

NERC News

September 2019

Inside This Issue

Compliance

[NERC Receives New Alignment Issue via Consistency Reporting Tool](#)

[Compliance Guidance Update](#)

[Effectiveness and Enhancement Survey Available](#)

[2020 ERO CMEP Implementation Plan Posted](#)

Reliability Risk Management

[Lesson Learned Posted](#)

[Webinar Resources Posted](#)

Standards

[Webinar Resources Posted](#)

[Nomination Period Open for Standards Committee](#)

[Supply Chain Security Guidelines and Training Presentations Posted](#)

Regional Entity Events

[Upcoming Events](#)

[Filings | Careers](#)

ERO Executive Spotlight – Edward Schwerdt, President and CEO, NPCC

Canadian Coordination and Collaboration Strengthens ERO Enterprise

The reliability and security of the U.S. and Canadian interconnected bulk power system is a shared responsibility inherent in the international ERO Enterprise model. Operational reliability risks, security threats and resilience challenges, such as extreme weather and cyber attacks, are not constrained within jurisdictional boundaries. The interconnected, international grid — which provides important economic, social and environmental benefits to both countries — requires adherence to a comparable set of Reliability Standards and operating principles. As one measure of the extent of this interdependency, Canada exported nearly 9 percent of the electricity it generated to the United States across 34 major international transmission lines in 2018.



The Canadian perspective enhances and is integrated into every level of the ERO Enterprise — from representation on applicable Regional Entity Boards of Directors, NERC’s Board of Trustees and the Member Representatives Committee to participation on significant initiatives and studies at regional committees, task forces and working groups. The activities undertaken in the program areas of Reliability Assessments and Performance Analysis, Standards and Compliance recognize the value in leveraging this North–South interdependency, using the differences to create synergies and implementing a high level of consistency across the multiple regulatory frameworks. [Continued on page 2](#)

Headlines

[Electricity, Oil and Natural Gas ISACs Form Partnership to Strengthen Cyber, Physical Security Collaboration](#)

[Comments Sought on Joint FERC/NERC White Paper on CIP NOPs](#)

Canadian Coordination (cont'd)

An example of accommodating and respecting differences while supporting a high level of comparable reliability is the incorporation of the Québec variance into NERC Reliability Standard PRC-006-3 – Automatic Underfrequency Load Shedding. The variance accommodates the unique operating characteristics of the separate Québec Interconnection while providing design and documentation requirements within the Québec system to arrest declining frequency, assist recovery of frequency following underfrequency events and provide last resort system preservation measures.

Another tool to support international reliability interdependency is the establishment of a comparable mandatory compliance and enforcement framework across the ERO Enterprise. Canadian compliance activities are implemented at a provincial level pursuant to memoranda of understanding (MOUs) and agreements that are tailored to each jurisdiction's unique regulatory structure. These MOUs and/or agreements ensure the application of the same rigor and thoroughness to achieve comparable levels of reliability internationally.

Additionally, the longstanding collaborative efforts to enhance operational coordination and support reliability assessments were recently augmented with increased cooperation and information sharing regarding cyber vulnerabilities and threats. Building on the Canadian experience of assessing and accounting for the energy sufficiency aspects of significant amounts of hydro resources enables the ERO Enterprise to better prepare for increasing volumes of intermittent distributed energy resources.

Working with our Canadian stakeholders, registered entities and provincial governmental and/or regulatory authorities, Northeast Power Coordinating Council's (NPCC's) activities and resources continue to focus on identifying, evaluating and addressing new and emerging issues affecting international bulk power system reliability and security, and improving communication strategies, knowledge transfer and engagement with

stakeholders across northeastern North America. We look forward to continuing to collaborate on emerging and complex issues such as the changing resource mix, energy sufficiency, extreme physical events and cyber security threats, which require focused attention by all those involved in electric reliability.

Edward Schwerdt is president and CEO of NPCC ■■■

Headlines

Electricity, Oil and Natural Gas ISACs Form Partnership to Strengthen Cyber, Physical Security Collaboration

NERC's Electricity Information Sharing and Analysis Center (E-ISAC) and the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) announced an agreement to improve information sharing between the organizations and their members to enhance the cyber security of North America.

Through a variety of tools, both the E-ISAC and the ONG-ISAC analyze potential physical and cyber security threats and, using their respective secure platforms, alert and advise members about mitigating threats. The goals of the E-ISAC and ONG-ISAC under the partnership include:

- Improving security collaboration on common threat information and incident response.
- Providing joint analysis of security concerns and events.
- Advancing effective processes for information sharing and situational awareness.
- Enhancing information sharing among all ISACs.

"Although some of the threats facing the energy sector are daunting, building a stronger collaborative defensive capability between our organizations will pay off before or during a cyber or physical security emergency," said Bill Lawrence, NERC vice president and chief security officer. "This agreement with the ONG-ISAC continues to strengthen the E-ISAC's relationships to predict and help mitigate potential threats to the grid and our increasingly interdependent critical infrastructure."

The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership and collaboration. The E-ISAC designed its information sharing systems to produce unclassified descriptions of the tactics, techniques and procedures adversaries use as well as methods to prevent or mitigate grid security threats.

“Formalizing this important partnership advances efforts to secure infrastructure across the energy sector,” said Angela Haun, ONG-ISAC executive director. “We have successfully established the need for a culture of safety and security, and now we need to take our efforts to the next level by fostering a culture of sharing threat intelligence through trusted relationships.”

The ONG-ISAC serves as a central point of coordination and communication to aid in the protection of exploration and oil and natural gas industry’s production, transportation, refining and delivery systems. The ONG-ISAC analyzes and shares trusted and timely cyber threat information, including vulnerability and threat activity specific to industrial control systems and supervisory control and data acquisition systems.

The E-ISAC and the ONG-ISAC have agreed to use existing policies and procedures for safeguarding sensitive information under the partnership.

NERC Contact: [Kimberly Mielcarek](#) | ONG-ISAC Contact: [Angela Haun](#)

Comments Sought on Joint FERC/NERC White Paper on CIP NOPs

The Federal Energy Regulatory Commission (FERC) is seeking public comment on a white paper jointly prepared by its staff and staff from the NERC. The joint staff white paper proposes to provide transparency and public access to information on violations of mandatory Reliability Standards governing cyber security of the Bulk Electric System while protecting sensitive information that could jeopardize security. [Joint White Paper](#) ■■■

Compliance

NERC Receives New Alignment Issue via Consistency Reporting Tool

NERC received a [new alignment issue](#) pertaining to data requests via the Consistency Reporting Tool. The ERO Enterprise Program Alignment Process enhances efforts to identify, prioritize and resolve alignment issues across the ERO Enterprise. Using this process, NERC captures identified issues from the various resources in a [centralized repository](#). The Consistency Reporting Tool uses a third-party application, EthicsPoint, which allows stakeholders to submit consistency issues— anonymously, if desired.

Compliance Guidance Update

A key factor in the success of compliance monitoring and enforcement of mandatory standards rests on a common understanding among industry and ERO Enterprise CMEP staff of how they can achieve and demonstrate compliance. For many standards, this is straightforward. For others, a variety of approaches may achieve the same objective. Industry develops Implementation Guidance, for industry, and the guidance requires ERO Enterprise endorsement. This guidance provides examples for implementing a standard.

There is one new proposed Implementation Guidance document, addressing [TOP-001-4 and IRO-002-5 Data Exchange Infrastructure and Testing Requirements \(OC\)](#), posted on the [NERC Compliance Guidance web page](#).

Effectiveness and Enhancement Survey Available

The [NERC Compliance Guidance program](#) has been in effect since 2016, and NERC, as part of our continuous improvement efforts, is in the process of assessing the effectiveness of this program. NERC is reaching out to industry for feedback and improvement suggestions.

As users of Implementation Guidance, industry can assist us and affect positive change by completing the short [survey](#). NERC requests you forward this survey to additional personnel you believe may be appropriate to reflect the broader industry.

This is a great opportunity to assist in improving this program from an Implementation Guidance user perspective. **The survey is open through October 11, 2019.**

2020 ERO CMEP Implementation Plan Posted

NERC has posted the [2020 ERO Compliance Monitoring and Enforcement Program \(CMEP\) Annual Implementation Plan](#) (IP). Compliance Enforcement Authorities (CEAs) use this annual operating plan to implement the CMEP. The CEAs, which include NERC and the six Regional Entities, carry out CMEP activities in accordance with the NERC Rules of Procedure (ROP) and Appendix 4C.

It includes the annual identification and prioritization of risk elements. The ERO identifies and prioritizes risks following the Risk Elements Development Process, which you can find as Appendix C in the [ERO Enterprise Guide for Compliance Monitoring](#). The risk elements are becoming more risk-based this year, as risks selected for increased focus are more specific than previously.

The ERO Enterprise is pleased to release an enhanced, easier to use CMEP IP for this year. Collectively, NERC and each RE have worked collaboratively throughout this IP's development to streamline the ROP timing and risk assessment processes into one cohesive narrative, compared to a main IP with several regional appendices as in years past. By streamlining the development in this manner, the ERO Enterprise believes that it is fulfilling the timing and risk assessment obligations of the CMEP IP more effectively and efficiently, which will enhance efforts to modify and adjust going forward. Through this enhancement, the ERO Enterprise will address areas where there may be specific regional considerations in the main risk element description itself.

The ERO Enterprise believes that this will make the IP both more user-friendly and relevant to registered entities. Specifically, the implementation plan represents the ERO Enterprise's high-level priorities for its CMEP. While the ERO Enterprise will determine individual monitoring decisions for each registered entity based on their unique characteristics, registered entities should consider the risk elements and their associated areas of

focus as they evaluate opportunities and their own prioritization to enhance internal controls and compliance operations focus. ■■■

Reliability Risk Management

Lesson Learned Posted

NERC has posted one new Lesson Learned on the [Lessons Learned](#) page.

The [Risks Posed by Firewall Firmware Vulnerabilities](#) Lesson Learned addresses an incident in which an unauthenticated attacker exploited a vulnerability in the web interface of a vendor's firewall, allowing the attacker to cause unexpected reboots of the devices. This resulted in a denial of service condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center. This Lesson Learned is of primary interest to Transmission Operators, Transmission Owners, Generation Operators, Generation Owners, Distribution Providers, Reliability Coordinators and Balancing Authorities.

A successful Lesson Learned document clearly identifies the lesson, contains sufficient information to understand the issues, visibly identifies the difference between the actual outcome and the desired outcome and includes an accurate sequence of events, when it provides clarity.

Webinar Resources Posted

NERC has posted the [streaming webinar](#) and [slide presentation](#) for the September 5, 2019 Winter Preparation for Severe Cold Weather webinar. ■■■

Standards

Webinar Resources Posted

NERC posted the [streaming webinar](#) and [slide presentation](#) from the September 12, 2019 Project 2016-02 – Modifications to CIP Standards | CIP-005 and Associated Definitions webinar. The webinar provided an overview of the proposed CIP-005 and associated definition modifications.

NERC posted the [streaming webinar](#) and [slide presentation](#) from the September 13, 2019 Electromagnetic Pulse (EMP) Task Force webinar.

NERC posted the [streaming webinar](#) and [slide presentation](#) for the CIP-008-6 Requirement Training webinar. FERC issued an order on June 20, 2019, approving CIP-008-6 – Cyber Security – Incident Reporting and Response Planning. CIP-008-6 will be effective on January 1, 2021.

NERC posted the [streaming webinar](#) and [slide presentation](#) from the September 23, 2019 Supply Chain Risk Assessment Data Request webinar.

Nomination Period Open for Standards Committee

Registered Ballot Body (RBB) members and others interested in NERC Reliability Standards are encouraged to submit nominations for industry segment representatives on the Standards Committee (SC). Reliability Standards are mandatory for all bulk power system owners, operators and users in North America, and the SC's oversight role is therefore increasingly important. The SC consists of two members from each of the ten Industry Segments that make up the RBB. In addition, [Appendix 3B](#) of the Rules of Procedure contains special provisions to achieve a balance of representation between the United States and Canada. Industry stakeholders elect SC members, who report directly to the NERC Board of Trustees. The SC meets up to 12 times each year, with four face-to-face meetings and the remainder by conference call. SC members who cannot travel to the meetings may participate by conference call. The [Standards Committee Charter](#) provides a description of the SC's responsibilities.

There are members representing ten segments whose terms will conclude at the end of December 2019. Therefore, the SC is holding an election to fill the two-year terms (2020–2021) for each of the ten segments. When submitting a [nomination form](#), indicate the segment you are interested in for membership. Please see the following table for concluding membership terms.

Membership Terms Concluding			
Segment	Representative	Title	Organization
1	Sean Cavote	Manager, NERC Compliance and Advocacy	Public Service Enterprise Group
2	Michael Puscas	Compliance Manager, Reliability and Operations Compliance	ISO New England, Inc.
3	Todd Bennett	Manager, Reliability Compliance	Associated Electric Cooperative, Inc.
4	Chris Gowder	Regulatory Compliance Manager	Florida Municipal Power Agency
5	Yee Chou	Director, NERC Compliance Services	American Electric Power
6	Jennifer Flandermeyer	Director, Federal Regulatory Policy	Evergy
7	Frank McElvain	Senior Manager, Consulting	Siemens Power Technologies International
8	Robert Blohm	Managing Director	Keen Resources Ltd.
9	Alexander Vedvik	Senior Electrical Engineer	Public Service Commission of Wisconsin
10	Guy Zito	Assistant Vice President, Standards	Northeast Power Coordinating Council

Any Industry Segment that intends to use a special procedure to elect its SC representatives must provide a copy of its procedure to [Linda Jenkins](#) by October 10, 2019.

Anyone may submit a nomination. To be eligible for nomination, a nominee shall be an employee or agent of an entity belonging in the applicable Segment. To allow verification of affiliation, a nominee must be a registered user in the NERC [RBB](#). It is not required that the nominee be the same person as the entity's RBB representative for the applicable Segment. [Appendix 3B](#) of the NERC Rules of Procedure contains instructions. Please submit completed SC [nomination forms](#) to [Linda Jenkins](#) no later than **October 10, 2019**. The SC will hold the election shortly after the nomination period closes.

Supply Chain Security Guidelines and Training Presentations Posted

The NERC Critical Infrastructure Protection Committee (CIPC) approved the following Supply Chain Security Guidelines at their September 2019 meeting:

- Open-Source Software
- Provenance
- Risk Management Lifecycle
- Secure Equipment Delivery
- Vendor Risk Management Lifecycle

Each approved guideline also has an associated training presentation that is also [available](#). The Supply Chain Working Group (SCWG), which reports to the CIPC, developed these guidelines and presentations. ■■■

Regional Entity Events

Midwest Reliability Organization (MRO)

- **CMEP Conference**, October 22 | [Details](#)
- **Reliability Advisory Council Meeting**, October 30 | [Details](#)
- **Security Advisory Council Meeting**, November 6 | [Details](#)
- **CMEP Advisory Council Meeting**, November 19 | [Details](#)
- **MRO Annual Member and Board of Directors Meeting**, December 5 | [Details](#)

Northeast Power Coordinating Council (NPCC)

- **2019 Fall Compliance and Standards Workshop**, November 20–21, Newport, R.I.

ReliabilityFirst (RF)

- **Reliability and Compliance Open Forum Call Conference Call**, October 21 | [Details](#)
- **Reliability and Compliance Open Forum Call Conference Call**, November 18 | [Details](#)
- **Reliability and Compliance Open Forum Call Conference Call**, December 16 | [Details](#)

SERC Reliability Corporation

- **Fall Compliance Seminar**, October 8–9 | [Details](#)

Texas RE

- **Fall Standards and Compliance Workshop** – October 24 | [Details](#)
- **Talk with Texas RE** – November 21 | [Details](#)
- **Board of Directors Meeting** – December 11 | [Details](#)

WECC

- **Reliability and Security Workshop**, October 22–24, Las Vegas | [Register](#) ■■■

Upcoming Events

For a full accounting of NERC events, such as meetings and conference calls for standard drafting teams, other standing committees, subcommittees, task forces and working groups, please refer to the [NERC calendar](#).

- **Improvements to Compliance and Enforcement Pages on NERC.com** – 2:00–2:30 p.m. Eastern, October 8 | [Register](#)
- **FERC/NERC/Regional Entity Cold Weather Event Report Webinar** – 2:00–3:00 p.m. Eastern, October 10 | [Register](#)
- **Member Representatives Committee Pre-Meeting Conference Call and Informational Webinar** – 11:00 a.m.–12:30 p.m. Eastern, October 10 | [Register](#) | [Agenda](#)
- **Recommended Improvements to Interconnection Requirements for Inverter-Based Resources Webinar** – 12:30–2:30 p.m. Eastern, October 11 | [Register](#)
- **GridSecCon 2019** – October 22–25, Atlanta | [Register](#)
- **Board Committees, Member Representatives Committee, and Board of Trustee Meetings** – November 5–6, Atlanta | [Meeting and Hotel Registration](#)
- **Improvements to Compliance and Enforcement Pages on NERC.com** – 3:00–3:30 p.m. Eastern, November 14 | [Register](#)
- **Improvements to Compliance and Enforcement Pages on NERC.com** – 2:00–2:30 p.m. Eastern, December 9 | [Register](#)
- **Probabilistic Analysis Forum** – December 11–13, Atlanta | Registration Coming Soon ■■■

Filings

NERC Filings to FERC

September 6, 2019

[Petition for Regional Reliability Standard BAL-002-WECC-3](#) | NERC and WECC submit a joint petition for the approval of proposed Regional Reliability Standard BAL-002-WECC-3. Proposed Reliability Standard BAL-002-WECC-3 reflects the retirement of Requirement 2 because it is now redundant to a continent-wide requirement in BAL-003-1.1.

September 26, 2019

[Annual Report of NERC on Wide-Area Analysis of Technical Feasibility Exceptions](#) | NERC submits to FERC the 2019 Annual Report of the Wide-Area Analysis of Technical Feasibility Exceptions in compliance with Paragraphs 220 and 221 of FERC's Order No. 706.

NERC Filings in Canada

September 11, 2019

Notice of Filing of Regional Reliability Standards BAL-002-WECC-3 | NERC and WECC submit a joint petition for the approval of proposed Regional Reliability Standard BAL-002-WECC-3. Proposed Reliability Standard BAL-002-WECC-3 reflects the retirement of Requirement 2 because it is now redundant to a continent-wide requirement in BAL-003-1.1. [Petition](#) | [Exhibits](#) ■ ■ ■

Careers at NERC

E-ISAC Security Operations Analyst

Location: Washington, D.C.

[Details](#)

Enforcement Analyst

Location: Washington, D.C.

[Details](#)

Senior CIP Technical Advisor – Advanced System Analytics Modeling and Security

Location: Atlanta

[Details](#)

Human Resource Business Partner

Location: Atlanta or Washington, D.C.

[Details](#)

Senior Auditor – Internal Audit and Corporate Risk Management

Location: Atlanta

[Details](#) ■ ■ ■