VIEW POINT

NERC CIP-015: MONITORING DEEP INSIDE CRITICAL NETWORKS TO KEEP ADVERSARIES OUTSIDE

AN INFOSYS GUIDE TO UNDERSTANDING AND IMPLEMENTING NERC'S LATEST CRITICAL INFRASTRUCTURE PROTECTION STANDARD FOR ELECTRIC UTILITIES

Infosys®
Navigate your next

Executive Summary

The North American Electric Reliability Corporation (NERC) has introduced CIP-015-1, a new standard designed to enhance cybersecurity in the electric utility sector by mandating Internal Network Security Monitoring (INSM). This comprehensive guide, prepared by Infosys for internal and client use, outlines the critical components of CIP-015, implementation timelines, and strategic approaches to achieve compliance.

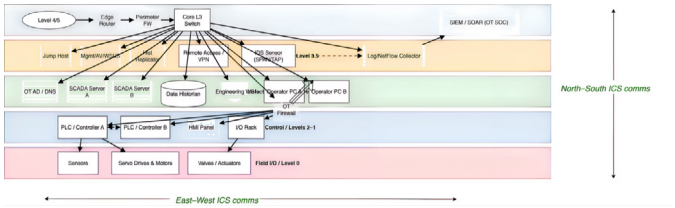
Core Requirements
CIP-015 mandates monitoring, detection, and analysis capabilities for network traffic inside Electronic Security Perimeters (ESPs), addressing a critical security gap in east-west traffic monitoring.

Implementation Timeline
High and Medium Impact Control Centers with External Routable Connectivity (ERC) must comply by October 1, 2028, while other Medium Impact facilities with ERC have until October 1, 2030.

Strategic Importance
This standard represents a significant advancement in electric sector cybersecurity, requiring utilities to detect adversarial activity that might otherwise remain hidden inside critical networks.

This guide will help Infosys teams and utility clients understand the requirements, technical considerations, and implementation strategies to successfully meet CIP-015 obligations and enhance overall security posture.

Understanding the Need for CIP-015

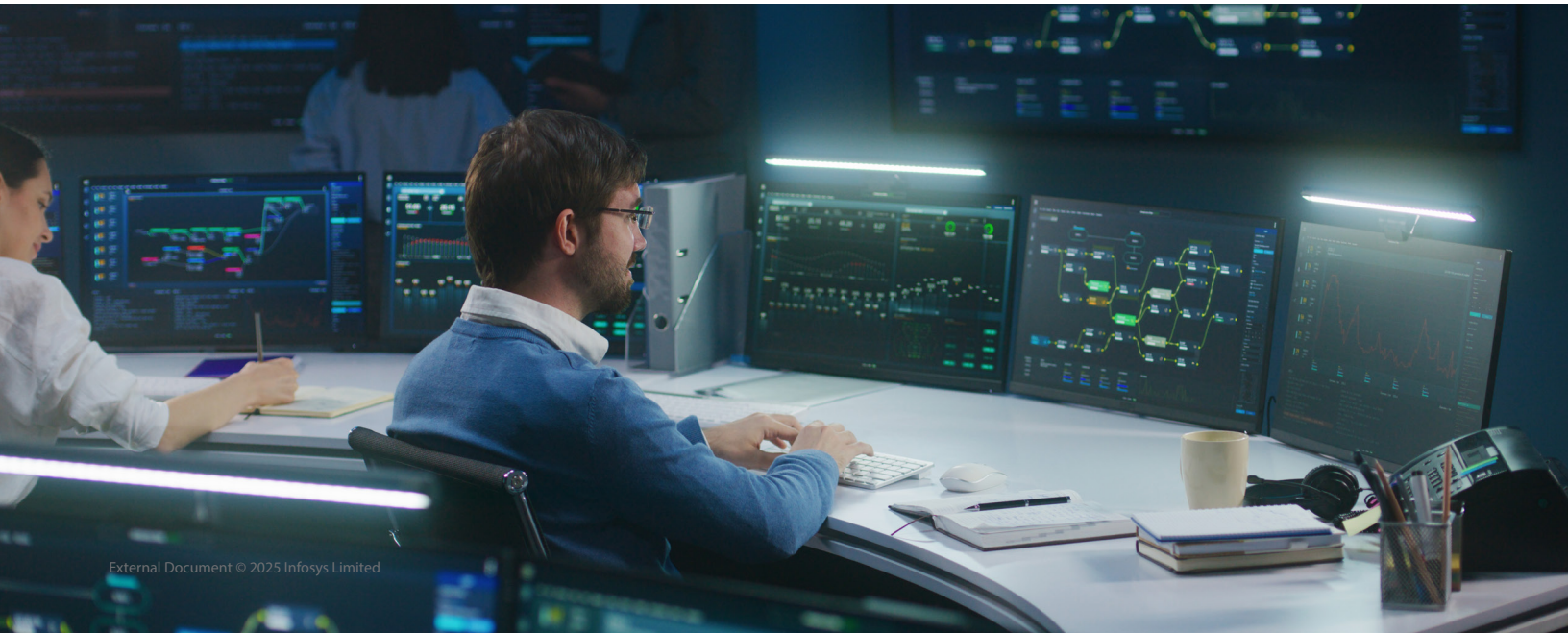


The existing NERC CIP Standards have focused primarily on preventive controls to establish Electronic Security Perimeters (ESPs) and control communications in and out of these perimeters (north-south traffic). However, adversaries have demonstrated the ability to bypass these controls and maintain persistence within operational networks.

To address this security gap, FERC directed NERC to develop new standards focused on monitoring network traffic inside protected networks (east-west traffic), leading to the development of CIP-015.

FERC Order 887 specifically called for the industry to address three key security objectives:

- Establish baselines of internal operational network traffic
- Monitor and detect unauthorized activity within the internal operational network
- Log network traffic in a manner that minimizes the likelihood of an attacker destroying or modifying the traffic



FERC's Role in Driving CIP-015

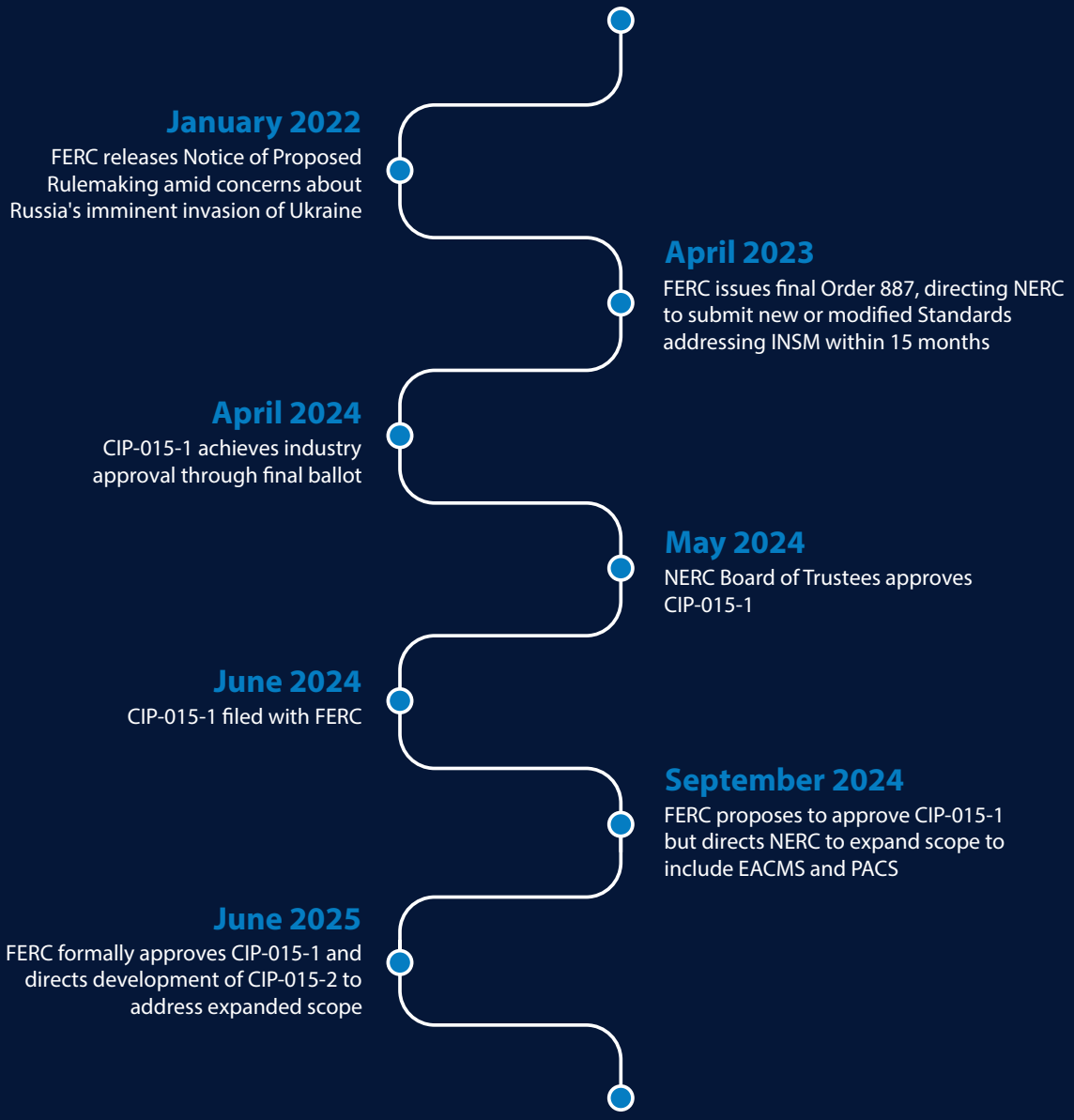
The Federal Energy Regulatory Commission (FERC) plays a pivotal role in identifying cybersecurity gaps and directing new standards development. For CIP-015, this process began in early 2022 amid growing concerns about potential Russian cyber threats related to the invasion of Ukraine.

While NERC CIP standards were originally voluntary when first developed in 2003, they became mandatory and enforceable through the Energy Policy Act of 2005. The standards development process remains collaborative, with asset owners and operators as primary authors, but FERC can direct specific changes based on assessed risks.

FERC Order 887, which became effective April 10, 2023, specifically directed the development of standards for Internal Network Security Monitoring (INSM) to address concerns about adversaries using living off the land (LotL) techniques and the need for expanded detective controls.

This directive represents FERC's recognition that existing standards were not sufficient to detect sophisticated threat actors who might establish persistence within critical infrastructure networks.

The Long Road to CIP-015 Approval



The lengthy development timeline ensures industry input but results in regulatory lag—often 3-8 years from identification of a security gap to mandatory implementation. For Infosys clients, this creates both challenges and opportunities in planning and implementation.

CIP-015-1 Implementation Timeline

NERC has established a staggered implementation timeline for CIP-015-1:

October 1, 2028

Effective date for High and Medium Impact Control Centers with External Routable Connectivity (ERC)

October 1, 2030

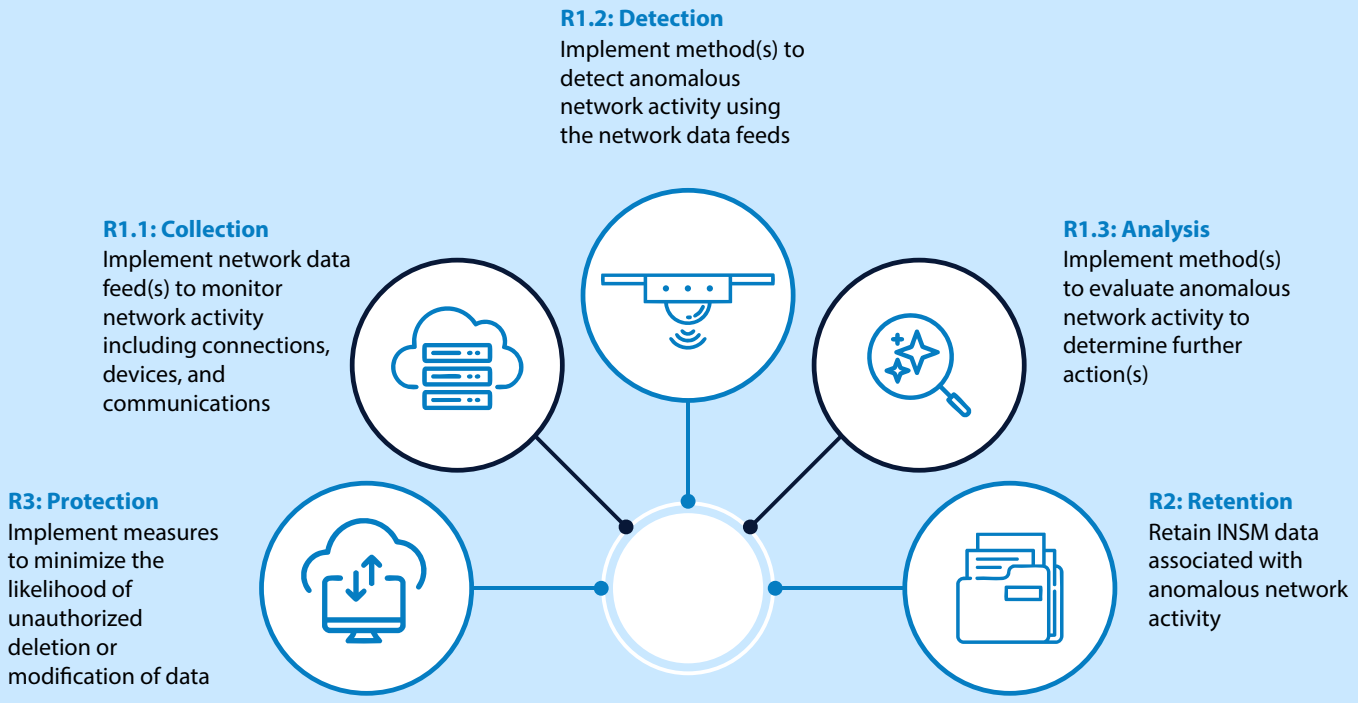
Effective date for other Medium Impact sites with ERC

The extended timeline acknowledges the significant effort required to implement these new capabilities across the electric sector. However, FERC has also directed NERC to develop CIP-015-2 within one year to expand the scope to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that reside outside the ESP.

This means utilities will need to begin planning now, even though compliance dates are years away. Infosys can help clients develop strategic implementation roadmaps that account for both current and anticipated future requirements.

Key Requirements of CIP-015-1

CIP-015-1 contains three primary requirements, with the first requirement divided into three sub-requirements that align with FERC's directive for a comprehensive Internal Network Security Monitoring approach.



These requirements represent a significant advancement in cybersecurity for electric utilities, moving beyond traditional perimeter defense to comprehensive internal monitoring.

Requirement 1.1: Monitor Network Activity

Requirement 1.1 focuses on implementing network data feeds to monitor activity, including connections, devices, and network communications. This requirement demands a risk-based rationale for selecting which data feeds to monitor.

Key Implementation Considerations:

- Identifying appropriate data feeds will require collaboration between operations personnel, system engineers, and cybersecurity practitioners
- Teams must understand system-to-system data flows and operational requirements
- Network infrastructure must support the necessary traffic collection
- Collection points must be strategically placed to ensure comprehensive coverage
- Targeted traffic capture and aggregation capabilities are essential

The success of subsequent detection and analysis requirements depends on establishing effective monitoring capabilities in this first phase.

A comprehensive monitoring solution must capture connections, devices, and communications within the ESP

Requirement 1.2: Detect Anomalous Activity

Baseline Establishment

Create comprehensive baselines of normal network activity for all BES Cyber Systems

OT-Specific Detections

Implement detection capabilities designed for industrial control system environments

Behavioral Analytics

Deploy solutions that can identify abnormal patterns or the absence of normal patterns

Deviation Detection

Establish capabilities to identify deviations from operational system models

Requirement 1.2 demands that utilities leverage the network activity data collected under Requirement 1.1 to detect anomalous network activity. This moves organizations into a higher maturity model where they need complete understanding of normal network behavior.

Traditional IT detection rules may help identify some malware or adversary activity, but this requirement demands OT-specific capabilities. This will likely require new tools and solutions, along with expanded workforce training to utilize them effectively.

Infosys can help clients evaluate and implement solutions that provide comprehensive anomalous activity detection, tailored to their specific operational environment.

Requirement 1.3: Evaluate Anomalous Activity

After implementing monitoring and detection capabilities, Requirement 1.3 mandates the evaluation of any detected anomalous activity. This analysis phase requires a comprehensive approach that includes:

False Positive Assessment

Evaluate detections to determine if they represent actual threats or benign anomalies

Threat Intelligence

Use evaluation results to inform future threat intelligence and detection capabilities

Threat Hunting

Implement capabilities to identify latent attacker actions that may not trigger automated alerts

Incident Response

Interface with CIP-008 incident response processes when suspicious activity is confirmed

This requirement demands both technical solutions and trained personnel who understand OT environments and adversary techniques. Analysis processes and playbooks will be essential for consistent evaluation.

Requirement 2: Data Retention

Requirement 2 addresses FERC's directive for "maintaining logs and other data collected regarding network traffic." It specifically requires the retention of INSM data associated with anomalous network activity identified under Requirement 1.2.

Key Retention Considerations:

- Retention period must be sufficient to support the analysis process in Requirement 1.3
- Data retention must also align with CIP-008 incident response retention obligations if anomalous activity relates to a Reportable Cyber Security Incident
- Organizations must develop benchmarks for data rates, storage requirements, and performance timing
- Storage infrastructure must be sized appropriately based on expected detection rates and false positives

As organizations implement and tune their detection capabilities, they will need to adjust their retention strategies based on operational experience.

Efficient data retention systems must balance compliance requirements with practical storage limitations

Requirement 3: Data Protection

Requirement 3 addresses FERC's directive to minimize the likelihood of an attacker removing evidence to further evade detection or analysis. Unlike Requirement 2, which focuses only on anomalous activity data, Requirement 3 extends to all data used in the monitoring, detection, and evaluation processes.

Access Controls

Implement robust authentication and authorization mechanisms to prevent unauthorized access to INSM data

Data Integrity

Ensure mechanisms are in place to prevent modification of collected network activity data

Segregation

Consider separating monitoring systems from operational networks to reduce attack surfaces

Redundancy

Implement redundant storage for critical detection and analysis data

Organizations must develop technical solutions and processes that protect all data used in the performance of Requirements 1 and 2, ensuring that evidence of potential compromise cannot be easily destroyed or altered by attackers.

Technical Capabilities for CIP-015 Compliance

When evaluating technology solutions for CIP-015 compliance, utilities must consider how each solution addresses the core requirements. Infosys can help clients assess and implement appropriate technologies, such as the Dragos Platform, which offers comprehensive capabilities aligned with CIP-015 requirements.

CIP-015 Requirement	Base Compliance Capabilities	Enhanced Capabilities
R1.1: Monitor Network Activity	Multiple sensor deployments within the environment to support various collection capabilities	Expanded sensor architecture with common dashboards consuming multiple feeds and collection types
R1.2: Detection	Indicator and behavior detection capabilities, baseline deviation monitoring	Intelligence-driven detections with indicators, threat behaviors, modeling, and configuration monitoring
R1.3: Evaluation	Analyst threat detection dashboards showing detection types	Integration with playbooks, case management tools, and threat intelligence
R2: Data Retention	Collection and storage of network activity data feeds	Expandable storage with flexible retention periods
R3: Data Protection	Ingestion of data into secure platforms with multiple storage locations	Case management capabilities with custom retention requirements

Remember that technology alone is not sufficient—successful implementation requires a partnership between technology, trained personnel, and well-designed processes.

Four Types of Threat Detection

A comprehensive threat detection approach should incorporate multiple detection methodologies to provide defense in depth. Solutions like the Dragos Platform use four complementary detection types:

Behavioral Detection
Codifies malicious adversary tradecraft for detection regardless of specific indicators, focusing on TTPs identified with specific threat groups or tool sets

Configuration Detection
Alerts on deviations from known architecture or changes to established baselines

Indicators Detection
Identifies specific attributes or evidence known as indicators of compromise (IoCs) based on previously observed threat data

Modeling Detection
Defines normal behavior and measures against divergence to detect both malicious actions and failing assets

By integrating these four types of detection, organizations can enhance their ability to meet CIP-015-1 requirements while providing the context needed to evaluate detections effectively.

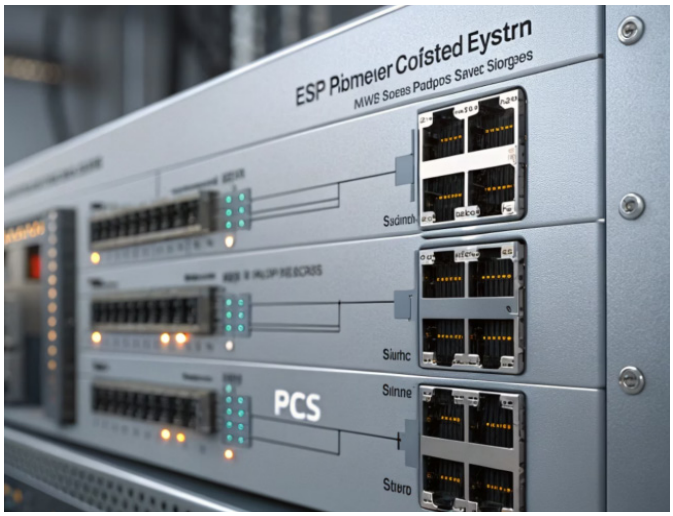
CIP-015-2: The Future Expansion

While CIP-015-1 has been approved, FERC has already directed NERC to develop CIP-015-2 to address an identified security gap. The key expansion in version 2 will be extending the scope beyond the Electronic Security Perimeter (ESP) to include:

- Electronic Access Control or Monitoring Systems (EACMS) located outside the ESP
- Physical Access Control Systems (PACS) located outside the ESP

FERC's directive states: "By restricting the implementation of INSM to within the electronic security perimeter, a reliability and security gap remains by not implementing INSM for the entire CIP-networked environment."

This expansion recognizes that compromise of systems outside the ESP can provide attackers with pathways into critical systems. NERC must develop and submit CIP-015-2 within 12 months of FERC's June 2025 order.



CIP-015-2 will require monitoring EACMS and PACS systems that reside outside the ESP

Implementation Timeline Uncertainties

With FERC's directive to develop CIP-015-2 before CIP-015-1 becomes effective, utilities face some uncertainty about implementation timelines. Historical precedents suggest several possible scenarios:

Direct to CIP-015-2
FERC could direct the industry to move directly to CIP-015-2, bypassing version 1 implementation (as happened with CIP v4 and v5 Standards)

Extended Implementation Timeline
CIP-015-2 could have a new implementation plan with compliance dates further out than the version 1 timeline with CIP v4 and v5 Standards)

Parallel Implementation
Utilities might need to implement CIP-015-1 for systems within the ESP by the original dates while preparing for additional requirements for systems outside the ESP

Despite this uncertainty, utilities now have significantly more clarity based on the approved CIP-015-1 Standard. Infosys recommends that clients begin planning now, focusing first on High and Medium Impact Control Centers with ERC, while maintaining flexibility to adapt to evolving requirements.

Implementation Strategy: Immediate Actions

While compliance deadlines may seem distant, utilities should begin taking action now to ensure successful implementation. Infosys recommends the following immediate actions:

Asset Inventory

Review current list of High and Medium Impact (with ERC) facilities to determine scope

Capability Assessment

Identify existing data collection capabilities within ESPs

Infrastructure Evaluation

Assess feasibility of performing network activity data feed collection from existing network infrastructure

Analysis Workflow

Identify where evaluation of detected anomalous activity would be performed

Solution Evaluation

Begin reviewing potential solutions that best fit your environment

By taking these steps now, utilities can develop a clear understanding of their current capabilities and the gaps that need to be addressed, allowing for more effective budget planning and resource allocation.

Implementation Strategy: Next Steps

Workforce Development

- Develop a comprehensive workforce plan addressing gaps in job roles and staffing levels
- Provide necessary training to develop individuals key to project and program initiatives
- Consider partnering with service providers like Infosys for specialized expertise

Technical Implementation

- Leverage existing test environments to evaluate solutions
- Configure solution detection capabilities for your specific environment
- Conduct active cybersecurity vulnerability assessments (CVAs) in test environments to validate detection capabilities

Process Development

- Develop processes supporting CIP-015-1 Requirements 1.1–1.3
- Establish playbooks and case management tools for anomaly evaluation
- Create data retention and protection procedures

Strategic Planning

- Prioritize projects across High and Medium Impact Control Centers with ERC
- Consider projects across other Medium Impact facilities with ERC
- Begin planning for expanded applicability to EACMS and PACS

Infosys can assist utilities in each of these areas, providing expertise in both technical implementation and process development. Our experience working with multiple utilities on CIP compliance gives us unique insights into effective implementation strategies.

Continuous Monitoring and Contribution

Beyond implementation, utilities should remain engaged with industry developments related to CIP-015. Infosys recommends the following ongoing activities:

Industry Participation

Engage in further industry activity on the directed changes from FERC to CIP-015-1, including participation in NERC drafting teams and commenting on proposed standards

Consistency Development

Work with industry peers on risk-based data feed selection approaches and consistent treatment of the term “anomalous” across entities

Regional Collaboration

Participate in Regional Entity collaboration and outreach efforts focused on CIP-015-1 implementation best practices

Incentive Programs

Consider pursuing early implementation under the FERC Order 893 incentive-based rate treatment for investment in advanced cybersecurity technologies

By actively participating in industry discussions, utilities can help shape the development of CIP-015-2 and ensure that implementation guidance reflects operational realities.

The Role of Partners Like Infosys

Implementing CIP-015 requirements will demand significant resources, expertise, and coordination across multiple disciplines. Partners like Infosys can provide valuable support throughout this journey:

Strategic Planning

- Gap analysis and roadmap development
- Budget planning and resource allocation
- Compliance program design

Technical Implementation

- Network architecture assessment
- Solution evaluation and selection
- Deployment and configuration
- Integration with existing systems

Process Development

- Detection and analysis workflow design
- Playbook development
- Documentation and evidence collection

Training and Support

- Staff augmentation
- Knowledge transfer
- Ongoing operational support
- Compliance readiness assessment

With experience across multiple utilities and deep expertise in both OT and IT environments, Infosys is well-positioned to help clients navigate the complex journey to CIP-015 compliance while enhancing their overall cybersecurity posture.

The Technology Landscape

Evaluating Solutions for CIP-015 Compliance

Key Capabilities for CIP-015 Solutions

When evaluating technology solutions for CIP-015 compliance, utilities should consider several key capabilities:

Packet Capture
The solution must be able to collect and analyze network traffic at various points within the ESP, supporting multiple protocols used in industrial control systems.

Network Visualization
Comprehensive asset discovery and relationship mapping capabilities help establish baselines and identify anomalous connections.

Protocol Analysis
Deep understanding of industrial protocols is essential for identifying anomalies in command sequences and parameters.

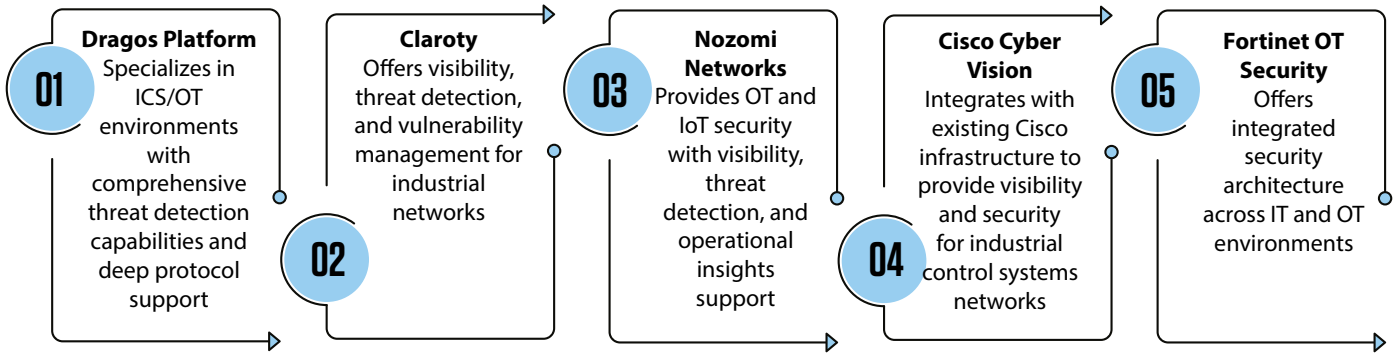
Anomaly Detection
Multiple detection methodologies should be supported, including behavioral, indicator-based, configuration, and model-based approaches.

Forensic Capabilities
Tools for investigating detected anomalies, including historical data access and context enrichment.

Secure Storage
Protected storage for collected data with controls to prevent unauthorized modification or deletion.

Infosys can help utilities evaluate solutions against these criteria and select the most appropriate technology for their specific environment.

Several vendors offer solutions that can support CIP-015 compliance. While specific vendor recommendations should be tailored to each utility's environment, leading options include:



Infosys maintains strategic partnerships with leading vendors and can help utilities evaluate and integrate these solutions based on their specific technical requirements, existing infrastructure, and security objectives.

Infosys 4D Approach for NERC CIP Security Compliance Management

Assess

Key Activities:

- Assess the organization's readiness for complying with NERC CIP requirements
- Discuss with the organization's stakeholders to get understanding of current security policy and processes
- Understand the current compliance framework and Identify and finalize control objectives and controls to be covered for NERC CIP
- Understand the metric and reporting requirements.
- Execute the sample controls testing
- Identify control gaps, document the same and recommend steps for remediation

Outcomes:

- Control framework (Control Objectives and Controls) mapped to NERC CIP
- Compliance Report with gaps if any

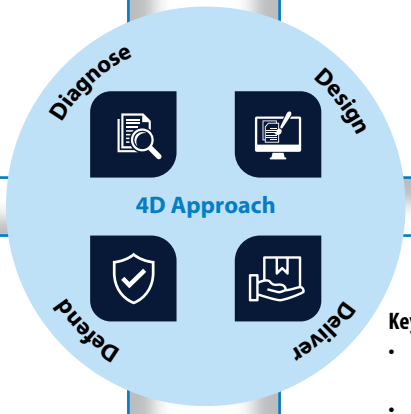
Analyze and Build

Key Activities:

- Design the Security Control Framework by considering NERC CIP requirements
- Agree and align with Stakeholders on the requirements of NERC CIP
- Create the compliance assessment plan
- Identify Security compliance KPI requirements
- Review RACI matrix for security & compliance standards
- Define plan for continuous compliance support and security risks management

Outcomes:

- The comprehensive Control framework
- Reporting template including KPIs and metrics



Continuous Support

Key Activities:

- Review non-compliance for violations as per KPI when required.
- Discuss & advise the remediation steps
- Annual Self Assessment for compliance requirements
- Support Security Compliance roadmap
- Report compliance violations, governance issues with a feedback for actions
- Manage and Track compliance gaps

Outcomes:

- Compliance reports & gaps tracking status
- Artefacts for reference

Apply

Key Activities:

- Implement the test once and compliance many methodology
- Execute out the compliance assessment and create a draft report along with finding and observations
- List applicable controls and evaluate their implementation gap
- Evaluate the identified gaps and prepare the report.
- Review assessment observations with stakeholders and receive inputs (if any)
- Share the final reports to concern stakeholders

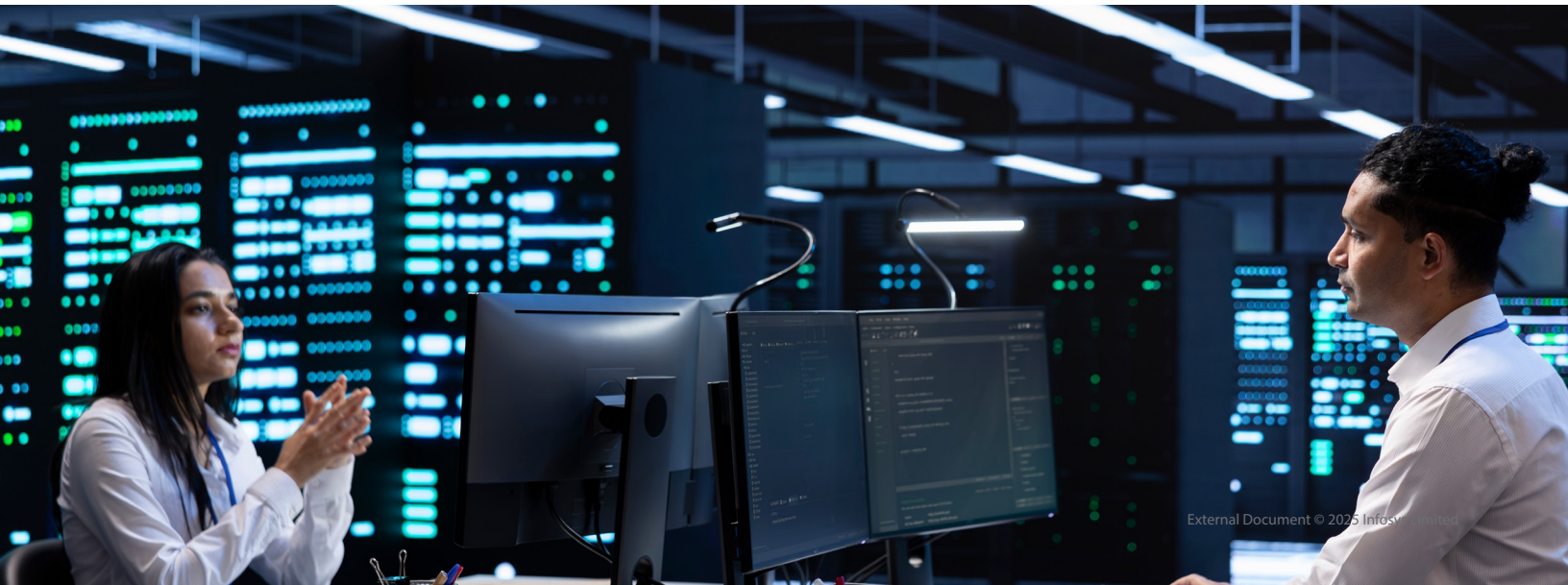
Outcomes:

- Assessment plan and compliance report
- Remediation Report

Infosys Approach to Deliver Services Compliant with NERC CIP

Given below are NERC CIP specific procedures that Infosys would propose:

NERC CIP Standard	Our Approach
CIP-002-5.1a: BES Cyber System Categorization	Infosys will use the existing BES Cyber Systems and their associated BES Cyber Assets at client.
CIP-003-8: Security Management Controls	Infosys will adhere to client's policies. A comprehensive list will be prepared based on Client's policies. Update access for BES Cyber Systems will be limited to onsite CIP certified personnel only.
CIP-004-6: Personnel and Training	Infosys will adhere to the detailed requirement as mentioned in the CIP requirements pertaining to personnel and training including the mandatory background checks and tests.
CIP-005-6: Electronic Security Perimeter(s)	Infosys will adhere to client's Electronic Security perimeter policies. A comprehensive list is prepared based on client's policies.
CIP-006-6: Physical Security of BES Cyber Systems	Infosys will adhere to client's Physical security policies.
CIP-007-6: Systems Security Management	Infosys will adhere to client's systems security policies. A comprehensive list will be prepared based on client's policies.
CIP-008-6: Incident Reporting and Response Planning	Infosys will adhere to client's Incident reporting and response policies. Infosys will work with client in reviewing and updating cyber security response plan as and when required.
CIP-009-6: Recovery Plans for BES Cyber Systems	Infosys will participate in testing and annual drills related to disaster recovery.
CIP-010-3: Configuration Change Management and Vulnerability Assessments	Infosys will adhere to client's policies and procedures for Configuration change Management and vulnerability assessments. Infosys will support the client in remediating the vulnerabilities identified and mitigate the risk.
CIP-011-2: Information Protection	Infosys will adhere to client's policies and procedures for Information Protection.
CIP-013-1: Supply Chain Risk Management	Infosys will adhere to client's Supply Chain Risk Management Framework.
CIP-014-2: Physical Security	Infosys will adhere to client's Physical policies and procedures.
CIP-015-1: Continuous Monitoring and Contribution	Infosys will support the client in Continuous Monitoring and Contribution



Conclusion: The Path Forward

The electric sector in North America has made consistent advances in cybersecurity capabilities and maturity over the past 20 years, but adversary capabilities have evolved as well. CIP-015 represents an important step forward in addressing sophisticated threats that can evade traditional perimeter defenses.

While the implementation timeline extends to 2028 and beyond, utilities should begin taking action now to:

- Understand the requirements and their implications
- Assess current capabilities and identify gaps
- Develop strategic implementation roadmaps
- Begin building the necessary technical and procedural foundations
- Stay engaged with industry developments and contribute to best practices

With proper planning and execution, CIP-015 compliance can enhance overall security posture and reduce the risk of successful attacks against critical infrastructure.

Implementation of CIP-015 will significantly enhance security for critical electric infrastructure

References

- https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
- https://www.ferc.gov/news-events/news/ferc-directs-new-cybersecurity-standards-internal-network-monitoring
- https://www.congress.gov/bill/109th-congress/house-bill/6
- https://www.nerc.com/comm/OC/RS/Pages/Internal-Network-Security-Monitoring.aspx
- https://www.dragos.com/blog/industry-news/ferc-order-887-internal-network-security-monitoring/
- https://www.sans.org/white-papers/ics/
- https://claroty.com/resources
- https://www.nozominetworks.com/resources/
- https://www.cisco.com/c/en/us/products/security/cyber-vision/index.html

About the Author

Michel Bruggeman,
Principal Cybersecurity Consultant | EMEA IoT & OT Lead

Michel is a distinguished cybersecurity leader with over 25 years of experience specializing in operational technology (OT) security, cyber resilience, and industrial cybersecurity architecture. He has held strategic roles across the insurance, manufacturing, energy, and semiconductor sectors, focusing on ICS/OT risk assessments, secure cloud adoption, and incident response readiness.

Michel is a SANS /ISA Mentor and Microsoft Certified Trainer, with deep expertise in IEC 62443, NIST, ISO 27001, DORA, and NIS2, and in his spare time he is a volunteer firefighter for more then two decades.

For more information, contact askus@infosys.com

Infosys®
Navigate your next