FORWARD TOGETHER RELIABILITYFIRST

# 2026 FALL RELIABILITY & SECURITY SUMMIT

## *TRACK 2: CRITICAL INFRASTRUCTURE PROTECTION (CIP)*

September 16, 2026

RELIABILITY FIRST

# 2026 FALL RELIABILITY & SECURITY SUMMIT


FORWARD TOGETHER RELIABILITYFIRST

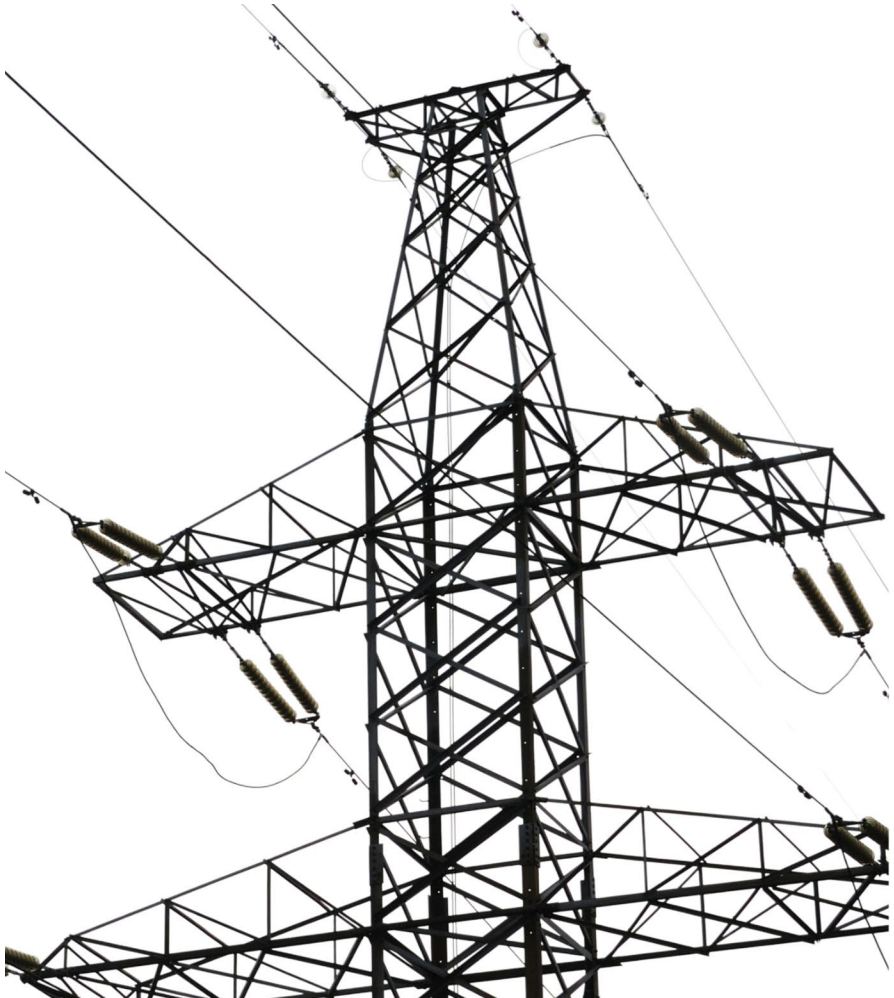
## Agenda

| | |
|---|---|
| 9:00-9:05 | **Welcome**<br>Lew Folkerth, Principal Reliability Consultant, External Affairs, ReliabilityFirst |
| 9:05-9:45 | **Cloud adoption and reliability: Insights from the Standards Drafting Team**<br>Lew Folkerth, Principal Reliability Consultant, External Affairs, ReliabilityFirst |
| 10:00-10:45 | **Supply chain risk management: Updates from the CIP-013 project 2025-06 Standard Drafting Team**<br>Natalie Fabian, Compliance Lead, Duke Energy |
| 11:00-11:45 | **CIP in practice: Lessons learned from real-world case studies**<br>Bridget McLean, Counsel, Enforcement, ReliabilityFirst |

# Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.



RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

# Project 2023-09 Risk Management for Third-Party Cloud Services

Drafting Team Update

September 16, 2026

**Lew Folkerth**
**Principal Reliability Consultant**
**ReliabilityFirst**

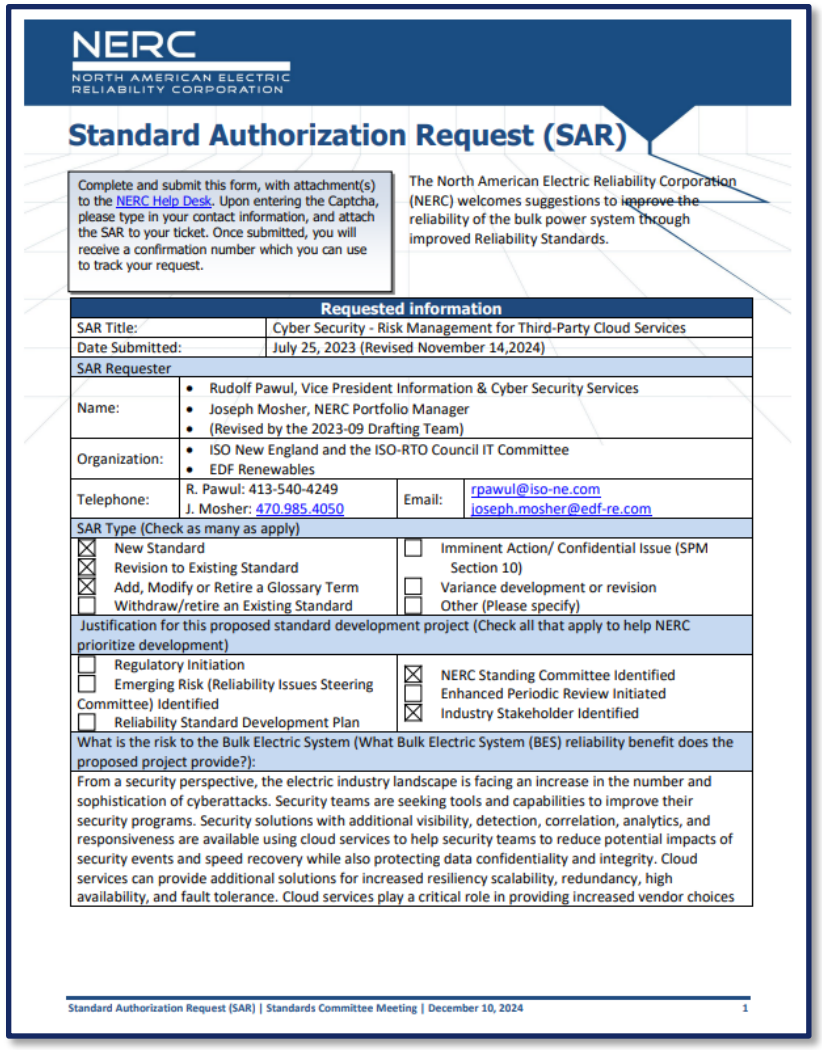
# Drafting Team

| Name | Entity |
|---|---|
| Matt Hyatt (Chair) | Georgia System Operations Corporation |
| Jay Cribb (Vice Chair) | Southern Company Services |
| Christopher Anderley | Great River Energy |
| Jeremy Lyon | Evergy |
| Lew Folkerth | ReliabilityFirst (RF) |
| David Dunn | ISO/RTO Council |
| Stephane Pellerin | Hydro-Quebec |
| Thad Ness | Florida Power & Light (NextEra Energy) |
| William Vesely | New York Power Authority (NYPA) |
| Monica Jain | Southern California Edison |
| Scott Klauminzer | Tacoma Public Utilities |
| Mikhail Falkovich | Microsoft |
| Bob Blackard | ERCOT |
| Frank Santoro | Consolidated Edison Company of New York |
| Sharon Koller | American Transmission Company, LLC |

# 2023-09 SAR Summary

**Cloud-based solutions are rapidly enhancing capabilities that could improve grid security and resiliency.**

- Must consider newly identified risks beyond the scope of the existing standards
- Consider prioritization of scope (EACMS first vs All-in)
- Flexible project scope required
  - Any/all CIP defined systems
  - Any/all CIP standards
- Seeks to minimize impacts on existing standards
- Advocates for Risk-based, outcome-driven requirements
- Consider how third-party certifications can be leveraged
- *Must allow but not require cloud use*



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Standard Authorization Request (SAR)**

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

| Requested information | | | |
|---|---|---|---|
| SAR Title: | Cyber Security - Risk Management for Third-Party Cloud Services | | |
| Date Submitted: | July 25, 2023 (Revised November 14,2024) | | |
| SAR Requester | | | |
| Name: | • Rudolf Pawul, Vice President Information & Cyber Security Services<br>• Joseph Mosher, NERC Portfolio Manager<br>• (Revised by the 2023-09 Drafting Team) | | |
| Organization: | • ISO New England and the ISO-RTO Council IT Committee<br>• EDF Renewables | | |
| Telephone: | R. Pawul: 413-540-4249<br>J. Mosher: 470.985.4050 | Email: | rpawul@iso-ne.com<br>joseph.mosher@edf-re.com |

SAR Type (Check as many as apply)

- ☒ New Standard
- ☒ Revision to Existing Standard
- ☒ Add, Modify or Retire a Glossary Term
- ☐ Withdraw/retire an Existing Standard
- ☐ Imminent Action/ Confidential Issue (SPM Section 10)
- ☐ Variance development or revision
- ☐ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

- ☐ Regulatory Initiation
- ☐ Emerging Risk (Reliability Issues Steering Committee) Identified
- ☐ Reliability Standard Development Plan
- ☒ NERC Standing Committee Identified
- ☐ Enhanced Periodic Review Initiated
- ☒ Industry Stakeholder Identified

What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks. Security teams are seeking tools and capabilities to improve their security programs. Security solutions with additional visibility, detection, correlation, analytics, and responsiveness are available using cloud services to help security teams to reduce potential impacts of security events and speed recovery while also protecting data confidentiality and integrity. Cloud services can provide additional solutions for increased resiliency scalability, redundancy, high availability, and fault tolerance. Cloud services play a critical role in providing increased vendor choices

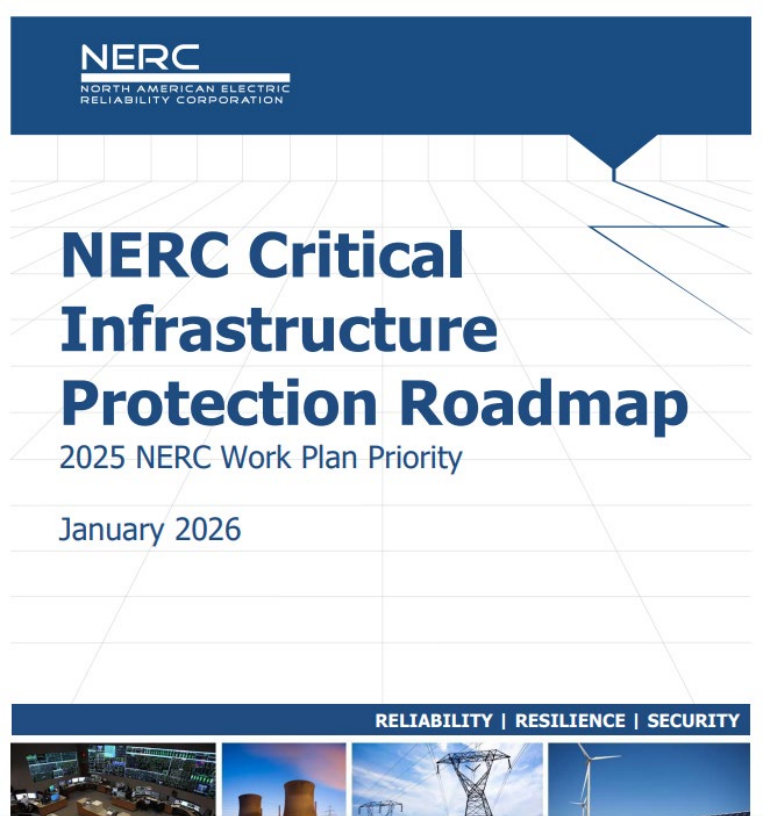
Standard Authorization Request (SAR) | Standards Committee Meeting | December 10, 2024 1

# Third party risks identified for CIP systems

- Procurement and supply chain
- Operational reliability and resiliency
- Communications to/from cloud environment
- Concentrated span of control
- Life-cycle considerations
- Key management
- Privatization
- Expanded attack surface
- Multi-tenancy / side-channel risks
- **Shared responsibility**
- Reliance on indirect services (sub-contracts)
- Data sovereignty / residency
- Regional considerations
- Blackstart scenarios
- Incident reporting
- Compliance and enforcement tasks
- Others as appropriate

# CIP Roadmap Updates

- Project 2023-09 specifically referenced as a priority and recommends a shift to high priority.
- Identifies cloud as offering enhancements to security and analytics platforms.
- Advocates for a risk-based approach regarding security objectives.
- *Project priority updated to "High" in February 2026*




Finally, cloud-native security solutions can offer enhanced visibility, detection, correlation, analytics, and responsiveness to help security teams reduce the potential impacts of security events and speed up recovery time. Additionally, cloud solutions can offer increased resiliency, scalability, high availability, and redundancy. The growing adoption of cloud-based systems designed to support grid operations is being seen predominantly in the spaces of big data analysis, AI, security tooling, IBR control systems, and distribution grid technologies. The application of cloud-based solutions also presents inherent challenges related to shared security responsibility between entities and cloud services providers; therefore, a measured regulatory solution should be risk-based and ensure that fundamental security objectives are met.

# White Paper


- Comment Period 12/18/2025 - 2/2/2026
- 45 sets of responses
- About 85 companies
- Representing 8 industry segments
- Mostly positive (93+%)
- Many constructive suggestions

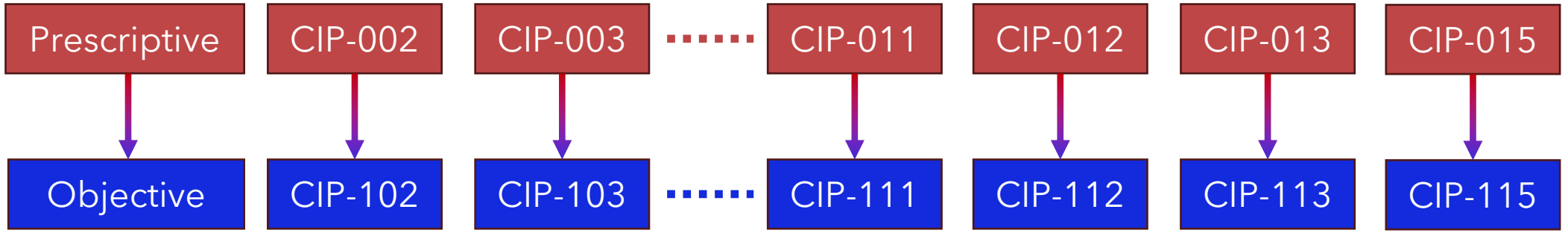
# White Paper Feedback

- *There is overwhelming agreement from industry (93%+) with the 100-series approach,* keeping the current CIP Standards relatively unchanged and developing the new series of CIP Standards to be implemented in parallel.
  - Further develop the 100-series approach to clarify the new structure and provide examples of how it will work.
  - Concerns with coordination between Drafting Teams; the 2023-09 drafting team should keep track of other CIP Standards under development and incorporate changes as needed.
  - Consider field trials before final approval.
  - Guidance is needed on risk-based objectives.
  - Commenters expressed concerns with keeping this parallel approach indefinitely and believe that a plan for retiring the 0-series standards should be part of the 100-series development. (Current SAR does not permit this change)

# What is the 100 series approach?

**A new series of parallel CIP standards would be developed with modified language and familiar numbering by topic.**

- Permit, but not require, cloud systems to be used with CIP standards
- Minimize changes - leverages existing standard language and structure
- Shifts existing language to risk-based objectives
- Provide flexibility to permit adoption of emerging technologies as needed
- Adoption of the 100-series standards would be opt-in, on a system-by-system basis
- First approach successful in satisfying rigor of the SMEs on the team



# How the two suites coexist

**Opt-in, system-by-system**

- Entities elect the 100-series for a given BES Cyber Service or System; systems not elected remain under the existing CIP standards
- No entity is forced to migrate; adoption follows need, such as a specific cloud use case

**CIP-002 is the surgical hinge**

- A single, highlighted change to CIP-002 applicability determines which suite governs a system
- No change to existing CIP-002 requirement language; applicability only

**Clean mutual exclusivity**

- Each system is governed by either the existing standards or their 100-series equivalent, never both
- Avoids double jeopardy and audit ambiguity between the two suites

# Device-based vs. service-based paradigm

- The existing CIP standards are effective for on-premise solutions and are based on the identification and protection of *devices*: "programmable electronic device."
- Cloud servers are based on *services* as a foundation and are currently broken into types such as Software as a Service(SaaS), Platform as a Service(PaaS), and Infrastructure as a Service(IaaS).
- Device-based standards cannot be applied reasonably to cloud-based services that are owned by 3rd party providers.

# Why now: The challenge of the status quo

**The device-based treadmill**

- Each new technology, such as virtualization, cloud, or otherwise has required its own SAR and another round of edits to device-based standards
- The result is continual change with no stable endpoint; complexity compounds with every cycle

**Bolting cloud onto the old model repeats the cycle**

- Mixing service-based and device-based language in one suite leaves industry unsure which requirements apply where
- The cloud market evolves rapidly; prescriptive, device-bound language cannot keep pace

**The 100-series represents a new path forward**

- Objective-based requirements absorb new technologies without a new SAR each time
- More change now buys an end to perpetual change later as future change can be focused on addressing security risks, not handling language complexity

# Location-based to function-based

- The 100 series standards focus on the functional role of technology, not where it is located.
- Existing CIP Standards are based on where technology is located, such as Substations, Plants, Control Centers, etc. The specific location of these assets often isn’t feasible in cloud-hosted systems.
- This shift addresses ambiguity of which systems are included or not. If they are a part of that identified functional operation of the bulk electric system, regardless of location, they need to meet the appropriate regulatory standards based on their impact rating.

# Risk-based objectives approach

- Treat **On-Premise** and **Cloud** equally, so the 100-series favors neither deployment model.
- Focus on addressing all existing and newly identified risks; including all security objectives from existing directives and orders.
- Shift to risk-based objectives; leveraging outcome-oriented language.
- Risk-based objectives will be more resilient to new technologies.

# System Security Plans (SSP)

**New concept in the 100-series standards**

- Promote alignment with other standards frameworks such as NIST
- Different requirements would “attach” to the SSP for a given “BES Cyber Service or System” with appropriate applicability for High, Medium, Low
- The CIP requirements would be objectives, or “what to accomplish” and would become a part of the SSP
- The SSP would be the basis of evidence for demonstrating compliance
- Would help define key concepts such as Shared Responsibility Models

# Summary of proposed changes

**CIP-002 – Identification & categorization**

- Applicability & mutual exclusion changes ensure no double jeopardy

**CIP-102 - Identification**

- Shift from Location-based to Function-based
- Retain existing brightline criteria for bulk electric systems

**CIP-103 - Governance**

- Establishes System Security Plan; vehicle for compliance evidence and establishing shared responsibility models throughout standards
- Removal of Low Impact Attachment; distributed as applicability to other standards as appropriate

**CIP-105 – System Protection**

- *Combines CIP-005 and CIP-007* into one System Protection standard
- Introduces vulnerability management concept

**CIP-113 – Supply Chain Risk Management**

- Added new supply chain risk assessment criteria to address cloud risks for procurement of Cloud Services

# Every Change Traces to the SAR

**Two categories of change**

- **Cloud-enabling:** removes a specific barrier that blocks a cloud use case today
- **Consistency:** the shift to objective language compels an aligned change to a related requirement

**In scope by design**

- The SAR directs risk-based, outcome-driven requirements that allow, but do not require, cloud use across CIP systems and standards
- Moving away from device-based language is a means the SAR contemplates and is a part of our scope

**Documented in the technical rationale**

- Each proposed change has specific TR developed to indicate why it is necessary

# How it works: A cloud-based control system example

**1. Identify (CIP-102)**

- A cloud-hosted control system function is identified as a “BES Cyber Service or System” and categorized by impact, with its associated supporting services identified.

**2. Apply the objectives (CIP-103-115)**

- The requirements state the expected security outcome to achieve, such as authorization or controlling and monitoring access, not a prescriptive device setting or activity.

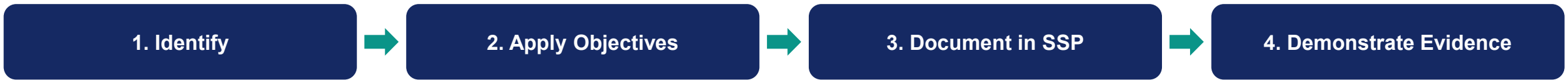
**3. Document the method in the System Security Plan (established in CIP-103, and referenced throughout)**

- The entity records how it meets the objectives in the SSP, including the shared-responsibility split between the entity and the provider

**4. Demonstrate with evidence**

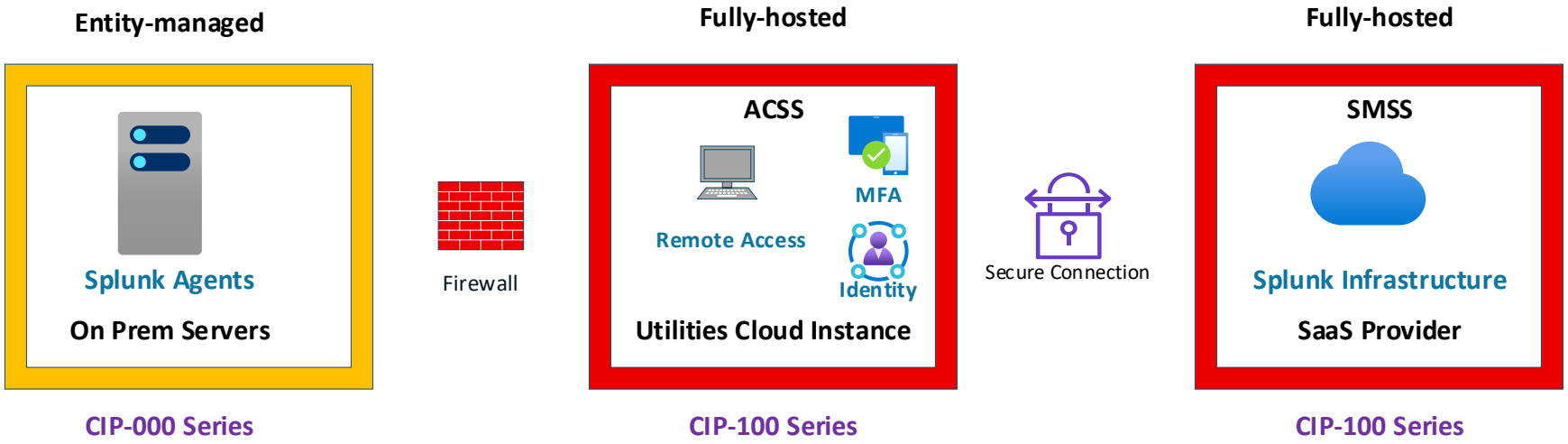
- Compliance is shown from the SSP, which may include the entities internal processes, capabilities, and provider attestations the entity obtains and evaluates (e.g., FedRAMP, SOC 2, ISO 27001), not a direct audit of the provider

***Bottom line: the auditor evaluates a documented plan and its evidence, consistently for on-premise and cloud systems***



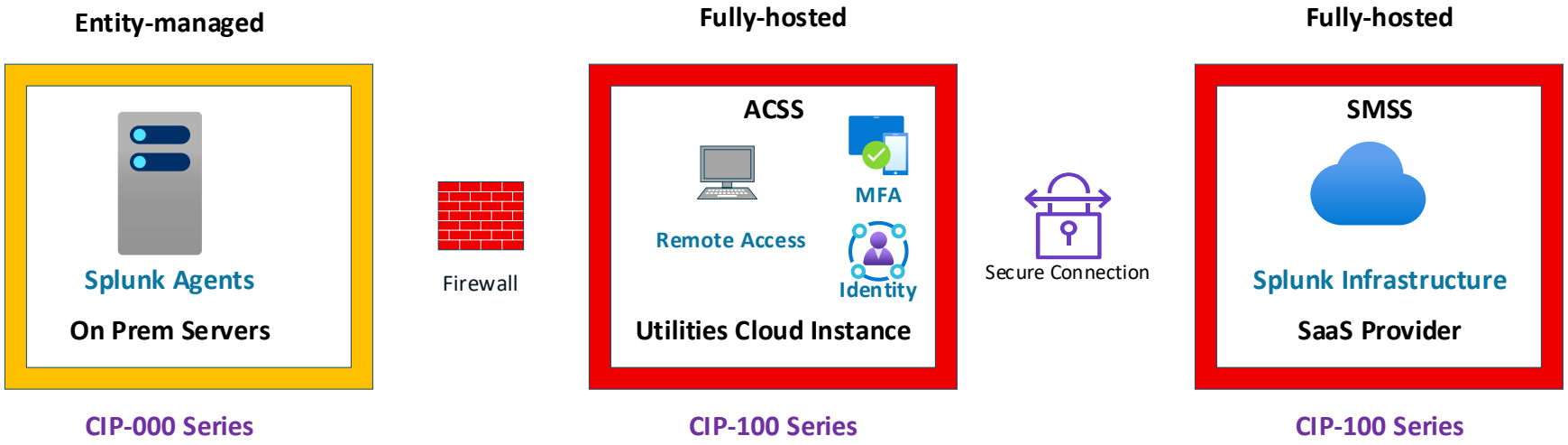
# Use case example – Cloud use case Splunk as SaaS

# Section 3: Cloud use case Splunk as SaaS



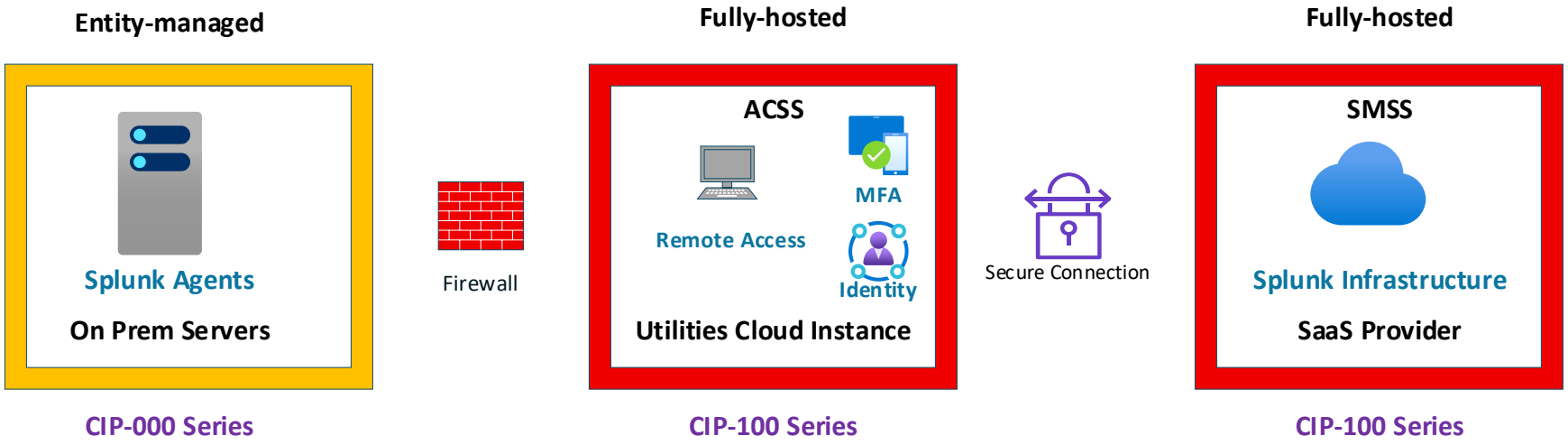

1. **Entity on premises servers**
   - Entity-managed/CIP-000 Series or CIP-100 Series (entity choice)
2. **Two tiers of the Shared Responsibility Model**
   - Fully-hosted/CIP-100 Series
   - Infrastructure as a Service (IaaS) (Remote Access, Identity, MFA)
     - Access Control Services and Systems (ACSS)
   - Software as a Service (SaaS) (Splunk)
     - Security Monitoring Services and Systems (SMSS)

# Section 3: Cloud use case Splunk as SaaS




1. **Entity-managed on prem servers**
   - Follow CIP-000 Series or move to CIP-100 Series your choice
   - CIP-005-7
     - Electronic Security Perimeter (ESP)
2. **System Security Plan (SSP)**
   - If the entity follows CIP-000 Series for entity-managed servers/services, they do not need to be included in SSP
3. **SaaS Provider (Splunk Infrastructure)**
   - CIP-113-1 Contract
   - CIP-104-1 Application layer accounts that the entity controls
   - Disclaimer this is not a complete list of applicable CIP standards

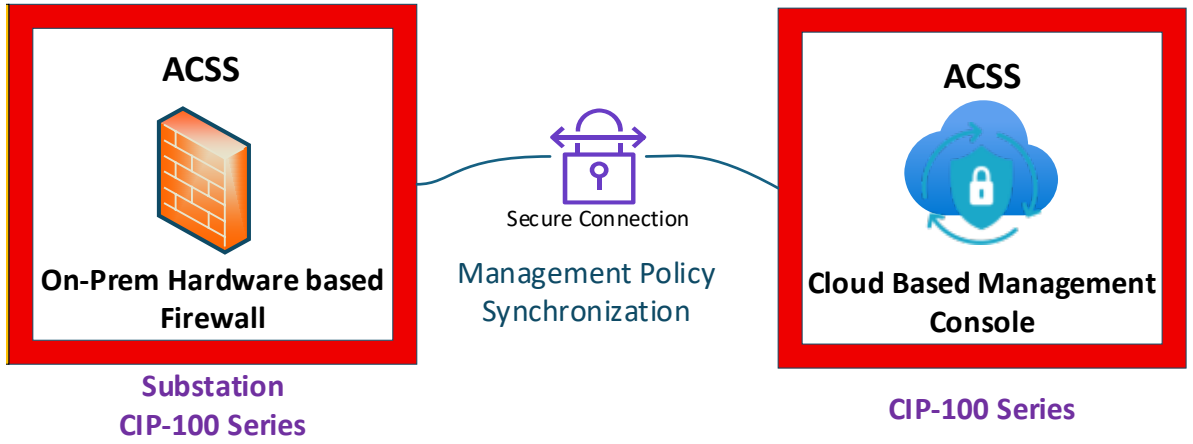
# Section 3: Cloud use case Splunk as SaaS




1. **Infrastructure as a Service (Entity's 3rd Party Cloud Provider)**
   - **CIP-113-1 Contract**
   - **CIP-103-1**
     - **Access Control Services and Systems (ACSS)**
   - **CIP-105-1**
     - **Conduit**
     - **Cyber Security Zone (CSZ)**
   - **Disclaimer this is not a complete list of applicable CIP standards**

# Use case example – Cloud-based hybrid firewall (Substation)

# Section 3: Use cases – Cloud-based hybrid firewall (Substation)



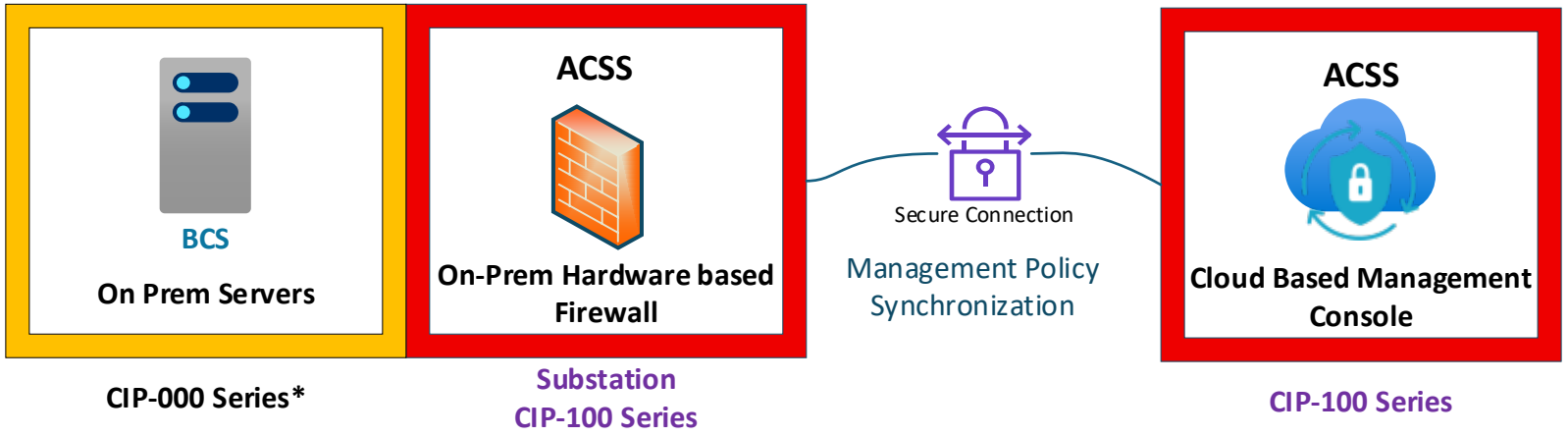

1. *On premise firewall (ACSS) managed by cloud service = 100 Series*

2. *Secure connection to management console = conduit*

3. *Management console (ACSS) 100 Series*
   - *Coordinated controls and evidence per CIP-103 addressing objective of entire 100 Series*

   *+ Risk Assessment needs under CIP-113*

# Section 3: Use cases – Cloud-based hybrid firewall (Substation)




1. *On premise firewall (ACSS) managed by cloud service = 100 Series*

2. *Secure connection to management console = conduit*

3. *Management console (ACSS) 100 Series*
   - *Coordinated controls and evidence per CIP-103 addressing objective of entire 100 Series*

   *+ Risk Assessment needs under CIP-113*

# Section 3: Use cases – Cloud-based hybrid firewall (Substation)

**1. Identify (CIP-102)**

- A cloud-hosted hybrid firewall (with on-premise component controlled through cloud management) is identified as an "Access Control Services and Systems (ACSS)" and associated by impact to a BCSS that it supports

**2. Apply the objectives (CIP-103-115)**

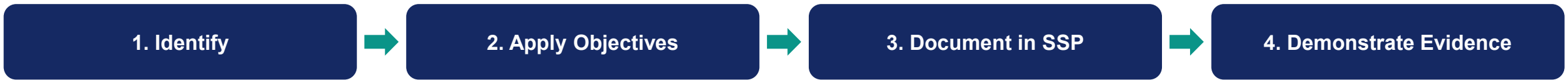
- Identify all Requirements that apply to an ACSS (either directly or through the ABSS definition)

**3. Document the method in the system security plan (established in CIP-103, and referenced throughout)**

- Document specific controls, responsibilities, and what evidence will be provided within the SSP

**4. Demonstrate with evidence**

- Evidence must show implementation of controls that the responsible entity performs through direct evidence, as well as implementation of controls that the CSP performs through indirect evidence such as audit reports (SOC 2 Type II, ISO-27000 Certification, etc.)

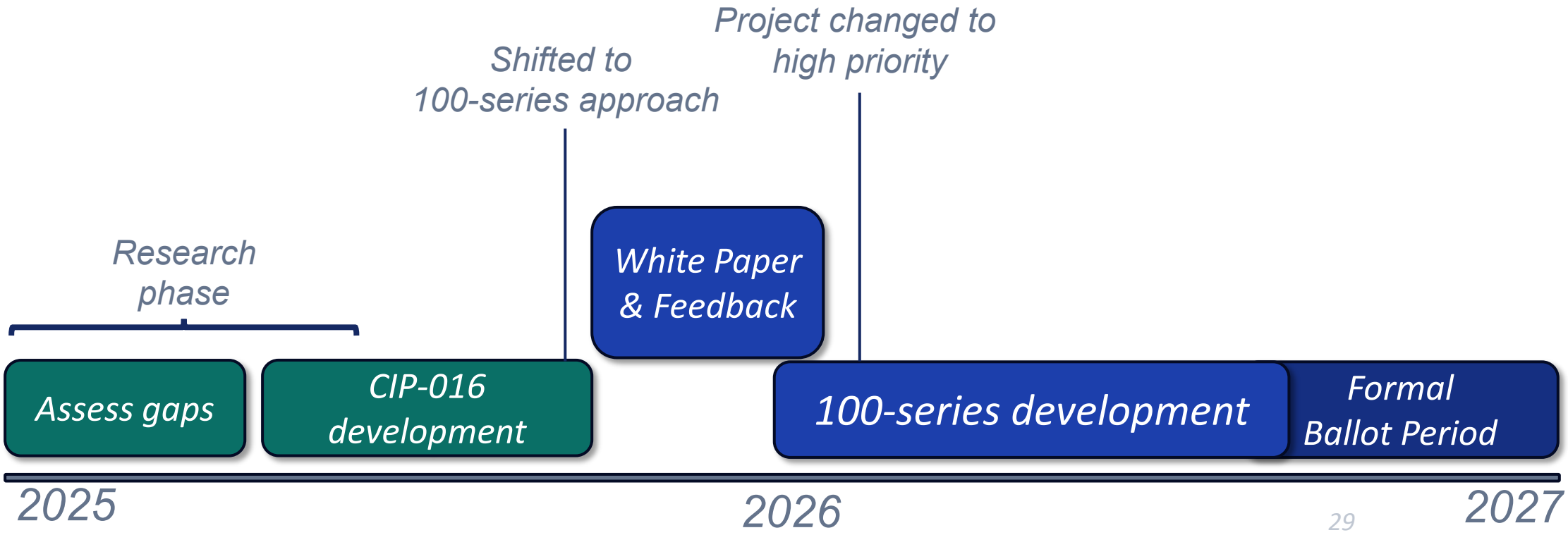


# Project 2023-09 development timeline

***Commissioned to start writing in January of 2025***

***Early research and first attempt focused on CIP-016 approaches***

***Shifted focus to 100-series in August of 2025; White paper confirmed industry support***



# Work products currently under development

- Informal posting for the following standards, Implementation Plan, and Technical Rationale:
  - CIP-002 – Includes mutual exclusion language
  - CIP-102 – Includes identification/definition updates
  - CIP-103 – Includes governance focused objectives
  - CIP-105 – Includes network/system focused objectives
    - Includes a combination of security objectives from CIP-005 and CIP-007
  - CIP-113 – Includes supply chain focused objectives
- Implementation Plan for 100-series
- Technical Rationale for each standard

# Next Steps

- Twice-weekly three-hour virtual meetings
- Leverage sub-teams “divide and conquer model” to accomplish more work in less time
- Webinar and informal posting on CIP-102 (Identification), CIP-103 (Governance), CIP-105 (Network/System Security), and CIP-113 (Supply Chain) to get feedback on approach
- Pending industry agreement, work to complete 100-series suite and formal posting.

# Resources

Project 2023-09 page

White Paper

CIP Roadmap

# Questions and Answers

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

# 2025-06 Project Update

## Changes to CIP-010-6 Configuration and Change Management and Vulnerability Assessments and CIP-013-4 Supply Chain Risk Management

(Revisions to current CIP-010-5 and CIP-013-3 under Project 2025-06)

**Natalie Fabian: DT Member, Duke Energy**
**Jessica Harris: NERC Standards Developer**

**September 2026**

# Purpose & Regulatory Basis (FERC Order 912)

**Regulatory Basis**

In FERC Order 912, the Commission identified gaps in the existing CIP-013-3 standards related to how Responsible Entities identify, reassess, and respond to supply chain cyber risks, including explicit protections for Protected Cyber Assets (PCAs).

**Project Objective**

Project 2025-06 updates CIP-010-5 and CIP-013-3 to implement the directives in FERC Order 912, while preserving flexibility for each Responsible Entity to design and maintain a supply chain risk management program and configuration and change management and vulnerability assessments appropriate to its individual risk profile and operating environment.

**Scope of Revisions**

The proposed modifications focus on strengthening risk identification and reassessment, documenting defensible risk-based decisions, and extending appropriate protections to PCAs.

- Per footnote 2 of FERC Order 912, the Commission directed that PCAs be included within CIP-005-8 and CIP-010-5 (current as of 04/01/2026).
- CIP-005-8 already includes PCAs and does not require modification.
- CIP-010-5 will require conforming updates to reflect PCA inclusion in Part 1.3.

**Priority and Direction**

This is a FERC-directed, high-priority project with a required completion date of May 21, 2027.

# Status, Next Steps & Industry Engagement

**Current Status**

- The initial ballot for CIP-010-6 and CIP-013-4 has concluded and the formal comment period has closed.
- The Drafting Team is reviewing industry comments and refining the draft requirements.
- Currently, the revised Standard packet will be open for comment in mid-October, with a 30 day comment period, with a formal ballot/comment period running from December 1 to December 10, 2026.

**What's Next**

- Revise draft standards to respond to comment themes, including pre-deployment reassessment intervals, emergency repairs, and periodic reassessment expectations.
- Post the revised drafts for an additional comment period and ballot.

**Continued Outreach & Engagement**

- Targeted industry outreach, including a Webinar (details to come), continues through the next ballot period to validate direction and resolve concerns early.

# FERC Order 912 Directives

| FERC ORDER 912 Directives |
| --- |
| fn2. In this notice of proposed rulemaking, the term SCRM Reliability Standards includes Reliability Standards CIP-005-7 (Electronic Security Perimeter(s)), CIP-010-4 (Configuration Change Management and Vulnerability Assessments), and CIP-013-2 (Supply Chain Risk Management). |
| p. 26 Standards that would establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks; NERC should establish (1) a maximum time frame between when an entity performs its initial risk assessment during the procurement process and when it installs the equipment and (2) periodic requirements for an entity to reassess the risk associated with vendors, products, and services procured under any contracts for supply chain risks that may have developed or changed since the contract commenced. |
| p. 29 Clarify that the directive here already includes reassessment of spare equipment and emergency repairs. |
| p. 32 that establish a maximum time frame between when a responsible entity performs its initial vendor and equipment risk assessment during the procurement process and when it deploys the equipment. If a responsible entity does not deploy the equipment or software within the specified time limit, the new or modified Reliability Standards should require responsible entities to perform an updated risk assessment prior to deployment. |
| p. 53 require responsible entities to establish a process to document, track, and respond to all identified supply chain risks; that existing SCRM Reliability Standards are inadequate to ensure consistent, timely, and appropriately documented responses to identified vendor risks. |
| p. 63 include PCAs as applicable assets |
| p. 69 to develop and submit for Commission approval new or modified Reliability Standards within 18 months of the effective date of this rule. |

# Ballot Results for CIP-010-6 and CIP-013-4

## Initial Ballot Summary

- Total votes cast: 244 of a 271-member ballot pool.
- Quorum: 90.04%.

## Weighted Segment Vote

- CIP-010-6: 64.55%.
- CIP-013-4: 30.64%.

## What This Tells Us

- Quorum was strong, but neither standard reached the two-thirds approval threshold.
- CIP-013-4 drew substantially more opposition, concentrated in the new risk assessment timing requirements.
- Comments received are driving targeted revisions ahead of the next posting.

# What Is Changing Under CIP-013-4

**Shift in focus to include Product-Based Risk Assessments**

- CIP-013-4 clarifies that supply chain risk management is also focused on products and services, rather than solely on vendors.
- Risk assessments are performed for specific products, software, and services, including spare equipment and emergency repairs.

**Mandatory Risk Reassessments**

- CIP-013-4 introduces explicit requirements to reassess supply chain risks, including:
  - Reassessment prior to deployment when prior assessments are no longer current, and
  - Periodic or event-driven post-deployment reassessments when supply chain risks may have changed.

**Why This Matters**

- These changes ensure supply chain risks are continuously evaluated across the system lifecycle, rather than assessed only at initial procurement.

# Comment Themes: Pre-Deployment Risk Reassessments (R1.3)

**Common Concerns**

- The proposed 24-month (high impact) and 36-month (medium impact) reassessment intervals were too short or confusing.
- Equipment procurement delays frequently exceed the proposed timelines, producing reassessments with little added security benefit.
- Many commenters asked that reassessments remain risk-based rather than strictly calendar-based.

**Drafting Team Updates:**

- The Drafting Team has reached a consensus that risk assessments and re-assessments must not exceed 36 months for either medium or high impact BES Cyber Systems or its related systems (EACMS, PACS, etc).
- A more detailed R1.3 has been drafted, with clarification around expectations, including “when the clock starts” for assessments or re-assessments.
- The Drafting Team is developing requirement language that preserves each Responsible Entity’s discretion to determine whether and when a product assessment or reassessment is warranted, and to define the role of vendor assessments and reassessments within that determination.

# Comment Themes: Emergency Repairs

**What Industry Told Us**

- Emergency restoration activities should never be delayed by compliance requirements.
- Entities need explicit authority to perform risk assessments after deployment during emergencies.
- Many commenters requested adding a CIP Exceptional Circumstance (CEC) provision.

**Drafting Team Updates:**

- The Drafting Team will not explicitly include CEC provisions, but language around CEC provisions may be included in footnotes.
- The Drafting Team will not define emergency repairs or spare equipment but will leave that up to the individual Responsible Entity to define and include the associated expectations within its documented supply chain cyber security risk management plan(s) or other procedures.
- Entities should be prepared to demonstrate that risk assessments associated with emergency deployments were completed in accordance with their plan(s), including the timing and rationale applied.

# Comment Themes: Document, Track and Respond (R1.5)

**Requested Clarifications**

Several commenters recommended clarifying what entities are expected to document, including:

- Risk disposition
- Mitigation
- Compensating controls
- Acceptance rationale
- Completion of response actions

**Drafting Team Consideration**

- Reviewing whether these expectations belong in requirement language or are better addressed in the Technical Rationale, so R1.5 stays outcome-based and auditable.
- The intent of R1.5 is that a Responsible Entity can demonstrate a traceable path from each identified supply chain risk to its disposition, whether that is mitigation, a compensating control, or documented risk acceptance. This can include risk mitigations the Responsible Entity is already doing.
- Entities retain flexibility in how this documentation is structured.
- The expected evidence is a record showing that identified risks were tracked through to completion of the associated response actions.

# Comment Themes: Periodic Reassessments (R1.4)

**Requested Clarifications**

- How often reassessments must occur.
- When the first reassessment is due.
- Whether reassessments apply only to active contracts.
- How the requirement interacts with implementation dates.

**Drafting Team Update**

- Additional clarification and details around when R1.4 would apply and how it would apply in conjunction with R1.1 and R1.3.
- Clarification will address how R1.4 interacts with the R1.1 procurement assessment and the R1.3 pre-deployment assessment, so that a single assessment can satisfy overlapping expectations rather than triggering duplicate work.
- The Technical Rationale is also being updated to clarify how the requirement applies to vendors, products, and services that no longer have an active contract, allowing entities to define reassessment criteria in their plan(s).

# VSL Changes and Implementation Plan

NERC

**Violation Severity Level (VSL) Updates**

- VSLs were reviewed and updated to ensure appropriate differentiation between:
  - Documentation-related deficiencies and
  - Failures to implement required processes
- Implementation failures generally align with higher VSLs than documentation-only issues, consistent with NERC VRF/VSL criteria, and FERC VSL Guidelines Issues
- **Drafting Team update:** Some changes were necessary after balloting to ensure consistency across VSLs and VSPs.

**Reliability Standard CIP-010-6 and CIP-013-04**

- Due to comments, the Drafting Team is updating the Implementation Plan become effective on the first day of the first calendar quarter that is twenty-four *(24)* months after approval of the standard.

**Performance Expectations**

- CIP-013-4 Part 1.3 and Part 1.4 risk assessments are not required prior to the effective date of the standard
- Protected Cyber Assets (PCAs) procured prior to the effective date do not require a Part 1.1 supply chain risk assessment under CIP-013-4

# Expanded Measures

The Drafting Team is considering incorporating expanded Measures that provide illustrative examples and additional direction to Responsible Entities.

The Drafting Team recognizes that Measures are not independently enforceable for compliance purposes; nevertheless, the revised Measures and the accompanying Technical Rationale are intended to provide clarity and guidance to Responsible Entities.

**Example – CIP-013-4 Table R1, Part 1.3.1**

| Part | Applicable Systems | Requirements | Measures |
|---|---|---|---|
| 1.3.1 | High Impact BES Cyber Systems and their associated EACMS, PACS, PCAs, and SCI<br>Medium Impact BES Cyber Systems and their associated EACMS, PACS, PCAs, and SCI | A risk assessment or risk reassessment shall be completed no later than 36 months after the most recent risk assessment or reassessment. | Examples of evidence may include, but are not limited to:<br>A reassessment performed in response to a known vulnerability and completed within the preceding 36 months.<br>A documented risk assessment performed pursuant to another CIP Requirement.<br>A record listing the dates of the assessments and reassessments performed within the preceding 36 months. |

NERC

# Discussion

# Point of Contact

- Point of contact
  - Jessica Harris, NERC Sr. Standards Developer
  - Jessica.Harris@nerc.net

  - Natalie Fabian, Drafting Team Member
  - Natalie.Fabian@duke-energy.com

# CIP IN PRACTICE

## *LESSONS LEARNED FROM CASE STUDIES*

**Bridget McLean, Counsel, Enforcement**

ReliabilityFirst Fall Summit
Columbus, Ohio – September 16, 2026

RELIABILITY FIRST

FORWARD TOGETHER RELIABILITYFIRST

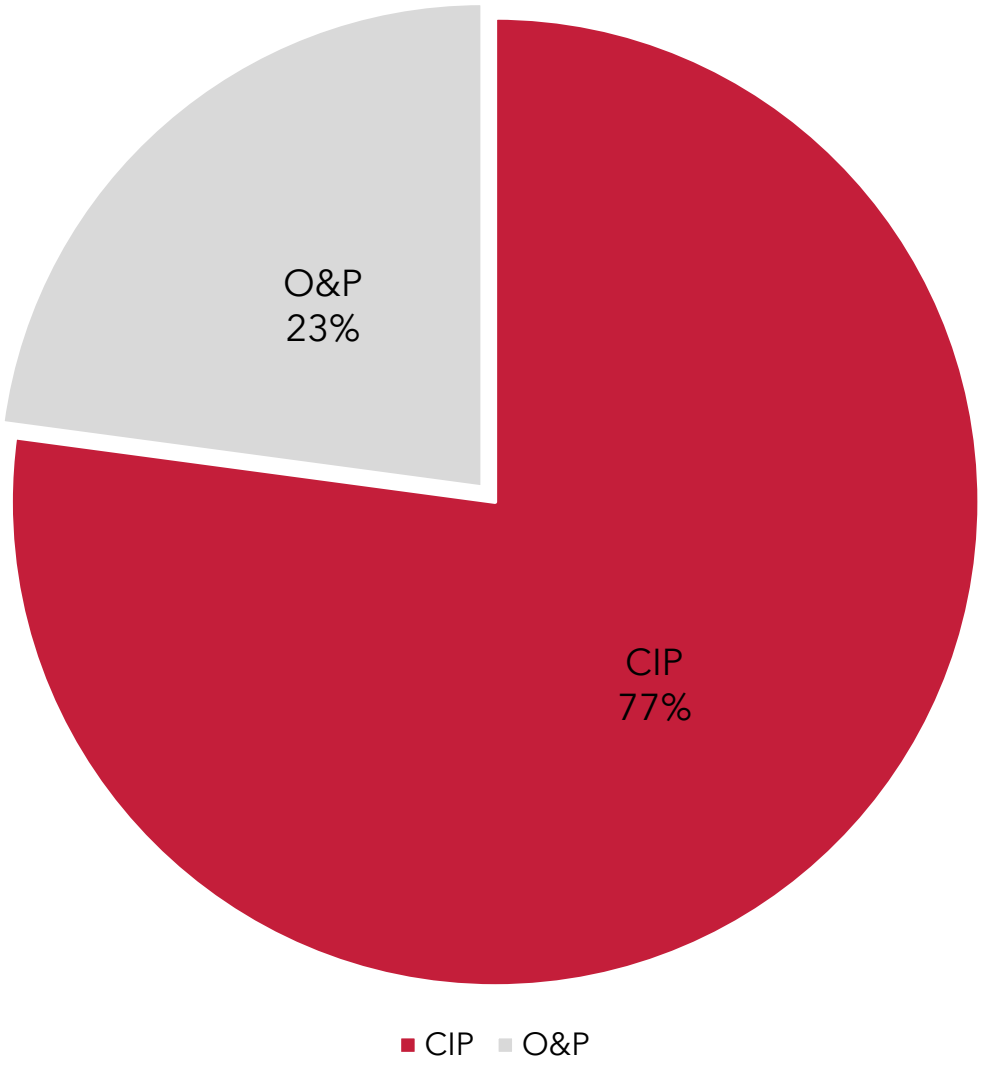
# AGENDA

- OVERVIEW OF ENFORCEMENT
- CIP METRICS
- CASE STUDIES
- QUESTIONS AND ANSWERS

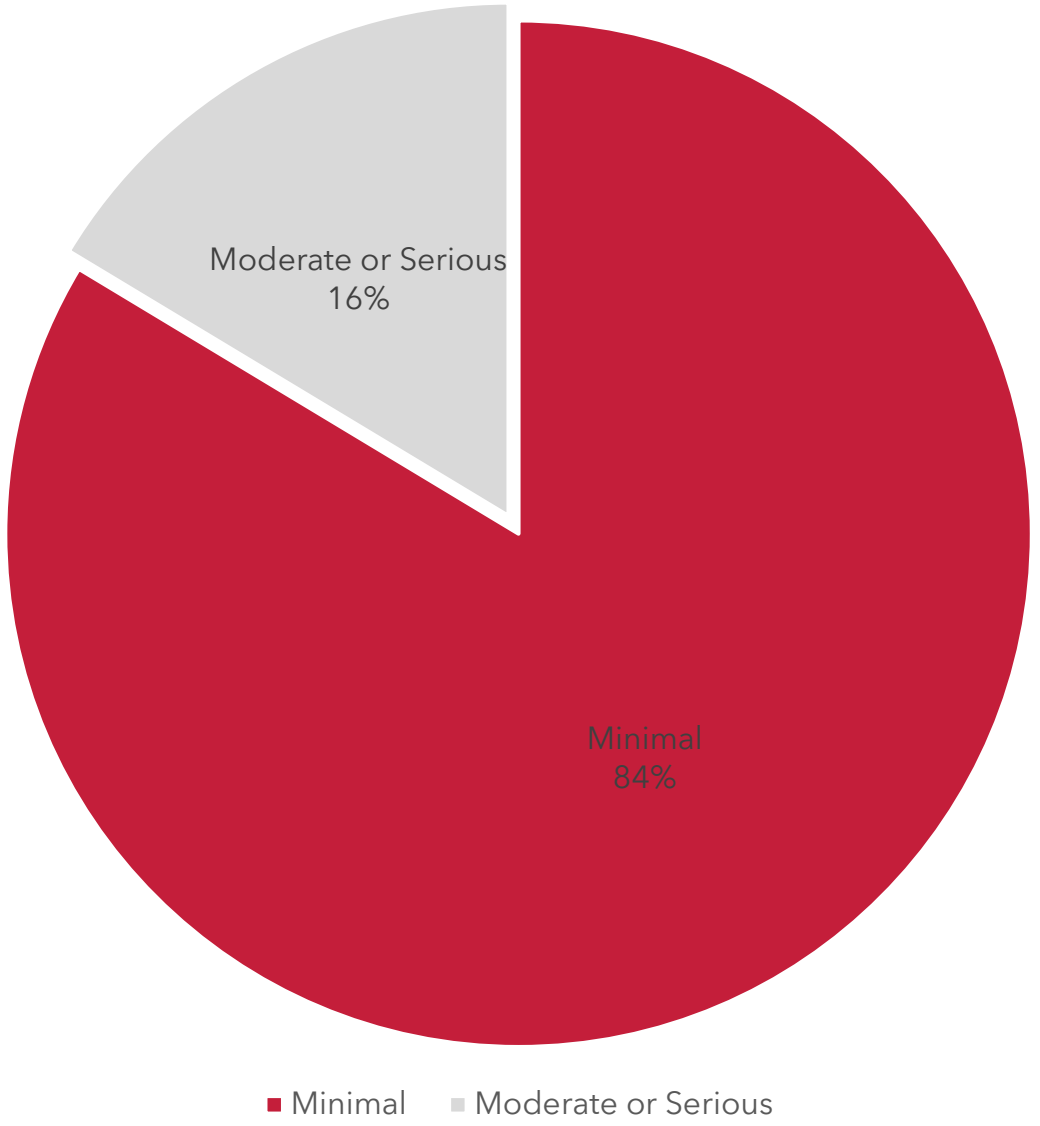
# ENFORCEMENT
## ROLES AND RESPONSIBILITIES

- Identify, understand, and define the risk surrounding each violation in concert with Subject Matter Experts (SMEs).
- Ensure that each violation is mitigated
- Send the appropriate message to the entity and broader regulated community

# CIP METRICS
## REPORTED VIOLATIONS



# CIP METRICS
## RISK DISTRIBUTION



# CIP METRICS

## MOST FREQUENTLY VIOLATED STANDARDS

1. CIP-010: Configuration Change Management and Vulnerability Assessments
2. CIP-007: System Security Management
3. CIP-004: Personnel and Training
4. CIP-006: Physical Security of Bulk Electric System (BES) Cyber Systems
5. CIP-003: Security Management Controls

# CASE STUDY 1
## ARTIFICIAL INTELLIGENCE

- Standard and Requirement: CIP-011-3 R1

- Facts: A SME wants to use a third-party Artificial Intelligence (AI) service to troubleshoot an issue with several BES Cyber Assets (BCA). The SME creates an anonymized document solely for the purpose of uploading to the AI service. The SME uploads the version of the document with the actual BES Cyber System Information (BCSI) for BCAs to the AI service.

- Summary of Noncompliance: Under most circumstances, the entity's Information Protection Program prohibits off-site storage of BCSI.

# CASE STUDY 1
## ARTIFICIAL INTELLIGENCE

- Risk Level: Minimal
- Disposition Track: Compliance Exception
- Risk Statement: Improper handling of BCSI could allow an adverse actor to access the information and use it to the detriment of the Bulk Power System.

# CASE STUDY 2
## BCSI ACCESS

- Standard and Requirement: CIP-004-7 R6

- Facts: The entity implemented a new system. As part of the roll out, the entity provisioned access to electronic BCSI for 42% of the entity's CIP-scoped devices to 500 personnel. The entity only intended to provision electronic access to the BCSI to 200/500 of the personnel. The entity did not detect the noncompliance for 7 years.

- Summary of Noncompliance: The entity failed to follow its documented access management program prior to authorizing access to BCSI for 42% of the entity's CIP-scoped devices to 300 people.

# CASE STUDY 2
## BCSI ACCESS

- Risk Level: Moderate
- Disposition Track: Settlement Agreement
- Risk Statement: The risk of failing posed by granting unauthorized personnel access to BCSI is that the unauthorized personnel may leverage their access to the detriment of the BPS.

# CASE STUDY 3
## STALE FIREWALL RULESETS

- Standard and Requirement: CIP-005-7 R1.3

- Facts: The entity identified that it had not been consistently removing obsolete firewall rulesets for four years. As a result, the entity allowed unnecessary communications to and from systems.

- Summary of Noncompliance: The entity failed to sufficiently limit inbound and outbound access because it failed to remove 21 outdated firewall rulesets.

# CASE STUDY 3
## STALE FIREWALL RULESETS

- Risk Level: Moderate
- Disposition Track: Find, Fix, Track (FFT)
- Risk Statement: The risk of failing to adequately control inbound and outbound access permissions is that a malicious actor could leverage overly broad or outdated permissions to the detriment of the BPS.

# CASE STUDY 4

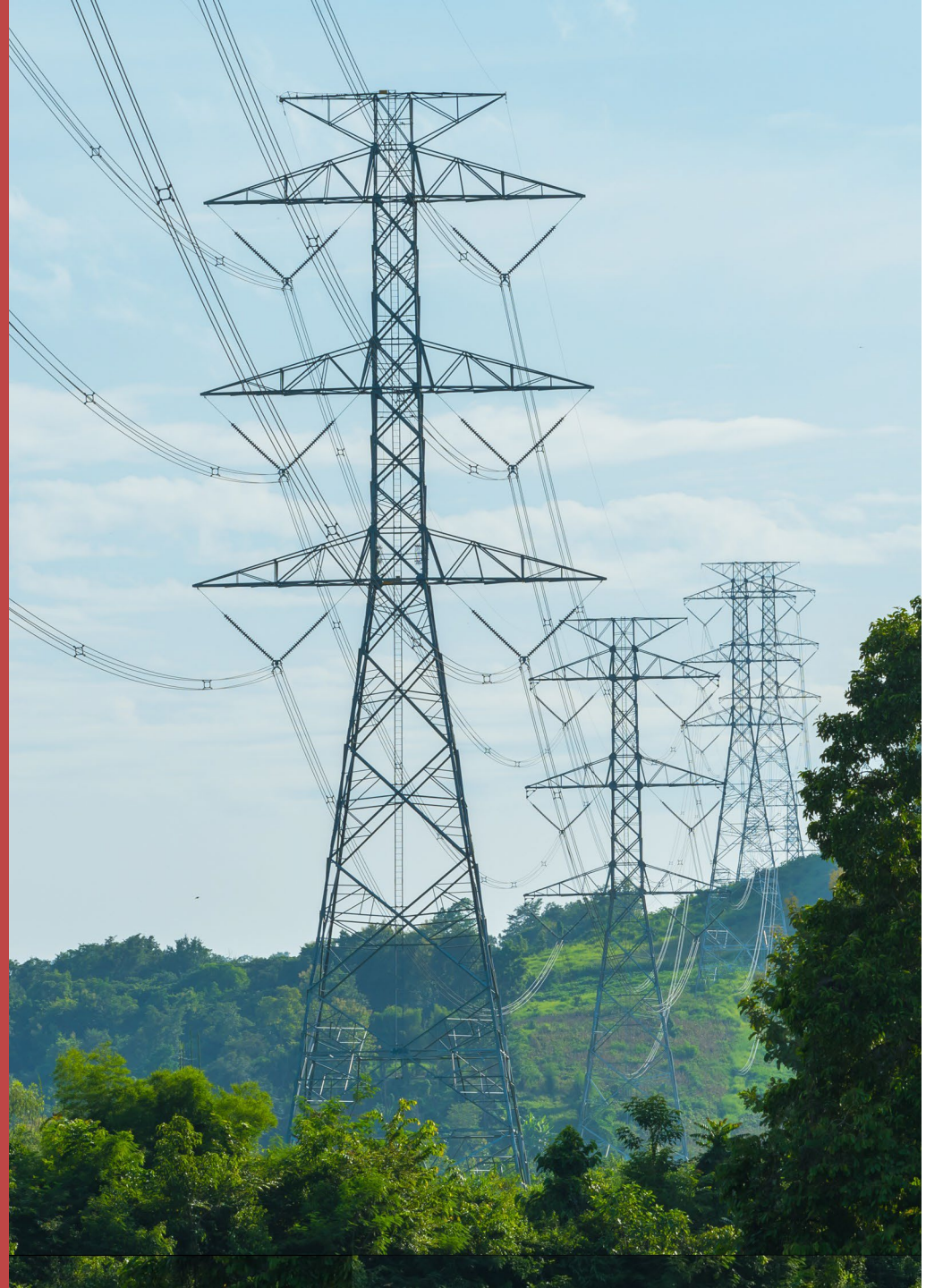
## IDENTIFICATION FAILURE WITH DOWNSTREAM IMPACTS

- Standard and Requirement: CIP-002-5.1a R1
- Facts: The entity commissioned a new substation, and it failed to identify 10 medium impact BCAs. Because the entity failed to identify the BCAs, it also failed to implement its patching program (CIP-007 R2); develop baselines (CIP-010 R1); and manage electronic access (CIP-004). The entity did implement some CIP protections including logging and alerting (CIP-007 R3), password protection mechanisms (CIP-007 R5) and physical access controls (CIP-006).
- Summary of Noncompliance: The entity's failure to identify 10 devices as medium impact BCAs led to noncompliance with three other CIP standards for seven years.

# CASE STUDY 4

## IDENTIFICATION FAILURE WITH DOWNSTREAM IMPACTS

- Risk Level: Moderate
- Disposition Track: Settlement Agreement
- Risk Statement: Entities must properly identify and categorize each BES Cyber System in accordance with its impact on the reliable operation of the BES for application of appropriate protective measures and enforcement of proper Reliability Standards to ensure continued reliable operation of the BES.



# QUESTIONS & ANSWERS

Bridget McLean

bridget.mclean@rfirst.org

# 2026 FALL RELIABILITY & SECURITY SUMMIT


FORWARD TOGETHER RELIABILITYFIRST

## Agenda

| | |
|---|---|
| 9:00-9:05 | **Welcome**<br>Lew Folkerth, Principal Reliability Consultant, External Affairs, ReliabilityFirst |
| 9:05-9:45 | **Cloud adoption and reliability: Insights from the Standards Drafting Team**<br>Lew Folkerth, Principal Reliability Consultant, External Affairs, ReliabilityFirst |
| 10:00-10:45 | **Supply chain risk management: Updates from the CIP-013 project 2025-06 Standard Drafting Team**<br>Natalie Fabian, Compliance Lead, Duke Energy |
| 11:00-11:45 | **CIP in practice: Lessons learned from real-world case studies**<br>Bridget McLean, Counsel, Enforcement, ReliabilityFirst |