Reliability & Security Workshop

WECC

March 17–18, 2026
San Diego, California

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

NERC

March 2026

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

Drafting Team Update
WECC Reliability and Security Workshop, San Diego, CA

Lew Folkerth, PE, LPI, +10
Principal Reliability Consultant, ReliabilityFirst

Lew’s Bio

49 years in electric utility industry

19 years full-time CIP

17 years with RF

5 years as CIP auditor

12 years outreach

60+ Lighthouse articles

Founder and lead of Cloud Technology Advisory Group (CTAG)

Selected for 2023-09 drafting team

Deep in ICS security – 2 licenses, 9 certifications, 1 certificate, 3 expired

Lew's Disclaimer

These slides are mine. Any errors or omissions are my fault.

If I express opinions, they are my opinions and not those of others.

I do not speak for the drafting team.

I do not speak for ReliabilityFirst.

I do not speak for NERC.

I do not speak for the Commission. Any Commission.

Outline

Introduction to Project 2023-09:

Risk Management for Third-party Cloud Services

The need for change

Early efforts

Change of direction

White paper and comments

CIP Roadmap

The path forward

Resources (How do I come up to speed?)

2023-09 SAR Key Points

- Cloud-based solutions are becoming essential to the purpose of keeping the electric grid secure
- Open project scope
  - Any/all CIP defined systems
  - Any/all CIP standards
- Minimize impacts on existing standards
- Must consider risks beyond the scope of the existing standards
- May take holistic or incremental approach
- Risk-based, outcome-driven
- Consider third-party certifications
- 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 • Joseph Mosher, NERC Portfolio Manager • (Revised by the 2023-09 Drafting Team)		
Organization:	• ISO New England and the ISO-RTO Council IT Committee • EDF Renewables		
Telephone:	R. Pawul: 413-540-4249 J. Mosher: 470.985.4050	Email:	rpawul@iso-ne.com 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

Drafting Team

NERC

Name	Entity
Matt Hyatt (Chair)	Georgia System Operations Corporation
Jay Cribb (Vice Chair)	Southern Company Services
Christopher Anderley	Great River Energy
Jeremy Lyon	Evergy
John Dirks	Salt River Project
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)

The Need for Change

- Software vendors, including services such as work management and network monitoring, are moving to cloud-based systems.
- On-premises systems such as endpoint detection and response (EDR) are becoming less capable and more expensive than cloud-based EDR solutions.
- Some smaller entities have implemented cloud-based GOP Control Centers. These entities continue to grow and are crossing the 1,500 MW threshold for medium impact.
- Some technologies, such as multi-factor authentication (MFA), are providing services using cloud-based applications. These cloud-based systems may prove to be more acceptable to their users than more traditional (token-based, etc.) approaches.

Device-based vs. Service-based

- The existing CIP standards are based on the identification and protection of devices: “programmable electronic device.” The cloud can be looked at as being largely service-based. Device-based standards cannot be applied to cloud-based services.
- The existing CIP standards rely heavily on network perimeter protection. This does not map well to cloud environments, where “identity is the new perimeter.”
- New methods of delivering software are being deployed in cloud environments, such as “serverless,” e.g., AWS Lambda, services.

First Efforts

July–December 2024

- Project 2023-09 at “Medium” priority
- Consideration of SAR comments
- Revised SAR
- Standards Committee approval of revised SAR

January–August 2025

- Work on fitting cloud considerations into existing standards with new standard for cloud (CIP-016)
- Too many changes to existing standards
- CIP-016 would be huge

Shift in Direction

NERC

August 2025

- First in-person meeting
- Revising existing standards determined to be too much of an uphill effort
- Developed concept of a new series of standards
  - Mapping but not duplicating existing standards
  - New standard for cloud-specific issues

September–November 2025

- Developed white paper describing new approach

December 2025

- Posted white paper for industry comment through 2/2/2026

Recent Events

NERC

January 2026

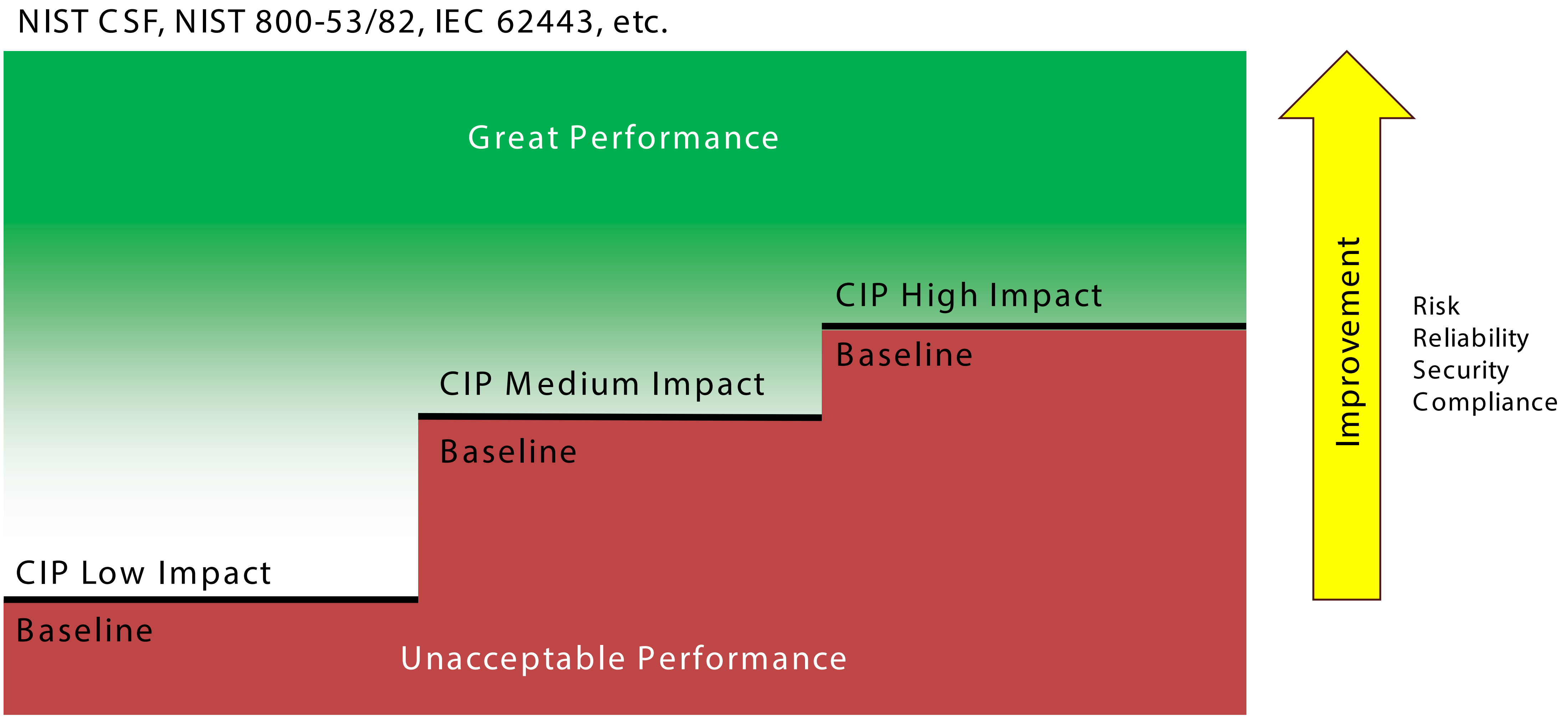
- In-person meeting scheduled for late February
- CIP Roadmap published
  - Recommends adjusting Project 2023-09 priority to “High”
- Project 2023-09 is now “High” priority
- Monthly in-person meetings
- Target date for posting initial ballot September 2026

Recent Events

February 2026

- Comments on white paper received and reviewed — very positive, many constructive suggestions
- In-person meeting
  - Detailed approaches — objective (outcome) based, risk-based system security plans
  - Sub-teams formed — network, system hardening, cloud-specific

CIP and Other Frameworks



White Paper


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

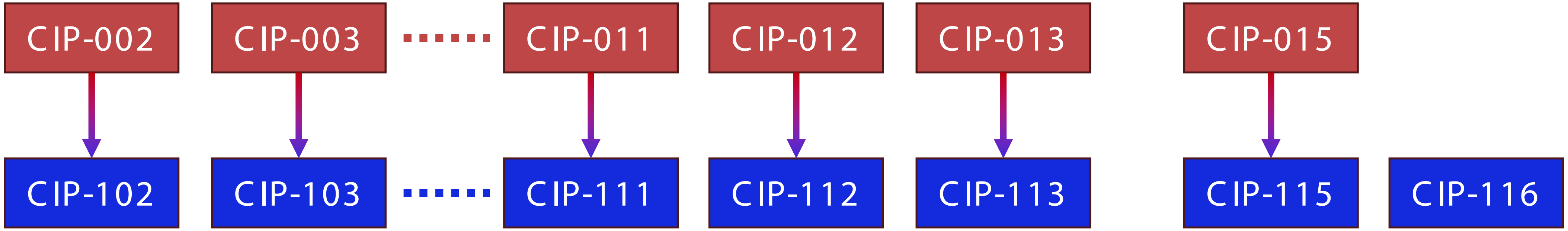
CIP & Cloud Services
A New Way Forward

Project 2023-09 Drafting Team

December 2025

- Published 12/18/2025
- Comments due 2/2/2026
- 45 sets of responses
- About 85 companies
- Representing 8 industry segments
- Mostly positive
- Many constructive suggestions

Approach



- Existing CIP standards will remain in place as untouched as possible
- The new 100-series standards will stand on their own – no reliance on the existing standards
- The 100-series standards will be objective-based
- The 100-series standards will permit cloud usage with appropriate controls
- The 100-series standards will be flexible to permit adoption of emerging technologies as needed
- The 100-series standards will use a risk-based System Security Plan approach
- Adoption of the 100-series standards will be on an opt-in, system-by-system basis

System Security Plan (SSP)

- The CIP requirements will be objectives, or “what to accomplish”
- The SSP will detail how the objectives are achieved
- Compliance evidence will demonstrate the execution of the SSP
- We are working on what this will look like — still in early stages

Implementation Options

NERC

Option 1: An entity can choose to remain subject to the existing CIP standard requirements as-is for all its systems that have no cloud component.

Option 2: An entity must use the new 100-series CIP standards for any systems that have cloud-based components.

Option 3: An entity can choose the 100-series standards for its on-premise cyber systems and its cloud-based services therefore maintaining a single compliance program.

Selected White Paper Comments

NERC

- There is overwhelming agreement 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.
- Many commenters are concerned about keeping this parallel approach indefinitely and believe that a plan for retiring the 0-series standards should be part of the 100-series development.
- The 2023-09 drafting team should keep track of other CIP Standards under development and incorporate changes as needed.
- Create a diagram of the 100-series approach to clarify the new structure and how it will work.
- Conduct field trials before final approval.
- Guidance is needed on risk-based plans.

CIP Roadmap

“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 cloudbased 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.”

-- CIP Roadmap, page 5

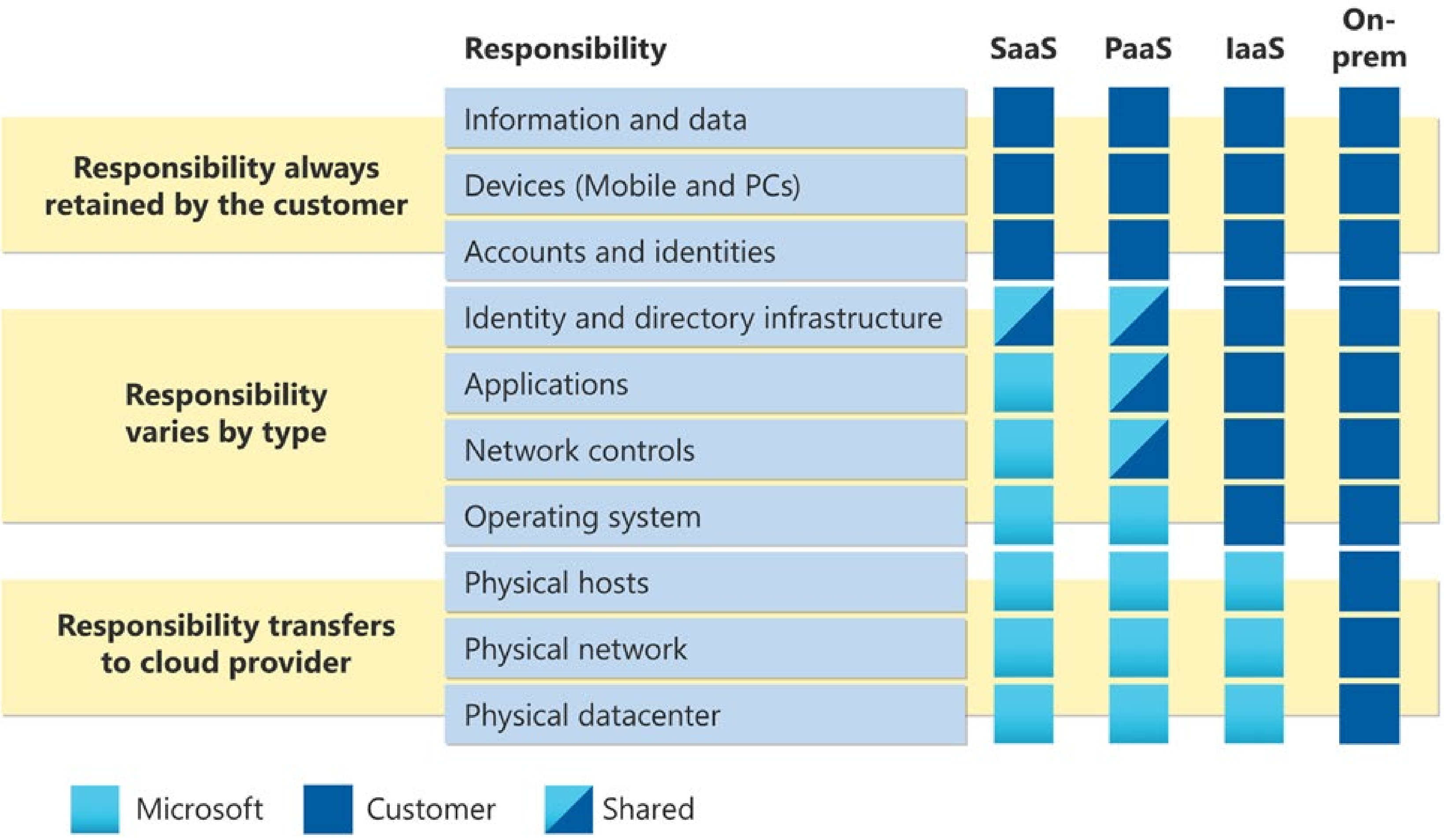
The Path Forward

NERC

- Monthly in-person meetings
- Twice-weekly Webex meetings
- Sub teams to accomplish more work in less time
- Planned progress-check white paper in April or May
- Planned submittal to SC for September meeting – authorization to post for initial ballot
- A supplemental nomination period for additional drafting team members for the Project 2023-09 Risk Management for Third-Party Cloud Services is open through 8 p.m. Eastern, Friday, March 20, 2026.

Present Development

NERC



https://learn.microsoft.com/th-th/azure/security/fundamentals/shared-responsibility

Resources

Project 2023-09 page

White paper

CIP Roadmap

The emerging risk of NOT using cloud services

Ctrl-Alt-Comply: NERC CIP in the Cloud (need a free SANS account)

1. Introduction and Current State
2. Regulated Electric Utility Perspective
3. Application Provider Perspective
4. Cloud Service Providers (CSP) Perspective
5. What are the current compliance challenges?
6. The Path Forward

Questions and Answers

Lew Folkerth
lew.folkerth@rfirst.org