WHITE PAPER

NERC CIP 100 Series

At a Glance

Cloud adoption within the electric utility industry continues to accelerate, creating new opportunities for scalability, resiliency, and operational efficiency. At the same time, cloud-based operating models challenge assumptions built into the existing NERC Critical Infrastructure Protection (CIP) Reliability Standards, which were developed around environments where registered entities directly own and manage the underlying structure.

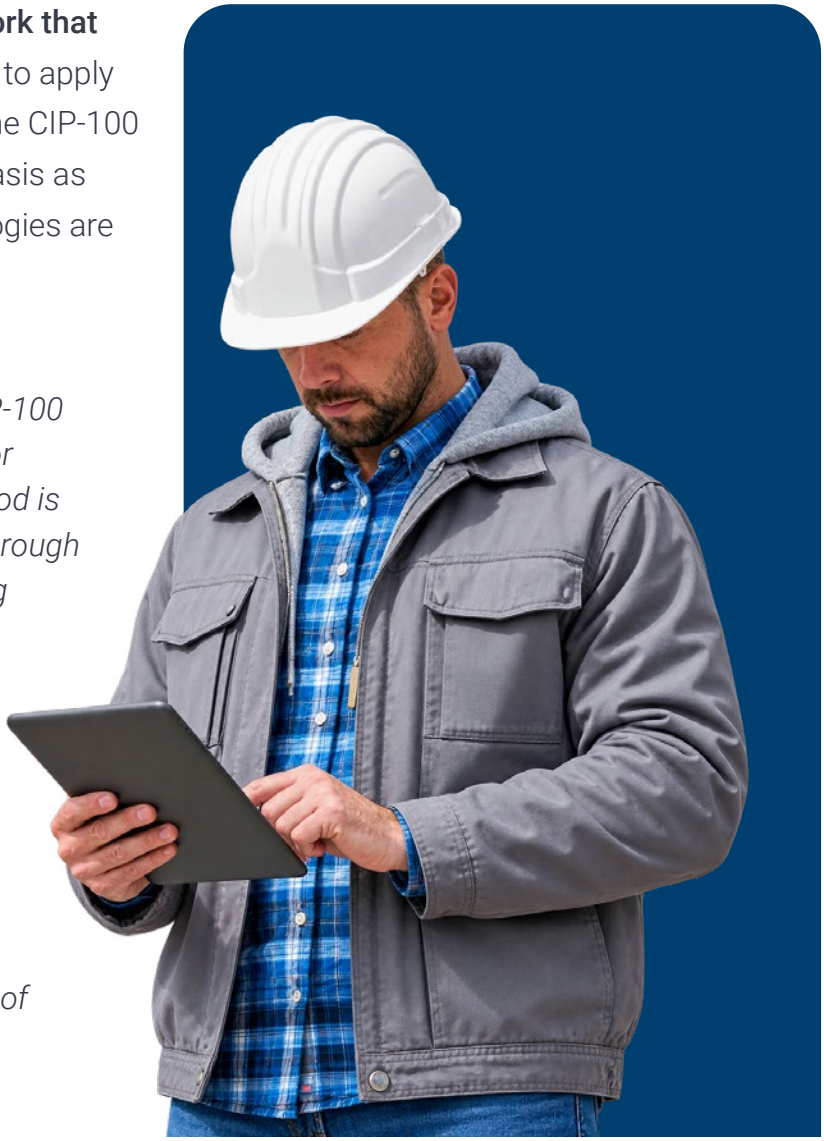
The proposed CIP-100 Series is NERC's effort to address this shift to cloud adoption. Rather than modifying the existing CIP standards, the proposal introduces an alternative compliance framework designed to support cloud-hosted and hybrid environments while maintaining cybersecurity and reliability outcomes comparable to what exists with the current standards.

Executive Summary

NERC is developing a proposed suite of CIP Reliability Standards, the CIP-100 Series, to address the growing use of third-party cloud services in Bulk Electric System (BES) operations.

The current CIP Standards were designed for traditional hardware-based environments and do not align well with today's cloud and hybrid technologies. Rather than extensively revising the existing standards, NERC's team is developing an alternative, mutually exclusive compliance framework that maintains equivalent cybersecurity outcomes while providing the flexibility needed to support responsible cloud adoption.

A key feature of the proposal is organizations can choose the compliance framework that best fits each system, allowing them to apply either the existing CIP standards or the CIP-100 framework on a system-by-system basis as cloud and hybrid operational technologies are implemented.



Current Status (August 2026): *No CIP-100 Series standards have been adopted or approved. The informal comment period is currently open and runs from July 8 through August 21, 2026. This informal posting includes draft language for CIP-102-1, CIP-103-1, CIP-105-1, and CIP-113-1 and related elements. Formal comments and ballot activity is anticipated later in 2026 if the project proceeds on its current path. Registered entities currently have no compliance obligations related to the CIP-100 Series. Continued monitoring of Project 2023-09 is recommended.*

Why the CIP-100 Series Was Proposed

The existing CIP Reliability Standards were developed around a basic assumption: registered entities own and directly control the computing infrastructure that supports BES operations. As organizations increasingly adopt cloud-based technologies, that assumption becomes more difficult to maintain. Infrastructure is often hosted off-site and managed by third-party cloud service providers, while software vendors continue to shift toward cloud-delivered solutions.

As a result, many registered entities are evaluating cloud technologies to support both operational and business functions. **This shift creates a need for a compliance framework that addresses cloud environments while maintaining the security and reliability expectations established by the CIP standards.**

Understanding the proposed framework now can help organizations evaluate potential impacts to technology strategies, governance models, and compliance programs well before any new standards become enforceable.

The CIP-100 Series is intended to:

- Establish risk-based, objective-driven requirements that treat cloud services in a manner consistent with other third-party resources.
- Enable the use of cloud technologies in CIP-regulated systems without creating overlapping or conflicting compliance frameworks.
- Maintain equivalent cybersecurity outcomes while supporting shared-responsibility models that clearly define security responsibilities between the registered entity and the cloud service provider.

Together, these objectives support the secure adoption of cloud technologies while preserving the reliability and security objectives of the existing CIP Reliability Standards.

Core Concepts of the CIP-100 Series

Mutual Exclusivity (System-Level Choice)

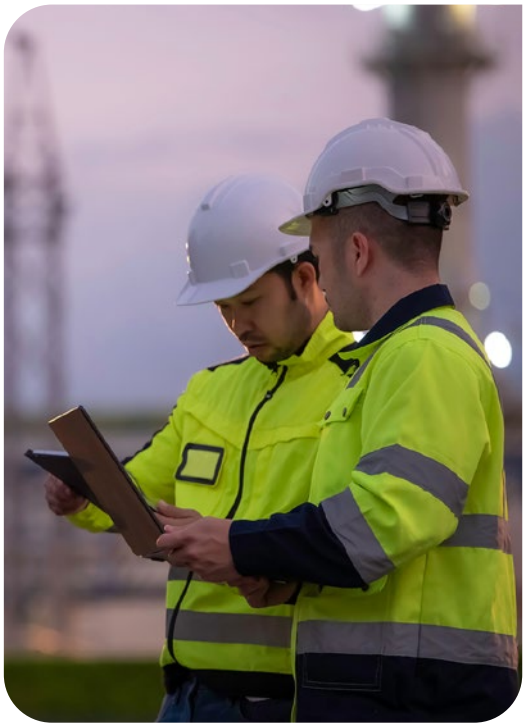
The CIP-100 Series and the existing CIP Reliability Standards are mutually exclusive at the system level. Organizations determine which framework applies to a specific system or logical group of systems, rather than the organization as a whole. This approach supports a gradual, controlled transition while avoiding overlapping or conflicting compliance requirements.

For example, an organization may continue applying the existing CIP Reliability Standards to its Energy Management System (EMS) while applying the CIP-100 Series to a cloud-hosted historian application.

Objective-Based Requirements

The CIP-100 Series focuses on security objectives rather than prescribing specific technologies, device configurations, or network architectures. For example, a requirement may direct organizations to authorize, control, and monitor access without specifying how those objectives must be achieved.

This technology-neutral approach is intended to accommodate both traditional on-premises and cloud-based implementations while maintaining equivalent cybersecurity outcomes.



BES Cyber Services and Systems (BCSS)

The CIP-100 Series introduces BES Cyber Services and Systems (BCSS) as the foundation of its cybersecurity protection requirements.

> **BCSS Definition:** "One or more cyber services or systems that, if rendered unavailable, degraded, or misused, would within 15 minutes of required operation adversely impact Facilities, systems, equipment, or services affecting Reliable Operation of the BES. Redundancy is not considered when determining adverse impact."

This definition applies regardless of where a service is hosted. Cloud-provided and cloud-integrated services are identified as BCSS when they meet the applicable impact criteria.

Supporting New Terms

To support this shift toward service-based security and compliance, the proposal introduces several new concepts and defined terms that organizations will need to understand:

- **Cyber Security Zone (CSZ)** – A logical boundary that groups systems with similar security needs, helping organizations define what must be protected and how. In many cases, this concept takes the place of the traditional Electric Security Perimeter.
- **Conduit** – A secure physical or virtual path used to move data between Cyber Security Zones.
- **Access Control Services and Systems (ACSS)** — Systems and services responsible for managing who can access protected cyber assets and under what conditions.
- **Security Monitoring Services and Systems (SMSS)** – The systems and services that watch activity across protected environments, record what happens, and help identify and respond to potential security threats.
- **Other Security Services and Systems (OSSS)** – Security services that support the overall security program but do not fit neatly into the ACSS or SMSS categories.
- **Protected Cyber Services and Systems (PCSS)** – Cyber services and systems that need protection because of how they connect to, support, or sit near BCSS.
- **System Security Plan (SSP)** – The main compliance document for explaining how security objectives are met and how responsibilities are assigned, including responsibilities shared with cloud providers. The CIP Senior Manager, or a delegate, reviews and approves the SSP at least every 15 calendar months.

Why This Matters

The proposed BCSS model marks a major shift in the proposed CIP framework. Rather than focusing primarily on where a system resides or who owns the underlying infrastructure, the framework focuses on the operational services and functions that support the reliable operation of the BES.

For registered entities evaluating cloud and hybrid environments, this shift provides greater flexibility while maintaining cybersecurity expectations comparable to those of the existing CIP Reliability Standards. The result is a framework designed to evaluate risk based on function and impact rather than technology or deployment model.

Mapping the CIP-100 Series to Existing CIP Standards

The CIP-100 Series is expected to address many of the same cybersecurity topics covered by the current NERC CIP Reliability Standards. The following table provides a high-level comparison based on the current proposal:

Proposed Standard	Primary Focus	Relationship to Current CIP Reliability Standards
CIP-102	Identification and Categorization of BCSS	Builds on CIP-002 by shifting the focus from device- and location-based identification to service- and function-based scoping while retaining the existing BES impact criteria.
CIP-103	Governance and Security Management Controls	Expands upon concepts in CIP-003 by establishing the System Security Plan (SSP) and distributing requirements currently associated with Low Impact BES Cyber Systems across multiple proposed standards.
CIP-105	System Protection	Combines concepts from CIP-005 and CIP-007, introducing Cyber Security Zones (CSZs), Conduits, and objective-based approaches to system protection and vulnerability management.
CIP-113	Supply Chain Risk Management	Expands on CIP-013 by introducing additional criteria for the procurement and ongoing risk management of cloud services.
CIP-104 through CIP-116	Additional Functional areas and cloud-specific topics	Covers areas such as personnel security, incident response, recovery, and residual cloud-related risks, including data sovereignty and interface misconfigurations.

While the proposed numbering generally aligns with familiar NERC CIP subject areas, the CIP-100 Series is not designed as a direct replacement for individual CIP Reliability Standards. Instead, requirements are reorganized, consolidated, and, in some cases, distributed across multiple standards to better address cloud and hybrid environments.

As a result, organizations should avoid looking for a one-to-one mapping between existing CIP requirements and the CIP-100 Series. **The more important consideration is how the underlying security objectives are preserved as the compliance structure evolves to support cloud and hybrid environments.**

Choosing a Compliance Framework

Under the proposed framework, organizations can take a hybrid approach by applying the existing CIP Reliability Standards to some systems and the CIP-100 Series to others. The two frameworks remain mutually exclusive for any individual system or logical group of systems, meaning both frameworks would not apply to the same systems at the same time.

Three Practical Options

Approach	Description	Typical Environment	Key Considerations
Stay with Existing CIP	Continue using the existing CIP Reliability Standards for a given system.	Traditional on-premises operational technology environments where the organization maintains direct control of the underlying infrastructure	No immediate changes to compliance processes or supporting documentation.
Adopt the CIP-100 Series	Transition a system or logical group of systems to the CIP-100 Series.	Cloud-hosted, cloud-integrated, or hybrid operational environments.	Uses objective-based requirements and the SSP to document how security objectives are met within shared-responsibility arrangements with cloud service providers.
Hybrid Approach	Apply the existing CIP Reliability Standards to some systems and the CIP-100 Series to others.	Environments transitioning from traditional on-premises infrastructure to cloud-enabled operational technologies.	Supports a phased transition but requires clearly defined system boundaries, documented framework selection, and appropriate compliance evidence.

Framework Selection Considerations

- Framework selection is made for each BCSS, or logical group of systems, rather than for the organization as a whole
- The selected framework should be documented for each BCSS. For systems governed by the CIP-100 Series, this documentation would be maintained within the System Security Plan (SSP). For systems governed by the existing CIP Reliability Standards, documentation should be maintained within the applicable compliance records.
- In most cases, a single logical system should remain under a single compliance framework to support clear governance and avoid overlapping compliance obligations.
- Where appropriate and justified, tightly integrated components may be treated as separate BCSS and governed under different frameworks.
- Over time, organizations may choose to transition cloud-hosted or cloud-integrated systems to the CIP-100 Series while continuing to manage traditional on-premises systems under the existing CIP Reliability Standards.

What Organizations Need to Know

One of the most important aspects of the proposed framework is flexibility. Organizations are not required to make an all-or-nothing transition. Traditional on-premises systems can continue operating under the existing CIP Reliability Standards, while cloud-hosted and hybrid-environments can move to the CIP-100 Series when it makes sense for the organization.

Because framework selection occurs on a system-by-system basis, registered entities can modernize their technology environments at a manageable pace while maintaining clear compliance accountability and governance.

Preparing for Potential Implementation

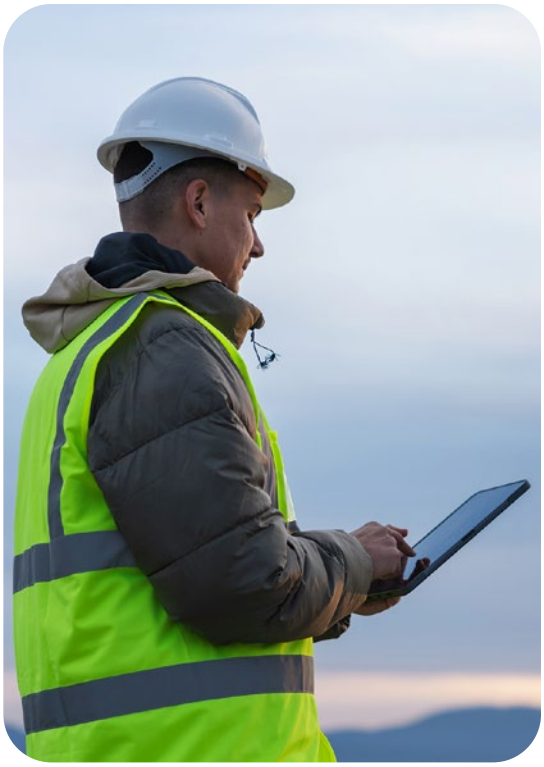
While the CIP-100 Series introduces a new approach to compliance for cloud-hosted and hybrid environments, organizations are not expected to fundamentally change their existing compliance programs. Understanding where the proposed framework applies, how compliance responsibilities are documented, and what changes may be required can help organizations begin evaluating their transition strategy well in advance of implementation.

- Organizations that continue operating fully on-premises systems can continue applying the existing CIP Reliability Standards with no immediate changes to their existing compliance programs.
- Organizations that deploy cloud-hosted or cloud-integrated BCSS may choose to transition those systems to the CIP-100 Series once the standards are approved and an implementation date is established.
- For systems governed by the CIP-100 Series, the SSP is expected to become the primary compliance document. It will document how security objectives are achieved and how responsibilities are shared between the registered entity and applicable cloud service providers.
- The CIP-100 Series eliminates the current Low Impact attachment by incorporating applicable requirements directly into the individual standards.

Recommendations

Although the CIP-100 Series remains under development, organizations do not need to wait for final approval to begin preparing. Taking proactive steps now can help compliance, security, and operational teams better understand potential impacts, evaluate cloud-related risks, and position the organization for a smoother transition if the standards move forward.

1. Continue monitoring Project 2023-09 throughout the NERC standards development process, including the informal comment period which ended August 21, 2026, future formal comment and ballot activities, implementation guidelines, and related project communications.
2. Evaluate current and planned cloud-hosted operational services to determine whether they may meet the proposed BCSS definition and assess potential compliance implications under the CIP-100 Series.
3. Review governance, procurement, and vendor risk management processes to evaluate alignment with the proposed SSP framework and the emerging shared-responsibility model applicable to cloud service providers.
4. Assess organizational readiness for a phased transition by identifying systems that may be appropriate candidates for future adoption of the CIP-100 Series if the standards are approved and become effective.



Conclusion

The CIP-100 Series marks a significant change in the NERC CIP framework. Instead of focusing primarily on infrastructure, it focuses on the systems and services that support reliable BES operations. It also gives organizations more flexibility by allowing them to choose the most appropriate compliance approach for each system.

While the CIP-100 Series remains under development, organizations should begin evaluating potential impacts to cloud strategies and compliance programs. Those that understand and prepare for the proposed framework now will be better positioned to adapt if the CIP-100 Series is ultimately approved and implemented.

About HSI

HSI is your single-source partner for EHS, Compliance, and Professional Development solutions. HSI provides integrated e-learning content, training solutions, and cloud-based software designed to enable your business to improve safety, operations, and employee development. Across all industries, HSI helps safety managers, and technical employees, human resources, first responders, and operational leaders train and develop their workforce, keep workers safe, and meet regulatory and operational compliance requirements. HSI's focus is on training, software, and services for safety and compliance, workforce development, industrial skills, and emergency care. HSI is a unique partner that offers a suite of cloud-based software solutions including learning management, safety management, chemical SDS management, and more, integrated with content and training so businesses can not only monitor and manage multiple workflows in one system, but train employees via one partner.

For more information, visit **hsi.com**