PREPARING FOR CIP-015-1 COMPLIANCE

APPLICATION BRIEF

zentera™

HEADQUARTERS	UEI	CAGE CODE
Milpitas, CA	FV52BTENJK2	9DR15

INTRODUCTION AND EXECUTIVE SUMMARY

On July 2, 2025, the Federal Energy Regulatory Commission (FERC) published a final rule formally adopting Reliability Standard CIP-015-01 to improve the cybersecurity of electric systems by requiring Internal Network Security Monitoring (INSM) within Electronic Security Perimeters (ESPs).

This brief outlines the requirements, affected entities, compliance timelines, challenges in achieving compliance, and explains how Zentera's CoIP® Platform helps Responsible Entities achieve compliance.

WHO IS AFFECTED BY CIP-015-1?

CIP-015-1 applies to Responsible Entities operating High-Impact or Medium-Impact Bulk Electric System (BES) Cyber Systems with External Routable Connectivity (ERC), including:

Balancing Authorities: Entities ensuring electricity supply matches demand in their region.

Distribution Providers: Organizations delivering electricity to end users.

Generator Operators/Owners: Entities operating or owning power generation facilities.

Reliability Coordinators: Entities overseeing grid reliability across large areas.

Transmission Operators/Owners: Entities managing or owning transmission infrastructure.

WHAT ARE THE COMPLIANCE REQUIREMENTS FOR CIP-015-1?

Responsible Entities must implement INSM to monitor network traffic within the ESP, detect and retain data on anomalous activity, and protect this data from unauthorized access or tampering. The standard includes three requirements:

R1: Develop and implement documented processes to monitor network activity (connections, devices, communications) within the ESP.

R2: Collect and retain data on anomalous network activity for analysis to detect potential cyber threats.

R3: Protect INSM data to ensure its confidentiality, integrity, and availability.

FERC has directed the North American Electric Reliability Corporation (NERC) to update CIP-015-1 by September 2, 2026, to extend INSM to Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) outside the ESP, addressing vulnerabilities in trusted access points.

WHY IS NERC CIP-015-1 COMPLIANCE CHALLENGING?

ESPs have been designed to protect the assets inside at the perimeter boundary. Much less emphasis is usually placed on protecting the assets inside from each other; this lateral access within the ESP is precisely what FERC is targeting. Many existing ESPs do not have the visibility needed to achieve the level of INSM that FERC envisions, meaning that Responsible Entities need to develop strategies to retrofit existing ESPs for visibility and then make sense of the data feeds. Both of these steps can be quite challenging.

One method for detecting anomalies relies on comparing traffic against a baseline and using protocol analysis, heuristics, and other statistical methods to identify anomalies. This approach requires careful tuning in order to avoid significant false positives or false negatives, either of which make the INSM ineffective. Another approach is categorizing traffic according to pre-defined policies and continuously comparing traffic against this policy baseline. This second model is a natural byproduct of Zero Trust initiatives that continually authorize and authenticate traffic according to policies.

Responsible Entities must carefully evaluate and select a path consistent with their current goals and future requirements.

WHAT ARE THE NERC CIP-015-1 COMPLIANCE DEADLINES?

The final rule is effective September 2, 2025. Compliance deadlines are:

High-Impact BES Cyber Systems: **September 2, 2028** (36 months from effective date). Medium-Impact BES Cyber Systems with ERC: **September 2, 2030** (60 months from effective date).

Responsible Entities should begin planning now for future requirements to ensure readiness for the updated standard.

GETTING READY FOR NERC CIP-015-1

HOW SHOULD RESPONSIBLE ENTITIES PLAN FOR CIP-015-1 COMPLIANCE?

To achieve CIP-015-1 compliance, Responsible Entities should follow this three-step process, designed to be actionable for all utilities:

1. **Understand Requirements and Assess Current State**

    - Review CIP-015-1 requirements (R1-R3) and FERC's guidance in the Federal Register (Federal Register).

    - Map network configurations, identifying BES Cyber Systems, EACMS, Protected Cyber Assets (PCAs, e.g., supporting servers), and PACS within the ESP.

    - Assess existing tools (e.g., SIEM) for INSM capabilities, such as monitoring network traffic and detecting anomalies.

    - Conduct a gap analysis to identify deficiencies in current monitoring capabilities and coverage within ESPs.

2. **Develop and Implement INSM Controls**

    - Develop documented INSM processes to monitor network activity, detect anomalies (e.g., unexpected SCADA traffic, unauthorized access), and protect data.

    - Deploy or enhance tools (e.g., network intrusion detection, behavioral analytics) to address identified gaps, ensuring alignment with R1 (monitoring), R2 (data retention), and R3 (data protection).

    - Train staff on INSM processes and tools to ensure operational readiness.

    - Plan for future requirements by assessing EACMS and PACS outside the ESP, leveraging FERC's incentives for early adoption.

3. **Validate and Sustain Compliance**

    - Conduct testing (e.g., simulated attacks, red teaming, tabletop exercises) to validate that INSM controls effectively detect and respond to anomalous activity.

    - Document INSM processes, configurations, and test results to demonstrate compliance during NERC audits under the Compliance Monitoring and Enforcement Program (CMEP).

    - Periodically review and update INSM controls to address evolving threats and prepare for the modified CIP-015-1 standard (expected by September 2, 2026).

    - Engage with the Electricity Information Sharing and Analysis Center (E-ISAC) for threat intelligence and best practices (E-ISAC).

HOW ZENTERA HELPS ACHIEVE CIP-015-1 COMPLIANCE

ESTABLISH VISIBILITY WITH A ZERO TRUST ARCHITECTURE

Since the focus on ESP security has traditionally been at the boundary, utilities may not have architected ESPs with the visibility needed to implement an INSM. While access control lists (ACLs) and network segmentation such as VLANs can filter traffic, they do not provide visibility.

Zentera's CoIP Platform provides a Zero Trust architecture that directly fulfills CIP-015-1's core INSM objectives: establishing network activity baselines through policy definition, detecting anomalies through policy violations, and maintaining comprehensive logs with identity context for incident investigation. Key features include:

Non-Disruptive Deployment: Deployed as a software agent (Windows, Linux, Mac) or inline gatekeeper, the platform integrates seamlessly to protect legacy Operational Technology (OT) systems, such as Power Control Relays and Remote Terminal Units (RTUs), without requiring network infrastructure changes.

Microsegmentation, Identity-Based Access, and Visibility: By creating policy enforcement points at protected assets, the platform microsegments the ESP, allowing only authorized communications. Identity-based policies enable richer anomaly detection (e.g., detecting SCADA access using unusual client software) compared to traditional packet-level monitoring.

Direct Alignment with CIP-015-1 INSM Requirements:
R1: Provides continuous network monitoring and visibility into all connection attempts within the ESP that is enriched with additional context about users, software, and devices, establishing baselines through policy definition and detecting anomalies through policy violations.

R2: Detects and logs anomalous activity in the zCenter orchestrator with configurable retention policies; exports events via integration with SIEM for analysis.

R3: Protects INSM data through secure deployment of orchestrators, as well as real-time replication to HA/DR orchestrators, ensuring protection for source data.

Scalability and Future-Readiness: Scalable across substations, control centers, and cloud environments, the platform prepares utilities for future CIP-015-1 modifications, such as INSM for EACMS and PACS outside the ESP.

Broader CIP Alignment: Beyond CIP-015-1, CoIP Platform supports compliance with CIP-005 (ESP management), CIP-007 (system security), CIP-011 (information protection), and emerging standards like CIP-005-8 (logical isolation), offering a holistic cybersecurity solution.

Example Use Case: An authorized user is connected to a jumphost in the ESP and attempts to access a SCADA system. The authorized user has proper entitlements and is using known good software; this access is allowed. A malicious process on the jumphost simultaneously attempts to access the SCADA system using different software. Since neither the malicious process nor the software is trusted, CoIP Platform flags this as an anomaly, blocks the access, and logs the event for SIEM analysis, protecting BES Cyber Systems. This demonstrates how a Zero Trust Architecture provides both INSM compliance and prevention - simultaneously detecting the anomalous activity (R1), logging the event with sufficient fidelity for investigation (R2), while protecting the monitoring data through secure orchestrator controls (R3).

ZERO TRUST: A SUPERIOR ARCHITECTURE FOR CIP-015-1

BEYOND COMPLIANCE: A FUNDAMENTALLY BETTER APPROACH

While traditional INSM solutions attempt to retrofit monitoring capabilities onto existing perimeter-based architectures, Zentera's Zero Trust approach **inherently fulfills CIP-015-1 objectives** through its core design principles. This architectural alignment provides utilities with superior compliance capabilities and operational efficiency.

TRADITIONAL INSM CHALLENGES VS ZERO TRUST

Conventional INSM (e.g., intrusion detection) can struggle to distinguish between unusual but legitimate activity and threats. This can result in high false positive rates, which in turn generate alert fatigue.

Fundamentally, traditional INSM is post-breach detection. It identifies attacks after they've *already* gained network access and are propagating.

ZERO TRUST: PROACTIVE AND PROTECTIVE

Baselines inform policy definitions; legitimate behavior is explicitly defined through authorized access policies. Every connection is authenticated and authorized, not just monitored. This means that any activity outside the defined policy is inherently anomalous.

Zero Trust blocks unauthorized activity while simultaneously logging attempts. Zero Trust alerts are high-fidelity, providing specific context (who, what, when, where) for investigation.

FUTURE-READINESS FOR EVOLVING CIP REQUIREMENTS

ALIGNMENT WITH EXPANDING CIP-NETWORKED ENVIRONMENT

As FERC extends INSM requirements to EACMS and PACS outside the ESP, Zero Trust Architectures provide *seamless scalability*:

Consistent Approach: Same policy-based monitoring applies across all network segments

Simplified Management: Centralized orchestration across distributed environments

Unified Visibility: Single pane of glass for ESP and extended CIP-networked environment

CLOUD AND HYBRID ENVIRONMENT READINESS

Traditional perimeter-based INSM struggles with cloud integration, while Zero Trust Architectures *natively support*:

Hybrid Deployments: Consistent security across on-premises and cloud environments

Remote Operations: Secure access for distributed operational teams

Third-Party Integration: Controlled vendor access with comprehensive monitoring

IMPLEMENTATION ADVANTAGES FOR UTILITIES

NON-DISRUPTIVE DEPLOYMENT

Overlay Architecture: Implements over existing infrastructure without requiring network topology changes, IP reassignment, VLAN changes, or any other reconfiguration

Incremental Rollout: Can be deployed asset-by-asset or network-by-network

Legacy Protection: Provides security for systems that cannot be modified with traditional security controls

CONCLUSION: ARCHITECTURAL ADVANTAGE

SIMPLIFIED COMPLIANCE

Integrated Evidence: Access logs provide direct evidence of R1, R2, and R3 compliance

Risk-Based Implementation: Aligns with CIP-015-1 R1.1 requirement for risk-based rationale

Audit Readiness: Policy documentation and access logs provide clear compliance

Zero Trust Architectures don't just meet CIP-015-1 requirements. They *exceed them* by providing inherently superior capabilities for network security monitoring. By establishing explicit baselines through policy definition, providing immediate detection and prevention of unauthorized activity, and maintaining comprehensive logs with rich context, Zero Trust offers utilities a path to both regulatory compliance and enhanced operational security.

This architectural advantage becomes even more valuable as CIP requirements continue to evolve toward more comprehensive network monitoring and enforcement across increasingly complex and distributed utility environments.

TAKE THE NEXT STEP

Schedule a demonstration to see how Zentera's CoIP Platform can streamline your CIP-015-1 compliance and enhance grid security. Contact sales@zentera.net or visit www.zentera.net.

zentera

GLOSSARY OF TERMS

- **BES: BULK ELECTRIC SYSTEM**

  The interconnected power grid infrastructure.
- **ERC: EXTERNAL ROUTABLE CONNECTIVITY**

  Network connections allowing communication outside the ESP via routable protocols (not through an intermediary system).
- **ESP: ELECTRONIC SECURITY PERIMETER**

  The logical boundary protecting BES Cyber Systems
- **EACMS: ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS**

  Systems like firewalls that control or monitor ESP access.
- **PACS: PHYSICAL ACCESS CONTROL SYSTEMS**

  Systems managing physical access to critical assets (e.g., electronic locks, badge readers).
- **INSM: INTERNAL NETWORK SECURITY MONITORING**

  Monitoring network traffic within the ESP to detect anomalies.
- **COIP (CYBER OVER IP) PLATFORM**
  Zentera's patented security platform that provides a software-defined overlay to isolate critical assets, enforce Zero Trust policies, and enable secure communication.
- **VIRTUAL CHAMBER**
  A logical network boundary within the CoIP Platform that isolates assets and enforces access control policies in accordance with Zero Trust principles.
- **ZERO TRUST ARCHITECTURE**
  A security framework that requires verification of every user, device, and process attempting to access resources, regardless of their location.
- **ZTNA (ZERO TRUST NETWORK ACCESS)**
  A security model that grants access to applications and data only after verifying the identity, context, and security status of users and devices.
- **zLINK**
  Zentera's agent software that is installed on endpoints to enforce access control policies and manage secure connections within the Virtual Chamber.

ABOUT ZENTERA SYSTEMS

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, the company offers award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or in the cloud. Global enterprises use Zentera's products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. The Silicon Valley-based company has received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.