Nov. 2, 2026

To: ReliabilityFirst Compliance Contacts
Subject: RF Compliance Program Update Letter – November 2026

NEW! RF launches refreshed suite of Security Self-Assessments

RF launched a refreshed suite of Security Self-Assessments in October:

- Cyber Resilience Assessment
- Insider Threat Assessment
- Incident Response Tabletops

These cyber and physical security assessments are carefully tailored to reveal risks and knowledge gaps outside of compliance. They are available using open-source software from the Cybersecurity and Infrastructure Security Agency (CISA) called the Cyber Security Evaluation Tool (CSET), which is a free, qualitative self-evaluation software that will generate an extensive report identifying areas of improvement for BPS operators. We have also made simplified Excel sheets to reflect the assessments as an alternative.

CSET is locally stored desktop software and RF will not have access to any information you submit. Entities can download our free custom assessments after applying through the form on our website. Import the RF assessments into CSET, read the descriptions, and submit your answers to evaluate your organization's posture on different focuses. Learn more and request access HERE.

NEW! Extreme Cold Weather Themes and Best Practices Report Posted

The ERO Enterprise is actively engaged in identifying and addressing challenges associated with extreme cold weather preparedness. To support these efforts, the ERO Enterprise has published the Extreme Cold Weather Themes and Best Practices report, which compiles insights gathered through outreach, educational activities, discussions at Regional Entity and NERC technical committee meetings, and monitoring, enforcement, and mitigation activities.

The report highlights common themes and challenges that can affect a registered entity's ability to prepare for and respond to extreme cold weather events. In addition, it outlines best practices designed to address these identified challenges and support registered entities in strengthening the mitigation measures they are implementing to reduce the risks associated with extreme cold weather.

NEW! NERC Board of Trustees adopts Reliability Standards for Computational Loads

NERC's Board of Trustees adopted foundational computational load Reliability Standards on October 26, following the October 14 final ballot. The board action is a major milestone in accelerated efforts to address the reliability risks associated with rapidly growing computational loads. NERC will file the Reliability Standards with the Federal Energy Regulatory Commission (FERC) for approval in the United States, and coordinate with applicable government authorities in Canada on next steps.

The board adoption is the first phase of NERC's broader Large Loads Action Plan to address the reliability challenges associated with large loads, with additional standards development efforts underway to address computational load performance, planning and reliability studies, and event reporting and model quality. For more information, please visit the Large Loads Action Plan page.

NEW! NERC Posts Modernization of Standards Processes and Procedures Initiative Update

NERC released the Modernization of Standards Processes and Procedures Initiative (MSPP) Q4 2026 Update, which highlights the latest progress toward modernizing the standards development process across the ERO Enterprise. This includes additional process documents being developed for industry comments, continued work by the Short-Term Advisory Group to support the computational loads project within the Large Loads Action Plan, ongoing technology initiatives, and a continued commitment to stakeholder engagement.

NEW! Revised RSAWs for PRC-028-1 and PRC-029-1

Two revised Reliability Audit Worksheets (RSAW) are posted to the RSAW webpage under the 'Current RSAWs for Use' for PRC-028-1 and PRC-029-1. Revisions were necessary to correct the referenced effective dates in the initially published PRC-028-1 RSAW and the sub-part requirement numbering in PRC-029-1. Details are included in the version history table of each RSAW.

A RSAW is a guide provided by the ERO Enterprise (collectively NERC and Regional Entities) that describes types of evidence registered entities may use to demonstrate compliance with a Reliability Standard. RSAWs also include information regarding how the ERO Enterprise may assess that evidence. RSAWs do not require specific evidence to be provided, and they are not intended to require a single, exclusive approach to assessing compliance with a Reliability Standard.

NEW! Recent Update to ERO Portal and CORES

A new feature update to https://eroportal.nerc.net (CORES) was released on October 14, 2026. Some highlights to expect, with comments and document attachments:

- Increased file size uploads to 100 MB
- Assignable file types
- Improved views and field names
- Unified file location
- NERC registration letter upload
- Improved comment communication functionality

NEW! NERC Examines International Blackouts to Strengthen North American Grid Reliability

NERC released a new white paper that examines three major international blackouts and identifies critical lessons for strengthening the reliability and resilience of North America's bulk power system. The paper looks at events in South Australia (September 2016), Chile (February 2025), and Spain and Portugal (April 2025), highlighting common reliability challenges and recommending improvements to system design, planning, and operations.

The white paper underscores the importance of designing power systems that can adapt to changing operating conditions while maintaining the essential reliability services historically provided by synchronous generators. This includes strengthening system-wide planning and coordination, advancing modeling and real-time monitoring capabilities, and evaluating technologies that can provide fast-acting frequency and voltage support as the resource mix evolves.

NEW! NERC posts two new episodes of Currently Compliant podcast

Two new episodes of NERC's compliance podcast, Currently Compliant, provide guidance and insights on the implementation of new Reliability Standards related to inverter-based resources (IBR) and critical infrastructure protection (CIP).

Episode 11 reviews the phased implementation plans and requirements for PRC-028, PRC-029, and PRC-030—three standards that emphasize ride-through capabilities to ensure IBRs stay connected and support the grid during disturbances. Hosted by NERC Senior Compliance Assurance Engineer Ryan Mauldin and featuring insights from subject matter experts Curtis Crews, principal engineer at Western Electricity Coordinating Council; James McGrane, senior counsel at NERC; and Beth Rettig, technical auditor at ReliabilityFirst, this episode outlines the timelines and expectations for these critical standards.

Episode 12 follows up on Federal Energy Regulatory Commission (FERC) Order 919 approving the CIP Virtualization Standards from Project 2016-02. The implementation plan allows for registered entities to elect to comply with the revised CIP standards and definitions prior to the effective date of July 1, 2028.

This episode takes a closer look at the early adoption details and how entities can access additional resources. It is hosted by NERC Compliance Assurance Manager Holly Peterson-Rowe and features insights from subject matter experts Gabriela Barragan, CIP cyber and physical security analyst at TexasRE; Udhay Ganesan, principal risk assessment and mitigation engineer at Midwest Reliability Organization; Chris Lewis, technical auditor at ReliabilityFirst; and James McGrane, senior counsel at NERC.

REMINDER! PRC-029-1 effective date reached on Oct. 1

Bulk Electric System (BES) Inverter-Based Resources (IBRs) must be design and operation compliant with PRC-029-1 (Frequency and Voltage Ride-through Requirements for Inverter-based Resources) by Oct. 1, 2026. More specifically, based upon commercial operations date, please reference the following breakdown:

- BES IBRs in operation before April 1, 2025:
  - R1-R3 Design and R4 100% of units by Oct. 1, 2026
  - R1-R3 Operation must be met as DME capability becomes available (per the PRC-028 Implementation Plan)

- BES IBRs in operation after April 1, 2025, and on or before July 31, 2026
  - R1-R3 Design and Operation and R4 100% of units by Oct. 1, 2026

- BES IBRs in operation after July 31, 2026
  - R1-R3 Design and Operation and R4 100% compliant on Oct. 1, 2026, or commercial operations date
  - R4 is limited to those units in-service by Oct. 1, 2026.

Note: R4 Hardware exemption submittals (for facilities with a COD prior to the effective date of the standard) are due by Oct. 1, 2027, for BES and non-BES IBRs.

Additionally, NERC released the ERO Enterprise CMEP Practice Guide: PRC-029-1 Enforcement Discretion (*new version was posted by NERC on 9/10/26*) and Enforcement Discretion Tracker. The purpose of this CMEP Practice Guide is to provide guidance to CMEP staff regarding the use of enforcement discretion for potential noncompliance with the design aspects of PRC-029-1 Requirements R1, R2, and R3 (Frequency and Voltage Ride-through Requirements for Inverter-based Generating Resources). Due to industry-wide constraints on qualified Inverter-Based Resource (IBR) original equipment manufacturers (OEMs) and vendors, some Generator Owners may be unable to complete the design implementation activities associated with Requirements R1 through R3 by the applicable compliance dates of October 1, 2026, for Bulk Electric System (BES) IBRs and January 1, 2027, for non-BES IBRs. For any questions or further guidance regarding this Practice Guide or completing the Enforcement Discretion Tracker, please contact EnforcementCU@rfirst.org.

REMINDER! Small Group Advisory Sessions on CIP Standards Addressing Virtualization Effective in 2028

NERC, in collaboration with the Regional Entities, will host a Small Group Advisory Session (SGAS) for registered entities to discuss the revised CIP Standard Requirements and modified definitions addressing Virtualization developed in Standard Drafting Project 2016-02. In addition to reviewing the changes to CIP Reliability Standards with mandatory compliance dates in 2028, the SGAS will also discuss early adoption, "per system capability" reporting, and industry questions.
The SGAS will consist of two parts:

1. General Session Live Webinar – A general session will be held to discuss revisions of the NERC CIP Reliability Standards addressing Virtualization. The General Session will be held on Monday, December 7, 2026, from 1:00–3:00 p.m. Eastern. **Registration for a one-on-one session is not necessary to participate in this general session.** Register here.
2. SGAS One-on-One Sessions – **Closed**, one-on-one discussions between a registered entity and ERO Enterprise (collectively, NERC and Regional Entities) staff about issues pertinent to their compliance with the CIP Reliability Standards for Virtualization. These sessions will occur between Tuesday, December 8, 2026, and Friday, December 11, 2026. NERC scheduled the one-on-one sessions as registration was received and coordinated with Regional Entity staff.

Request for questions – To provide as much benefit as possible and address topics of concern from industry during the General Session, NERC continues to request that industry submit any questions they may have relevant to the revised CIP Reliability Standards. Please use the link to submit your questions, contact information, and categorization of questions (specific to CIP Standard or Requirement, Early Adoption/Implementation Plan, Per System Capability, Other). Multiple questions can be submitted in one request.



IMPORTANT REMINDER – UPDATE COMPLIANCE CONTACT INFORMATION in CORES
Registered entities are expected to review and update their compliance contacts information as changes occur. Updating compliance contact information is critical to ensure that our contact data remains fresh, accurate and is current always. **Please verify and update as necessary the names, addresses, phone numbers (cell) and email addresses for your Compliance Contacts (PCC/ACC/PCO) in the ERO Portal/CORES system.**

NEW! Monthly Technical Talk with RF

The next Tech Talk with RF will be held on Monday, November 16, at 2:00 PM ET.

ReliabilityFirst (RF) offers a regularly scheduled monthly call to provide entities and stakeholders with a forum for addressing topics and questions relevant to reliability, resilience and security.

While RF Subject Matter Experts (SMEs) will provide presentations and updates, they will not address entity-specific questions and issues. These types of questions can be handled offline by using the RF Assist Visit program. If you have any questions, please reach out to Mike Hughes, Entity Engagement Manager, 216-503-0617.

Event Information

November Technical Talk with RF
Monday, Nov. 16, 2026, 2:00 PM | (UTC-04:00) Eastern Time (US & Canada)
Join link:
https://reliabilityfirst.webex.com/reliabilityfirst/j.php?MTID=m22e775b2c996f345a520a39f75b3f89f
Meeting number:
2301 112 6928
Meeting password:
0123456 (0123456 when dialing from a phone or video system)
Join by phone:1-650-479-3207 Call-in toll number (US/Canada)
Access code: 230 111 26928
Please join us on Slido.com using #TechTalkRF as the event code

Agenda

Lessons Learned from FERC's 2026 CIP Reliability Audits

Alan Herd, Deputy Director, Division of Cyber Security, Federal Energy Regulatory Commission (FERC)

Alan Herd will review key lessons from FERC staff's 2026 Commission-led CIP Reliability Audits report, including considerations related to registration and CIP compliance for generation resources, BES cyber system identification and categorization, and access to BES cyber systems and BCSI facilitated by super intelligence tools.

ERO Organization Certification: Process and Expectations

Sam Ciccone, Principal Reliability Consultant, and David Sopata, Principal Reliability Consultant, Entity Engagement, RF

Learn how the ERO Organization Certification Program evaluates an entity's readiness to reliably perform critical functions. Sam Ciccone and David Sopata will walk through certification activities, common review triggers, the typical process and timeline, CIP considerations, and what entities can expect throughout the review.

IMPORTANT! NERC Registration and Certification Information

Notification of additional changes in registration status

Section 501.1.3.5 of NERC's Rules of Procedure requires the **registered entity to notify NERC through its corresponding Regional Entity of any changes in registration, ownership, corporate structure, or similar matters that affect the entity's responsibilities with respect to the Reliability Standards.** Failure to notify NERC through its corresponding Regional Entity will not relieve the registered entity from any responsibility to comply with the Reliability Standards or liability for any penalties or sanctions associated with failing to comply with such standards. **RF requests that registered entities provide RF Registration with 30-60 days advance notice of any such changes impacting NERC Registration.** Contact Beth Smail, Senior Analyst, Registration and Entity Services, with any questions at beth.smail@rfirst.org.

IMPORTANT! NERC Alert System Registration

NERC's Alert System is the tool used to disseminate information that is critical to ensuring the reliability of the BPS in North America. NERC distributes alerts broadly to owners, operators, and users of the BPS utilizing the listing of the NCR. Entities registered with NERC are required to provide and maintain up-to-date compliance and cyber security contacts.

As a separate part of the NERC registration process and inclusion on the NCR, please contact NERC via email at NERC.Alert@nerc.net to register or revise your listing for the NERC Alert System. Alternatively, you may call the NERC Alerts Hotline at 404.446.9797 to speak with someone. Each registered entity identified in the NCR is required to notify NERC Alert of any corrections, revisions, deletions, changes in ownership, corporate structure, or similar matters that affect the registered entity's responsibilities with respect to the Reliability Standards.

Remember to always keep your NERC Alert Contacts current and up-to-date at all times.

E-ISAC Membership Registration

It is important, and expected, that qualified registered entities will join the Electricity Information Sharing and Analysis Center (E-ISAC).[1] E-ISAC membership is available to qualified North American asset owners and operators (AOOs) and select partner organizations, and there is no cost to join. The E-ISAC encourages individuals with cyber, physical, or operational technology security responsibilities to apply for membership on behalf of your organization. This individual will serve as a point of contact for E-ISAC security-related communications and will have access to emerging threat information and analysis.

Please complete the E-ISAC Membership application here: https://www.eisac.com/portal. You may also contact the E-ISAC at memberservices@eisac.com with any questions.

[1] Created in 1999 and located in Washington, D.C., the E-ISAC is operated by NERC. The E-ISAC acts as the primary communications channel for industry members and partners to voluntarily exchange cyber and physical security threat information. E-ISAC security experts analyze this information to identify patterns and trends, providing industry with a detailed view of the threat landscape and advice on how to navigate it. Both NERC and the E-ISAC adhere to a strict code of conduct that reinforces the E-ISAC's organizational isolation from NERC's enforcement activities.

Align Training Resources

The NERC Align Project page and FAQ document contain helpful information for registered entities. Self-service training resources provided for registered entity staff, including training videos and user guides, are available on the NERC Training Site.

NERC's training site provides training and materials on a variety of topics for Align and other tools used by NERC, Regional Entity, and registered entity staff. Your Primary Compliance Contact is the designated Access Approver for Align for your company. Remember to check out NERC's Align project page or reach out to AskAlign@NERC.net for additional information.

Align Violations Reporting

As a reminder, any new violation of a Reliability Standard identified by a registered entity should be immediately self-reported to RF via the ERO Align system. Contact Shirley Ortiz, Senior Paralegal, at (216) 503-0674 with any questions concerning self-reports.

Align support – ERO Help Desk Ticketing System

If users encounter any access or system problems with Align, CORES or any of the other NERC applications, first and foremost, try to resolve the issues yourself by using any one of the many self-service resources, guides and videos NERC has made available to you at training.nerc.net.

If you are unable to resolve the issue on your own, place a ticket using the NERC Helpdesk Ticket Submission System: support.nerc.net. The ERO Help Desk Ticketing System (Footprints) is available to registered entity users 24/7 and is monitored by the regions and NERC. We will do our best to address your questions, issues, and tickets as promptly as possible during normal business hours.

Upcoming Standards Subject to Future Enforcement

BAL-007-1.1	Near-term Energy Reliability Assessments	April 1, 2027
EOP-004-5	Event Reporting	Oct. 1, 2027
MOD-032-2	Data for Power System Modeling and Analysis	April 1, 2028
CIP-002-8	Cyber Security - BES Cyber System Categorization	July 1, 2028
CIP-003-10	Cyber Security – Security Management Controls	July 1, 2028
CIP-004-8	Cyber Security — Personnel & Training	July 1, 2028
CIP-005-8	Cyber Security — Electronic Security Perimeter(s)	July 1, 2028
CIP-006-7.1	Cyber Security — Physical Security of BES Cyber Systems	July 1, 2028
CIP-007-7.1	Cyber Security — System Security Management	July 1, 2028

CIP-008-7.1	Cyber Security — Incident Reporting and Response Planning	July 1, 2028
CIP-009-7.1	Cyber Security — Recovery Plans for BES Cyber Systems	July 1, 2028
CIP-010-5	Cyber Security — Configuration Change Management and Vulnerability Assessments	July 1, 2028
CIP-011-4.1	Cyber Security — Information Protection	July 1, 2028
CIP-013-3	Cyber Security - Supply Chain Risk Management	July 1, 2028
CIP-015-1	Cyber Security – Internal Network Security Monitoring	Oct. 1, 2028
CIP-014-4	Physical Security	Oct. 1, 2028
IRO-010-6	Reliability Coordinator Data and Information Specification and Collection	April 1, 2029
TOP-003-8	Transmission Operator and Balancing Authority Data and Information Specification and Collection	April 1, 2029
CIP-003-11	Cyber Security – Security Management Controls	July 1, 2029
CIP-015-2	Cyber Security – Internal Network Security Monitoring	Oct. 1, 2029

Please refer to the U.S. Effective Dates page on the NERC website for additional detail.

Periodic Data Submittals Due in November 2026			
11/29/2026	PRC-004	GO, TO, DP	Protection System Misoperations - Section 1600 data request for Q3-2026 (July 1 – September 30). **Submit in MIDAS portal**

Periodic Data Submittals Due in December 2026 - None

If you experience any issues with your data submittals, please contact PDS@rfirst.org.