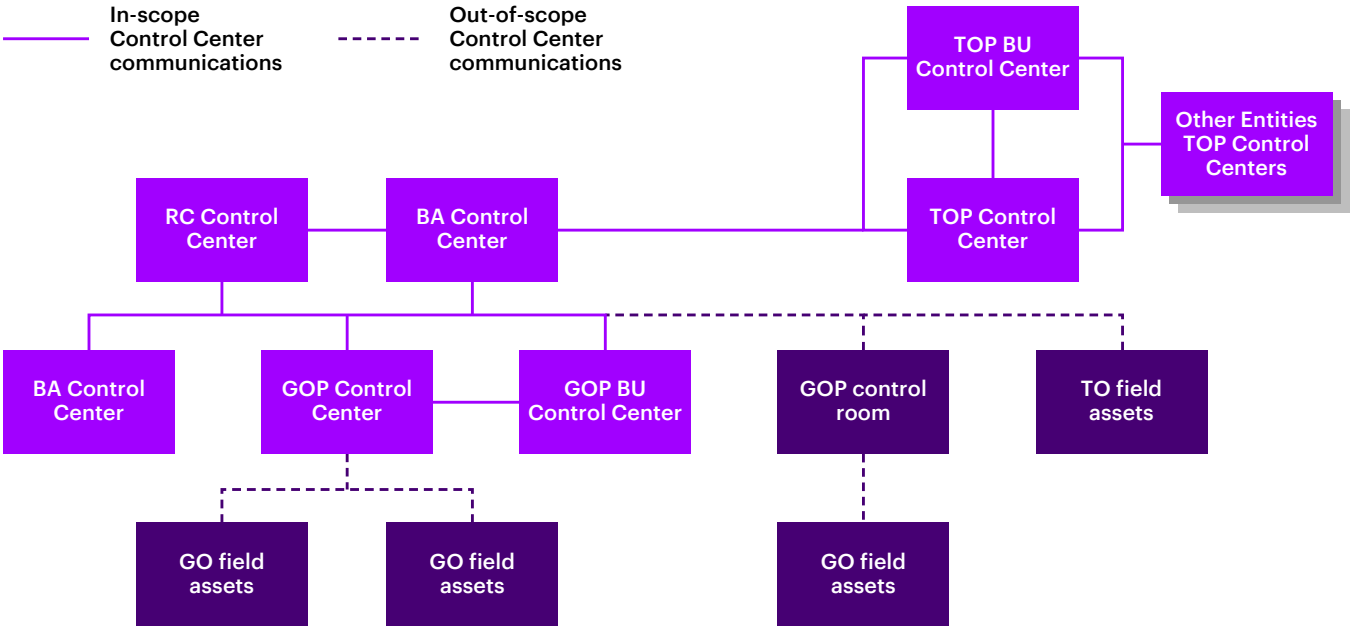
CIP-012-1 compliance requires responsible entities to meet a mix of technical and people-centered requirements.

TECHNICAL CONSIDERATIONS

Technical stipulations include the identification of the utility's control centers, their respective data centers, all real-time data links between control centers, all demarcation points, the security controls employed to protect data, and critical roles and responsibilities.

To identify which data connections fall within the scope of the regulation, NERC is proposing a new definition of "control centers" and has provided a diagram indicating in-scope control center communications in the "CIP-012-1 Technical Rationale" document. Note that the major difference in the responsibility highlighted below is when a Balancing Authority (BA), Generator Operator (GOP) or Transmission Operator (TOP) controls only one field asset (for example, peaker plant) or when communicating with field switching personnel. For more definition, please see the "proposed definition of control center" document from NERC.

Control Centers in scope



A wide variety of control center communications will typically fall within the scope of the regulation. They include:

- The Inter-Control Center Communications Protocol (ICCP), an operational protocol used by electrical utilities
- Other supervisory control and data acquisition (SCADA) data links
- Real-time assessment data links (primarily ICCP) used for state estimator power system analysis
- Contingency analysis
- Stability assessments

The regulation also covers many wide-area monitoring data links and communications to Web portals for transmission equipment outages, including outage scheduling solutions. Other CIP-012-1 communications include market interfaces such as PJM eTools, the real-time data synchronization between primary and backup control centers, and automatic generation control data that is transmitted between control centers.

Given the breadth and depth of the affected communications, complying with CIP-012-1 could require an array of potential solutions that utilities will want to consider carefully. They also need to coordinate the implementation of these technologies with their vendors and with other responsible entities associated with the control center to which they connect. These could include network- or application-level encryption, the exchange of cryptographic keys, secure SCADA protocols and private data networks.

PEOPLE PLANS

Utilities need to identify the personnel required for ongoing management and process governance for CIP-012-1. Other key positions include the ongoing management of affected operating technology and information technology (OT/IT) support staffs, especially the network engineers and data engineers, developers, administrators, as well as communications and data link support personnel. It is also possible that security operations center (SOC) personnel will receive alerts for some indicators of compromise (IOC) on an in-scope data link. The subsequent reaction process should include steps for proper escalation and the recording of potential evidence artifacts for CIP-012-1.

Each utility should include NERC CIP-012-1 as part of the existing NERC Governance and Compliance structure for all NERC standard processes.

As part of the process for design, vendor engagement, implementation, ongoing management and maintenance, as well as governance, the utility should engage and seek input and consensus from many stakeholders within the organization. Suggestions include transmission and distribution operations, reliability coordinators, network application engineers, OT/IT engineering and support, IT governance and compliance, and corporate, NERC governance and compliance.

Addressing potential challenges

Other CIP standards determine which compliance requirements apply based on whether the affected bulk electric system (BES) cyber assets receive a low-, medium- or high-impact rating. In contrast, CIP-012-1, which covers communications between in-scope industry control centers, applies to all impact levels, whether high, medium or low. To help responsible entities correctly identify facilities where CIP-012-1 requirements apply, NERC is proposing a new glossary definition of the term "control centers." While the NERC CIP glossary will define a control center, the actual perceived limiting factors regarding what it includes or omits could lead to competing definitions.

Three ways to overcome these and other CIP-012-1 compliance challenges involve understanding the scope of the plan, choosing the right partners, and making several production changes.

FOCUSING ON SCOPE

The following three suggestions can help utilities identify any gaps in the work they need to perform to achieve compliance with CIP-012-1.

1. Assemble an accurate inventory of all circuits* that feed into the control center.
2. Identify which circuits are in-scope by understanding each circuit's purpose.
3. Identify the key data to collect for each circuit. For example, include the unique circuit identifier, protocols transmitted over the circuit, who "owns" the circuit, and where the demarcation points reside.

*** Note:** This refers to technology circuits rather than electrical circuits.

Several other key indicators for gaps include currently used protocols with known vulnerabilities. For example, insecure SCADA protocols such as ICCP or DNP3. Responsible entities should transition to secure versions of these protocols as soon as possible. For other unencrypted communications, it also makes sense to transition to secure protocols such as transport layer security (TLS) protocols, or similar.

CRAVING COLLABORATION

Utilities will need support from vendors, especially energy management system (EMS) and SCADA suppliers. Integrators and vendors should build CIP-012-1 controls into their system designs from the outset, not only for legacy systems and communications, but also when modernizing the grid system as well.

They should engage vendors to gain access to the required functionality and compatibility to communicate between control centers. For example, two utilities use different vendors. Unsecured communications exist between the two vendors, and the first vendor's planned secure communications are incompatible with the second's. To resolve such issues, utilities should engage with their vendors as early as possible. Utilities should also coordinate with the control centers of other entities and work to ensure that the implementation timing of the underlying technology on both ends meets the needs of all parties. Problems can occur when one entity may be ready to transition sooner than the other.

SAFEGUARDING PRODUCTION CHANGES

A CIP-012-1 goal is making the transition without disrupting the exchange of production data. Transitioning from an unprotected or unencrypted communications circuit to an encrypted one means decommissioning a "working" circuit and replacing it with a new and untested version. Success will require the careful planning, design, testing, and scheduling of a cut-over from an old circuit to the new one. Testing prior to the planned cut-over should be a priority. Utilities also need a fall-back scenario in case the new circuit causes an outage of required production data.

The transition to CIP-012-1 requires strong and continuous inter-entity communications and notifications, especially concerning planned changes. Other entities may not know about CIP-012-1 implementation plans, which could cause the reclassification of the status of a data link from out-of-scope to in-scope. The lack of communication could also cause both parties to drift out of compliance when they institute changes. To gain the time needed to comply in such circumstances, one or both players may have to delay planned changes. Utilities occasionally find IT/OT monitoring and diagnostic tools may not work on encrypted circuits, making communications' troubleshooting more difficult. Many times, security control and circuit troubleshooting can depend on having sufficient visibility of the transmitted data. The point in the network at which a utility monitors network traffic may require changes to accommodate a lack of monitoring capability of encrypted data. Therefore, companies should plan ahead to safeguard the IT monitoring capabilities they seek to maintain.

Next steps toward CIP-012-1 compliance

How does a utility successfully achieve CIP-012-1 compliance? As any track star knows, a good start can provide the momentum to win at the finish line. In this case, a good start involves developing a comprehensive strategy that considers a responsible entity's strengths and weaknesses. Organizations also need to assemble and mobilize an empowered CIP-012-1 team, and work to ensure the sustainability of the program from the outset.

DEVELOPING A STRATEGY

Start a CIP-012-1 compliance conversation among all stakeholders both within and beyond the organization. CIP-012-1 will have interdependencies with other NERC standards, and teams need to recognize the types of inter-control center communications required, and determine which ones also must also achieve CIP-012-1 compliance. Several operational standards concerning state estimator systems and data availability may affect or inform CIP-012-1 actions. Additionally, the proposed changes to the definition of a control center could expand the NERC's CIP coverage and lead to additional actions.

Responsible entities can take several steps immediately regarding CIP-012-1 compliance. For example, they can determine ownership and responsibility within the business and the compliance organization and begin a dialogue with key stakeholders and vendors. Other steps include setting aside enough time to define and implement the controls, demonstrating evidence within the enforcement timeframe, and compiling a complete inventory of communication circuits.

During these initial discussions and activities, responsible entities might consider identifying the key internal and external stakeholders and understanding the differences between the CIP-012-1 requirements and existing protection for communications between control centers. They can also identify timeline and implementation phases and work to understand the interrelationships between CIP-012-1 and other CIP standards.

MOBILIZE YOUR CIP-012-1 TEAM

As responsible entities mobilize their CIP-012-1 compliance teams, key considerations include determining executive sponsorship for the governance and steering organizations and identifying contacts beyond the organization, such as utility partners, the International Standards Organization (ISO) or reliability organizations. It also makes sense to take automation lessons from the broader NERC CIP compliance program, and to ensure that evidence collection follows the leading practices developed through prior cycles of regulatory audit.

PLAN FOR SUSTAINABILITY FROM THE START

It is crucial to plan for sustainability from the outset. To do this, utilities should:

- **Design CIP-012-1 controls** to include compliance and verification processes in an orchestrated fashion with minimal manual reviews required
- **Redesign circuit provisioning processes—**in alignment with change control processes—to ensure the correct classifications and controls are consistently applied when provisioning new circuits and appropriate evidence is collected to justify the classification

- **Standardize all evidence-gathering processes and tooling** while orchestrating and converting them to appropriate formats, such as reliability standard audit worksheets (RSAWs) for audits, with an eye toward automating them as much as possible
- **Establish a robust change control program** in accordance with CIP-010. This program should identify, approve and document all modifications and updates for BES high- and medium-impact cyber systems and applicable associated systems

A final note: unlike many other CIP standards, at the time of writing, CIP-012-1 does not require an annual review.

STANDARD APPROVAL

NERC CIP stakeholders approved the final ballot of CIP-012-1 on August 13, 2018. NERC Board of Trustees subsequently adopted and submitted CIP-012-1 standards to FERC for regulatory approval. Assuming the standard FERC review and approval process timing, the estimated effective date will be in the first half of the 2022 calendar year.

References

i https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

CONTACTS

Gilbert Sorebo
Senior Manager
Accenture Security
gilbert.n.sorebo@accenture.com

James Wright
Senior Manager
Accenture Security
j.a.wright@accenture.com

Thomas Ryan
Principal Director
Utilities Industry
Accenture Consulting
thomas.c.ryan@accenture.com

Jamie Bass
Managing Director
Accenture Security
james.bass@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.