Reliability & Security Oversight Update

WECC

February 19, 2026
2–3 p.m. MST

WECC

Reliability & Security Oversight Update

Mailee Cook
Training and Outreach Specialist

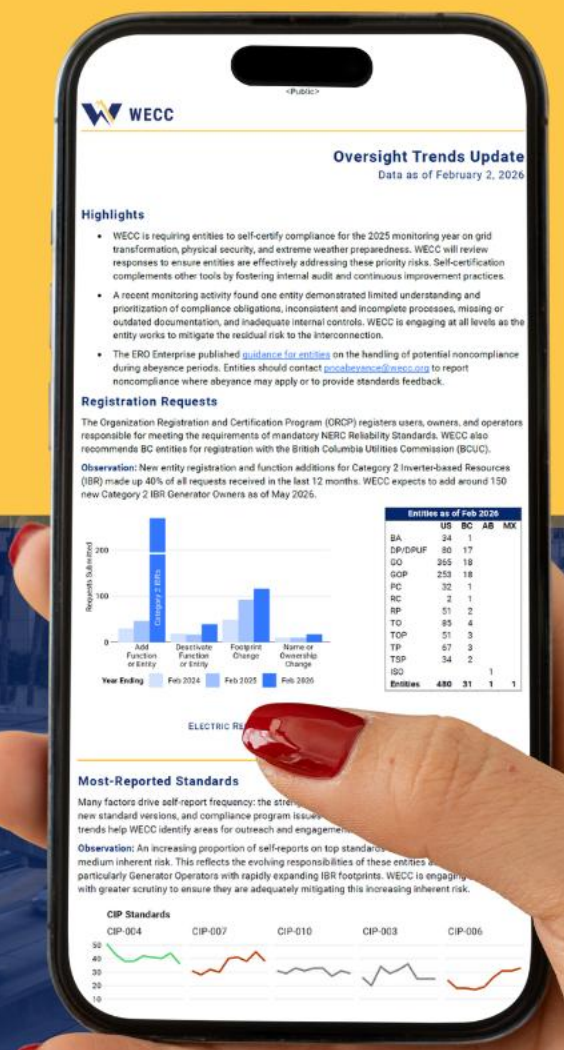
Electric Reliability & Security for the West

February 19, 2026

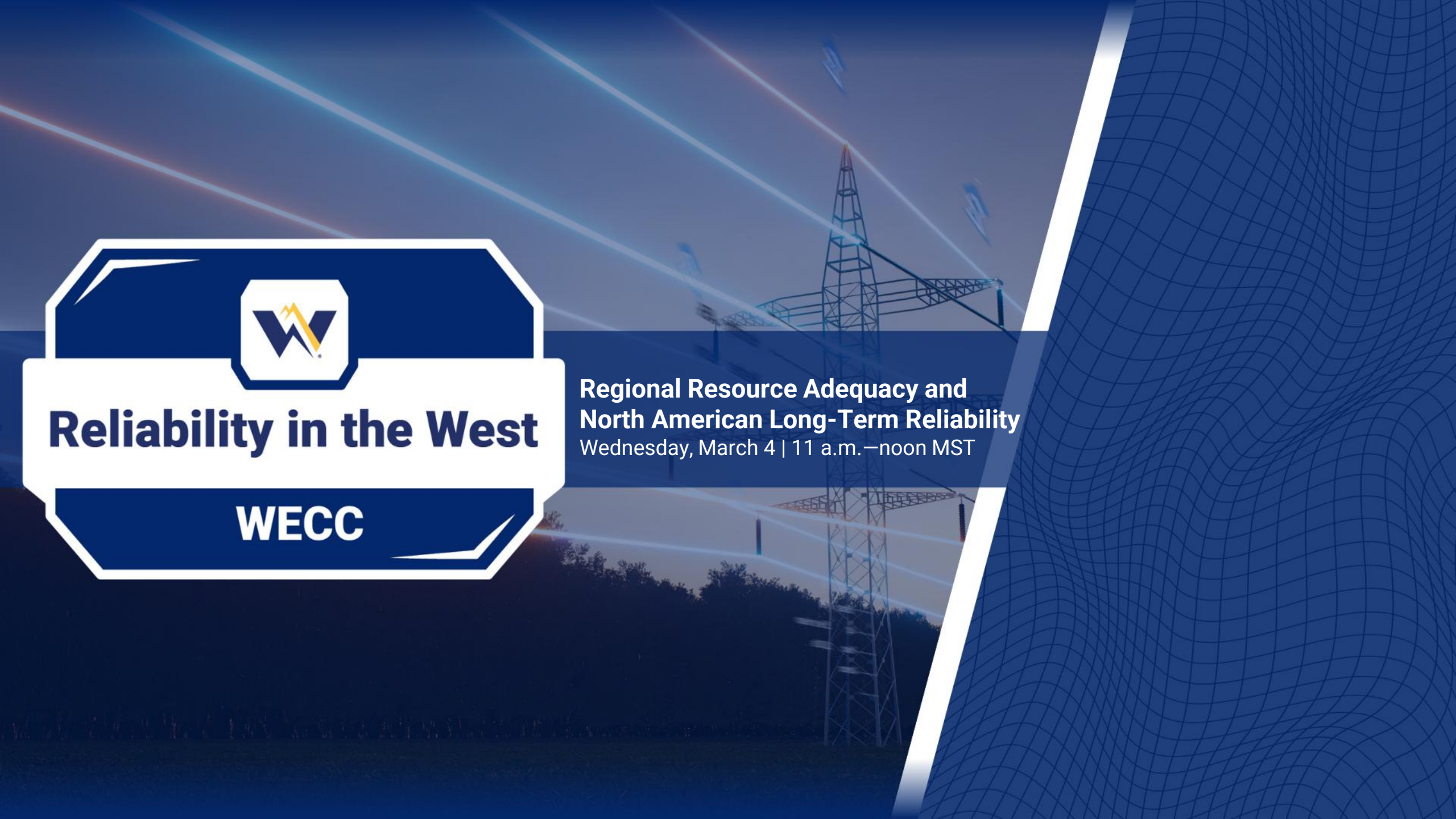
Oversight Trends Update

WECC

Q1 2026




Grid Fundamentals
WECC
February 24–25, 2026
1–5 p.m. MST (Virtual)

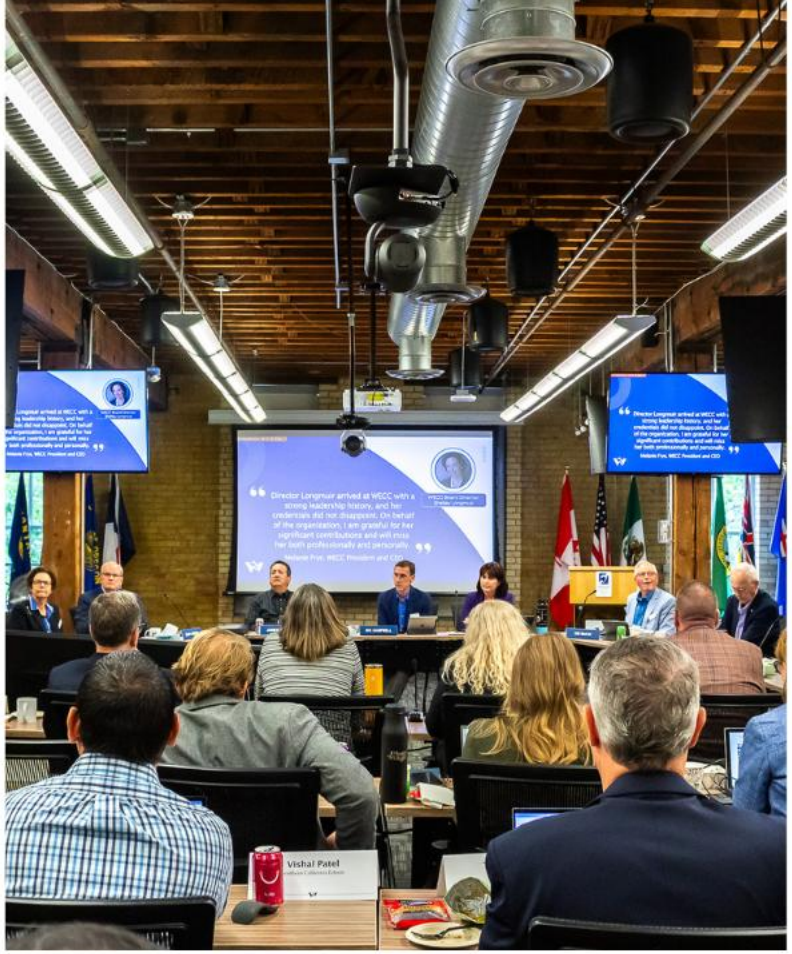


Regional Resource Adequacy and North American Long-Term Reliability

Wednesday, March 4 | 11 a.m.—noon MST

BOARD AND ASSOCIATED MEETINGS

March 10–11




Reliability & Security
Workshop
WECC
March 17–18, 2026
San Diego, California

Agenda

- NERC & WECC Happenings
  - Fahad Ansari, Senior Technical Advisor, WECC
- Standards Update
  - Donovan Crane, Senior Engineer, Standards, WECC
- Inverter-based Resources Initiative Update
  - Abby Fellinger, Senior Registration & Certification Engineer, WECC
- Cold Weather Update
  - Curtis Crews, Senior Technical Advisor, WECC
- Finding Updates in Align
  - Tom Williams, Senior Enforcement Mitigation Engineer, CIP, WECC
- ERO Enterprise Critical Infrastructure Protection Evidence Request Tool v10
  - Teri Kelly, Senior Auditor, Cybersecurity, WECC
  - Monica Vela, Senior Auditor, Cybersecurity, WECC

NERC and WECC Happenings

Fahad Ansari
Senior Technical Advisor, Oversight Planning

Electric Reliability
& Security for the West

February 19, 2026

NERC and WECC Happenings

- Lesson Learned
  - Generator Field Breaker Failure
- Assist Me! ERO
  - Webinar recording
- Letter to CEOs
- Reliability Insights
  - Complex Cyber Threats Require Brilliance at the Basics
- NERC 2025 Long-Term Reliability Assessment
- Coordinated Oversight Program — Update

NERC and WECC Happenings

- Jeffrey Droubay Named WECC President and CEO
- Engage with WECC
- 2025 Western Assessment of Resource Adequacy
- WECC Publishes 2024–2026 UFLS Assessment Report

Standards Update

Donovan Crane
Senior Engineer

Electric Reliability
& Security for the West

February 19, 2026

Standards Update — WECC Projects

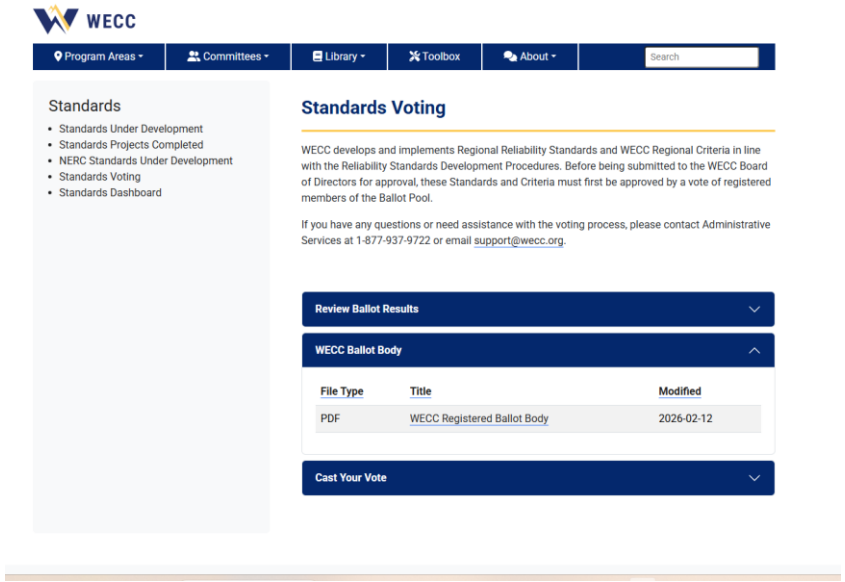
[WECC-0157: PRC-006-5 Automatic Underfrequency Load Shedding, Update to the WECC Regional Variance]	Prepping for industry ballot Anticipated for March 2026
[WECC-0158: IRO-002-7, Reliability Coordination—Monitoring and Analysis with WECC Regional Variance, Five-Year Review]	Sending recommendation of “No Change” to the WSC
[WECC-0159: IRO-006-WECC-3 Qualified Path Unscheduled Flow (USF) Relief, Five-Year Review]	Sending recommendation of “No Change” to the WSC
WECC EMT Criterion SAR and Project Coming	Group from the EMT workshop is working on putting a SAR together to create a WECC Criterion focused on EMT modeling

Standards Update — NERC Projects

2023-06 CIP-014 Risk Assessment Refinement	• Trying to get redlines and comments ready for a 4th ballot
2025-03 Order No. 901 Operational Studies	• Goal to ask SC for initial 45-day posting in March
2025-04 Order No. 901 Planning Studies	• Will ask for initial 45-day posting in March
2025-02 Internal Network Security Monitoring Standard Revision | Draft 1(CIP-015-2)	• Passed ballot with 84.33% • Implementation Plan passed with 81.25%
2023-01 EOP-004 IBR Event Reporting	• Passed ballot with 91% approval no final ballot needed

WECC Ballot Body

- Standard Voting Segments (SVS) will change with the implementation of the MSPPTF recommendations.
  - WECC SVS will change at the same time, and the ballot body and registrations will need to be updated.
- Current ballot body can be found on the Standards Voting webpage at https://www.wecc.org/program-areas/standards/standards-voting



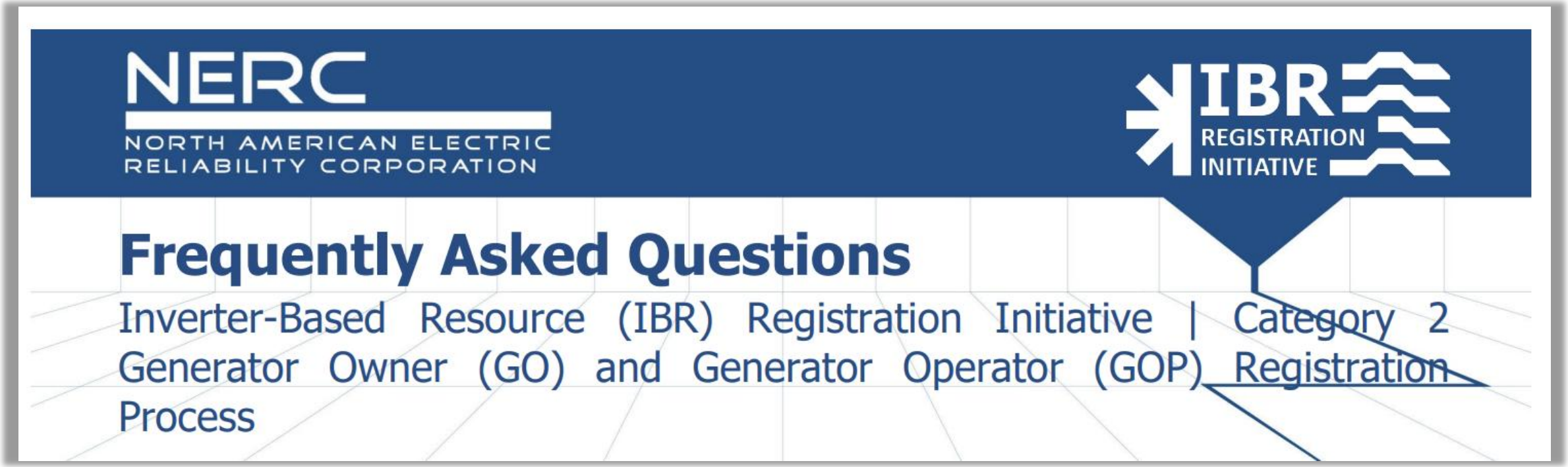
Inverter-based Resources Initiative Updates

Abby Fellinger
Senior Registration & Certification Engineer

Electric Reliability & Security for the West

February 19, 2026

FAQ: IBR Registration Process for Category 2 Entities



- Highlights from the IBR Registration Initiative: FAQ for Category 2 GO and GOP Registrations that was published on December 22, 2025
  - Upcoming Reporting Obligations
  - Available Resources

FAQ: IBR Registration Process for Category 2 Entities

Question: I received a notification that I need to complete a Reporting Confirmation for 2026. Is this required?

Answer: Technically, no. However, even though you are not yet required to submit GADS data, please submit the Reporting Confirmation to indicate whether your entity meets the GADS reporting criteria, available on the NERC website. Although you technically do not need to complete the Section 1600 confirmation until May, we recommend completing it now while it is fresh in your mind.

Question: Do I need to begin submitting Generating Availability Data System (GADS) information after I receive my registration letter from NERC?

Answer: No, Category 2 entities are not required to submit GADS information until May 15, 2026.

FAQ: IBR Registration Process for Category 2 Entities

- GADS
- GADS Solar
  - gadssolar@nerc.net
- GADS Wind
  - gadswind@nerc.net

Deadlines for Data Submission into GADS Conventional, GADS Wind, and GADS Solar

When a deadline falls on a weekend or holiday, reporting will be extended through the following business day.

Reporting Deadline*	Period of Operation to Report
February 15	Any updates for prior year
May 15	Quarter 1: January 1 - March 31
August 15	Quarter 2: April 1 - June 30
November 15	Quarter 3: July 1 - September 30
February 15	Quarter 4: October 1 - December 31

- Category 2 GO reporting obligations are effective on May 15, 2026 (in the middle of Q2).
  - The first reporting deadline for GADS Solar or GADS Wind data submissions is August 15, 2026 (45 days after the end of the quarter).
  - More information about how to sign up for a GADS Solar or a GADS Wind user account will be sent out sometime after the final 2025 reporting deadline has passed (around early April is the target).

FAQ: IBR Registration Process for Category 2 Entities

Question: Where can I find resources to help me as a new entity?

Answer: NERC has developed numerous resources as part of a broader effort to welcome new participants into the ERO Enterprise and provide the tools and guidance needed to support reliability and compliance from the start. All of these resources are available on the **IBR Registration Initiative page** on NERC's website, a frequently updated project hub that allows stakeholders to easily locate key project updates and resources, as well as the **Registration page**. We encourage you to explore these resources and become actively involved in the ongoing efforts to enhance grid reliability today and in the future. Your input and expertise are invaluable as we work together to reliably integrate IBRs into the BPS.

IBR Registration Initiative

Organization Registration

FAQ: IBR Registration Initiative Resources

Examples of Resources Available

Learn More
Open Letter to New Registrants
101 Resource Document
IBR Video
ERO Enterprise Informational Package 101

Quarterly Updates - 2025
Q4 Update | Q3 Update | Q2 Update | Q1 Update

Registration
Category 2 GO/GOP Registration FAQ
Changes to the NERC Compliance Registry
ERO Enterprise CMEP Guide
Expanding Your Registration
Joining the ERO Enterprise
Quick Reference Guide: Candidate for Registration

Standards
NERC Files Order No. 901 Milestone 3 Projects with FERC
Reliability Compliance Dates for Generator Owners & Generator Operators
Milestone 3 Summary
Milestone 3 Infographic
Standards Under Development page

Industry Resources
NATF IBR Interconnection Lifecycle: Requests and Studies Practices
NATF IBR Interconnection Lifecycle: Interconnection Agreements and Requirements Practice

Webinars
July 2025 Recording | March 2025 Recording | November 2024 Recording

WECC Registration Information

WECC Registration Website

Registration Contacts | Registration@wecc.org

- Mark Rogers | Manager, Registration & Certification | mrogers@wecc.org
- Abby Fellinger | Senior Registration & Certification Engineer | afellinger@wecc.org
- Andrew Williamson | Senior Registration & Certification Engineer | awilliamson@wecc.org
- Chris Murphy | Senior Registration & Certification Engineer | cmurphy@wecc.org
- Sarah Mitchell | Staff Engineer, Registration | smitchell@wecc.org

Cold Weather Update

Curtis Crews
Senior Technical Advisor

Electric Reliability
& Security for the West

February 19, 2026

Updating a Finding in Align

Tom Williams
Senior Enforcement Mitigation Engineer

Electric Reliability
& Security for the West

February 19, 2026

Agenda

- This presentation is intended to provide guidance on how to update a noncompliance in Align using the Finding Update functionality.
- We will discuss multiple reasons why entities will need to do this.
- Through three scenarios, in quiz format with multiple choice, we will reinforce when to submit a Finding Update in Align versus when to upload documents to the Secure Evidence Locker (SEL).

Updating a Finding

Providing More Information for a Finding in Align

- There are three methods for providing more information in Align for a finding:
  1. Submit a Finding Update.
  2. Update a mitigation.
  3. Respond to a Request for Information (RFI).
     - An RFI could request a Finding Update.
- This presentation is specific to the first method.

ERO Portal
Align and Secure Evidence Locker
BESnet Notification and Exceptions Tool
Centralized Organization Registration ERO System
Data Stores & Extranet Sites
Email Distribution Lists
Membership Application
Standards Balloting System

Align and SEL Entity User Guides

Registered Entity Align Attestations User Guide
July 12, 2025 PDF

Registered Entity Align Enforcement and Mitigation User Guide
March 14, 2025 PDF

Registered Entity SEL Portal Guide
January 9, 2026 PDF

Registered Entity Align IRA and COP User Guide
March 14, 2025 PDF

Registered Entity Align PDS User Guide
March 14, 2025 PDF

Registered Entity Align Self-Certifications User Guide
March 14, 2025 PDF

Registered Entity Align TFE User Guide
March 14, 2025 PDF

Align Enforcement and Mitigation User Guide

Welcome to the Align Enforcement and Mitigation Registered Entity User Guide. Along with the Align **instructional videos**, this user guide will help you navigate through all of the features included in these modules. Click on a topic in the list below or in the ribbon above to begin.

Uses of a Finding Update

- Use a Finding Update to add/change/supplement the:
  - Start or end dates of the noncompliance
  - Extent of condition (EOC) of the noncompliance
  - Causes of the noncompliance
  - Potential impact, likelihood of impact, or actual impact on the bulk power system
  - Additional instances of noncompliance that have the same causes and same mitigation for the same Requirement/Part as the originally submitted noncompliance

Incorrect Uses of a Finding Update

- Finding Updates are not for additional instances of noncompliance that have:
  - Different causes
  - Different mitigations
  - Different Requirements/Parts
- When it is unclear whether additional noncompliance should be a Finding Update or a new Self-Report/Self-Log, feel free to reach out to your attorney case manager or mitigation engineer in WECC Enforcement.

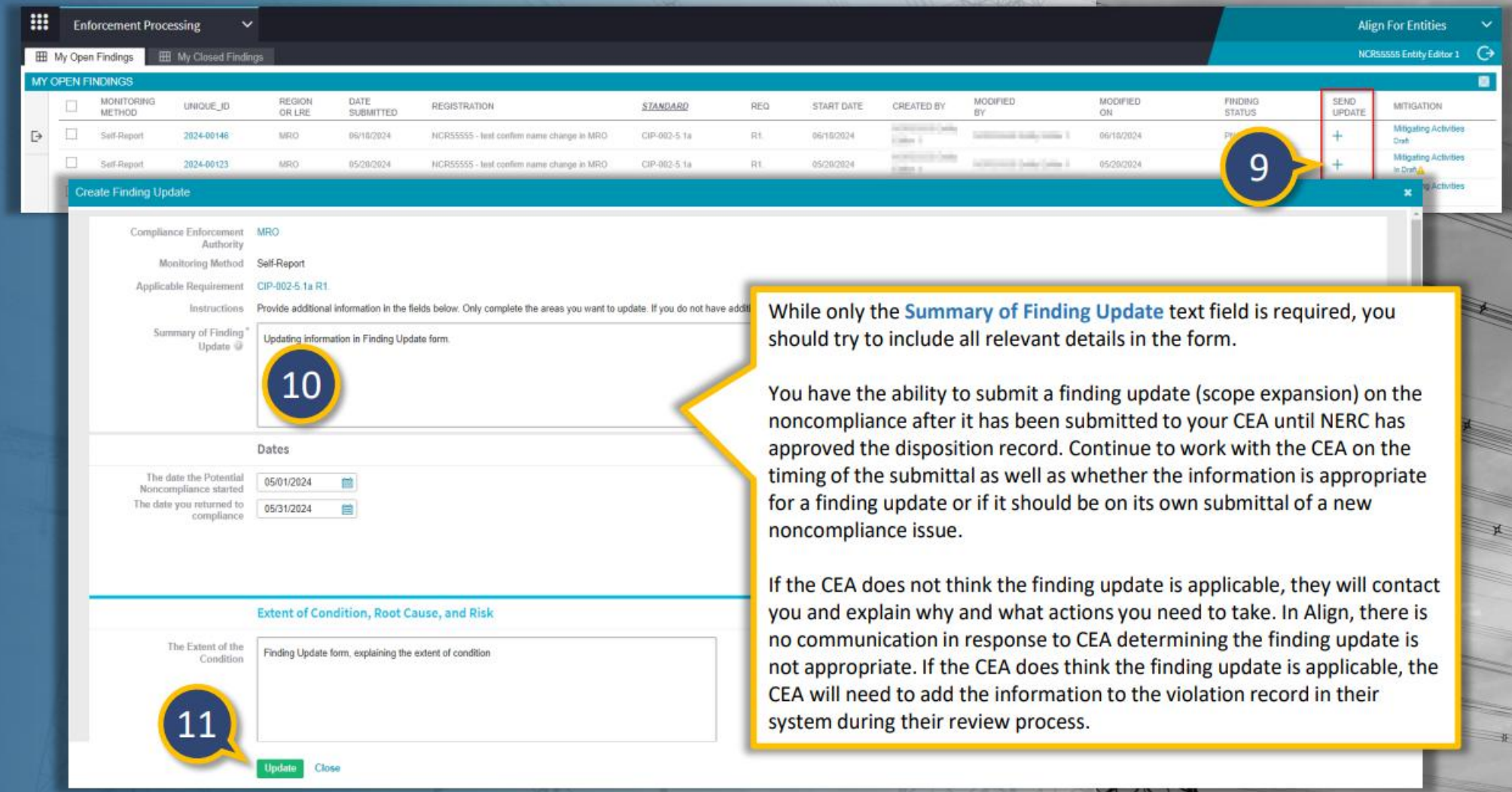
Updating a Finding

Once you have located the finding that needs to be updated:

9. Click the **+** icon in the **Send Update** column

10. Enter a summary of the changes that you are making into the **Summary of Finding Update** field and add the updated data into the relevant fields

11. Click the **Update** button



While only the **Summary of Finding Update** text field is required, you should try to include all relevant details in the form.

You have the ability to submit a finding update (scope expansion) on the noncompliance after it has been submitted to your CEA until NERC has approved the disposition record. Continue to work with the CEA on the timing of the submittal as well as whether the information is appropriate for a finding update or if it should be on its own submittal of a new noncompliance issue.

If the CEA does not think the finding update is applicable, they will contact you and explain why and what actions you need to take. In Align, there is no communication in response to CEA determining the finding update is not appropriate. If the CEA does think the finding update is applicable, the CEA will need to add the information to the violation record in their system during their review process.

Three Scenarios

Scenario One

- You are reviewing EOC for a Self-Reported/Self-Logged noncompliance.
- You find additional instances of noncompliance for the same Requirement/Part with the same causes and the same mitigation.
- What do you do?
  A. Submit a new Self-Report/Self-Log.
  B. Submit an update to the SEL.
  C. Submit a Finding Update on the existing noncompliance in Align.

Scenario Two

- You are reviewing EOC for a Self-Reported/Self-Logged noncompliance.
- You find additional noncompliance in a different Requirement/Part with different causes and different mitigation.
- What do you do?

  A. Submit a new Self-Report/Self-Log.

  B. Submit an update to the SEL.

  C. Submit a Finding Update on the existing noncompliance in Align.

Scenario Three

- You are responding to an RFI for a Self-Reported/Self-Logged noncompliance.
- You have a response prepared that includes both narrative and evidence.
- What do you do?
  A. Submit an update to the SEL.
  B. Provide the narrative in Align and upload the evidence to the SEL.
  C. Submit a Finding Update on the existing noncompliance in Align.
  D. Could be one or more of the above.
- **As a rule, an RFI response containing CEII/BCSI/CUI should go to the SEL, and any documents (Word, PDF, Excel) need to go to SEL.**

Resources

NERC Align and Secure Evidence Locker Webpage

NERC Align Self-Report and Mitigation Guide

Registered Entity Self-Report and Mitigation Plan User Guide

WECC Self-Report and Mitigation Checklist

WECC

CIP Evidence Request Tool (ERT) Version 10.0

Teri Kelly
Senior CIP Auditor

Monica Vela
Senior CIP Auditor

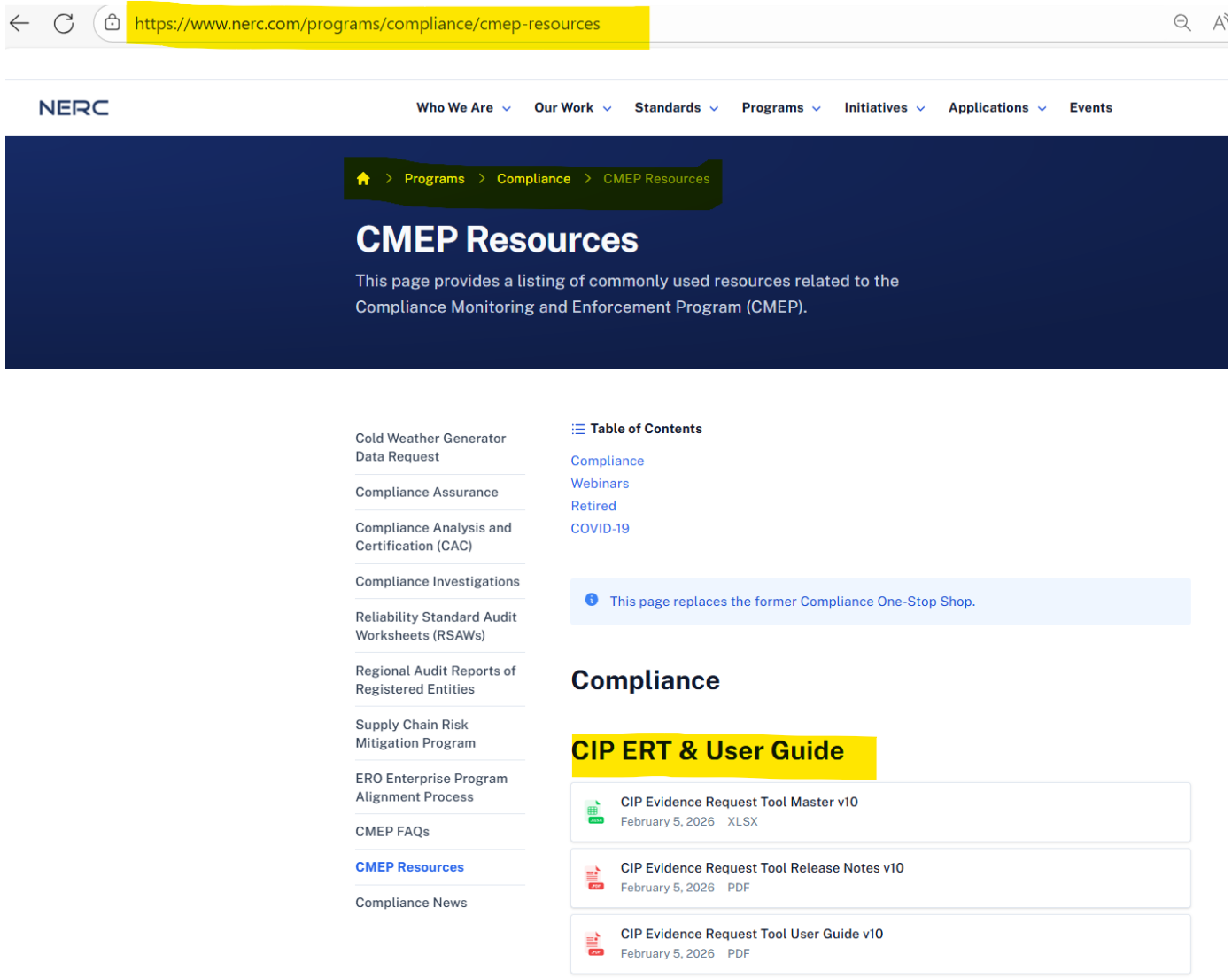
Electric Reliability & Security for the West

February 19, 2026

ERT Version 10.0

- The ERO Enterprise implements major versions annually
  - NERC and Regional Entities such as WECC participate
- NERC Security Working Group (SWG)
  - Industry group
  - Comments and feedback
- Updated for approval and early adoption of Project 2016-02
- Starting with audits in mid-June

ERT on NERC website



General Changes

- Added Level 1 and Level 2 Requests and Sample Sets for Reliability Standards from Standard Drafting Project 2016-02 (pending FERC Approval):
  - CIP-002-7, CIP-003-10, CIP-004-8, CIP-005-8, CIP-006-7, CIP-007-7, CIP-008-7, CIP-009-7, CIP-010-5, CIP-011-4, and CIP-013-3
- Added classifications on the CA tab for virtualization
- Updated some field and column names to be more concise and consistent (see User Guide for details on what is requested for each field)
- Updated all *TRUE/<blank>* validation fields to *TRUE/FALSE*
- Updates to formulas, sample sets, and dates to assist audit team with sampling
- Revamped and updated the ERT User Guide

User Guide

- Format changed into a table
  - Added a few string, drop-downs, and Boolean data types

Table 1: BES Assets Tab

Field Name	Description	Data Type	Constraints	Example
BES Asset ID	A unique identifier or name associated with the asset.	String	Must be unique	North Control Center
Asset Type	The category type associated with this asset (values are the identified asset types within CIP-002 R1).	List	▪ Control Center ▪ Substation ▪ Generation ▪ System Restoration ▪ SPS/RAS ▪ DP Protection System ▪ Associated Data Center	Control Center
Description	A description of the BES asset.	String		Primary control center
Commission Date	The date the asset was commissioned if the BES asset was provisioned within the audit period. Otherwise, leave this field blank.	String	ISO 8601 date string	2020-04-15
Decommission Date	The date the asset was decommissioned if the BES asset was decommissioned within the audit period. Otherwise, leave this field blank.	String	ISO 8601 date string	2020-04-15
Location	A brief description of the location of the asset, such as city and/or state name, or floor within a building.	String		Western Idaho
High Impact	The BES asset contains a high impact BES Cyber System.	Boolean		TRUE
Medium Impact	The BES asset contains a medium impact BES Cyber System.	Boolean		TRUE
Low Impact	The BES asset contains a low impact BES Cyber System.	Boolean		TRUE

Level 1 Changes

Detail Tab or Request ID	Standard	Requirement	Evidence Request
CIP-005-7-R1-L1-02	CIP-005-7	R1 Part 1.1	Provide ESP network topology, such as schematics, diagrams, or other documentation, showing the relationship(s) among ESP(s), including identification of all network devices internal to the ESP.
CIP-006-6-R1-L1-02	CIP-006-6	R1	Provide details of PACS network connectivity, such as schematics, diagrams, or other documentation, to control panels at applicable physical access points (e.g., PACS servers, workstations, database units, and/or control panels at physical access points).
CIP-007-6-R2-L1-01	CIP-007-6	R2	Provide each documented process that collectively includes each of the applicable requirement parts in CIP-007 R2.
CIP-007-6-R2-L1-02	CIP-007-6	R2	For each applicable Cyber Asset that is updateable and for which a patching source exists, include the identification of a source or sources that are tracked for the release of cyber security patches.

Split CIP-007-6-R2-L1-01 from ERT v9 into two Request IDs in v10

Level 2 Changes

Request ID	Standard	Requirement	Sample Set Evidence Request
CIP-005-7-R2-L2-01	CIP-005-7	R2 Part 2.1 R2 Part 2.2 R2 Part 2.3	For each Electronic Security Perimeter in Index Sample Set ESP-L2-02, provide: 1. Evidence that an Intermediate System is used such that the Cyber Asset initiating Interactive Remote Access does not directly access applicable Cyber Assets, or that an approved TFE is applicable to Cyber Assets within the Electronic Security Perimeter. [Part 2.1] 2. Evidence that communications between the Cyber Asset initiating Interactive Remote Access and the Intermediate System are encrypted and that encryption terminates at the Intermediate System, or that an approved TFE is applicable to Cyber Assets within the Electronic Security Perimeter. [Part 2.2] 3. Evidence that all Interactive Remote Access sessions require multi-factor authentication, or that an approved TFE is applicable to Cyber Assets within the Electronic Security Perimeter. [Part 2.3]
CIP-005-7-R2-L2-02	CIP-005-7	R2 Part 2.4 R2 Part 2.5	For each Electronic Security Perimeter in Index Sample Set ESP-L2-02, provide: 1. Evidence that method(s) for determining active vendor remote access sessions have been implemented. [Part 2.4] 2. Evidence that method(s) to disable active vendor remote access have been implemented. [Part 2.5]
CIP-010-4-R1-L2-01	CIP-010-4	R1 Part 1.1	For each Cyber Asset in Index Sample Set CA-L2-10, provide the baseline configuration installed in production for this Cyber Asset as of the date in SS-DATE-03 or the most recent version. If baselines are configured by group, denote which Cyber Assets are part of this group and provide the baseline configuration installed in production for this group as of the date in SS-DATE-03 or the most recent version.

Sample from Electronic Security Perimeter tab as opposed to Cyber Asset tab

BES Asset Tab

CONFIDENTIAL

	Contains BES Cyber System							Sample Count:
Location	High Impact	Medium Impac	Low Impa	Accessible Via a Routable Protocol - Low Impac	External Routable Connectivity - High/Medium Impact	Is Vendor Remote Access Enabled to this asset?	Is Dial-up Connectivity present at this asset?	Region (MRO, NPCC, RF, SERC, Texas RE, WECC	Function (TO, TOP, GO, GOP, etc.)

CONFIDENTIAL

	Contains BES Cyber System							Sample Count:
Location	High Impact	Medium Impac	Low Impa	Low Routable	External Routable Connectivity	Vendor Remote Access	Dial-up Connectivit	Regional Entities	Registered Functions

CA Tab

	Cyber Assets							
Index	Cyber Asset	Cyber Asset Classification	Impact Rating	BES Cyber System ID(s)	BES Asset ID(s	Cyber Asset located at and/or associated with Control Center	External Routable Connectivity	Connected to a Network Via a Routable Protocol?

	Cyber Assets/Shared Cyber Infrastructure										
Index	ID	Classification	Virtual (future us	Impact Rating	BES Cyber System IDs	BES Asset ID	Associated with Control Center	SCI ID (future us	VCA Classifications (future use)	Routable	External Routable Connectivity

CA Tab: Virtualization (Project 2016-02 Pending)

ID
Unique ID of Cyber Asset
or
Shared Cyber Infrastructure (SCI)

Classification
- BCA
- EACMS
- PACS
- PCA
- SCI Host

Virtual
True
Or
False

SCI ID
ID of SCI Host in which the VCA resides

VCA Classification
- BCA
- PCA
- EACMS
- PACS
- BCA, PCA
- BCA, EACMS
- BCA, PACS
- PCA, EACMS
- PCA, PACS
- EACMS, PACS
- BCA, PCA, EACMS
- BCA, PCA, PACS
- BCA, EACMS, PACS
- PCA, EACMS, PACS
- BCA, PCA, EACMS, PACS

One or more programmable electronic device, including the software that shares the device resources, that:

- Hosts one or more virtual cyber assets (VCA) included in a BES Cyber Systems (BCS) or their associated electronic access control or monitoring systems (EACMS) or physical access control systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

CA Tab: Virtualization (Project 2016-02 Pending)

Electronic Capabilities					Physical Properties				
IP Address	ESP ID [If Any]	Accessible via Dial-up Connectivity	Is IRA Enabled to this CA?	Is Vendor Remote Access Enabled to this CA?	PSP ID [If Any]	Date of Activation in a Production Environment, if Activated During the Audit Perio	Date of Deactivation from a Production Environment, if Deactivated During the Audit Perio	Cyber Asset Function	If Cyber Asset Function is Other, please specify

Electronic Capabilities										Physical Prope	
IP Addresse	ESP ID	EACMS Controls ESP? (future use)	Dial-up Connectivity	Interactive Remote Acce	Vendor Remote Acce	PSP ID	Intermediate System	Activation Date	Deactivation Date	Device Function	If Function is Other, please specif

The cyber asset or shared cyber infrastructure controls access to an ESP

ELECTRIC RELIABILITY & SECURITY FOR THE WEST

ENGAGE WITH WECC


Reliability & Security
Oversight Update
WECC
April 16, 2026
2–3 p.m. MST


WECC
www.wecc.org | 801-582-0353
155 N 400 W, Salt Lake City, Utah 84103, USA