Nov. 3, 2023

To: ReliabilityFirst Compliance Contacts
Subject: RF Compliance Program Update Letter – November 2023

NEW! ERO Enterprise Coordinated Oversight MRRE FAQ Posted
NERC posted the updated [ERO Enterprise Coordinated Oversight Program FAQ for Multi-Region Registered Entity](#) (MRRE) to the One-Stop Shop web page.

UPDATED! ERO Enterprise Updates GO/GOP Asset Verification Form

The ERO Enterprise has implemented a new revised [Generator Owner (GO)/Generator Operator (GOP) Asset Verification Form](#), effective Oct. 2, 2023. The updated form ensures that entities have only one form to complete regarding generator assets during the Registration and Coordinated Oversight data collection process.

As before, completing the form will apply to new entities and existing entities where any of the following activities occur:

- Requesting a new registration (New NCR ID)

- Adding/removing assets for existing registered entities (applies to GO and GOP functions)

  - Blackstart changes

  - Building new generation facilities

  - Buying, transferring, or selling assets (ownership changes)

  - Consolidation of assets

  - Footprint changes

  - Retirement of assets

- Activating/deactivating a Coordinated Functional Registration and Joint Registered Organizations

- Changing entity mapping relationships

- Changing entity name

Attached is a copy of the new form for your use. The new revised [ERO Enterprise GO GOP Asset verification Form](#) can also be found on the NERC website or on the [Registration page](#) on the RF Public website under documents. This form does not need to be completed unless any of the above registration activities occur. If you have any questions about this form or the process, please reach out to Bob Folt, Principal Analyst, RAM/Registration, at bob.folt@rfirst.org.

UPDATED! NERC to Issue Section 800 Data Request to Assess the Extent of Cross-Border Operation Control of Bulk Power System Elements

Over the past year, NERC has identified instances of cross-border operation or control of bulk power system elements. Technological advancements, which were previously not available, have enabled dispersed management systems used by distributed energy resource aggregators, Internet-of-Things devices and outage management systems and have increased automation/integration of operational technology networks, increasing the opportunity for cross-border operations.

NERC developed a Section 800 data request (survey) that would enable NERC to identify the extent to which non-U.S. entities have the ability to operate or control U.S. bulk power system assets. Those cross-border operations would include activities stemming from Canada and Mexico, as well as outside of North America.

This data request will be sent to all **Generator Owners, Generator Operators, and Transmission Owners and Transmission Operators**. This data request as presented at the recent Reliability Steering Technical Committee meeting, will allow NERC to assess the extent of risk and begin to evaluate potential next steps.

UPDATE - NERC has sent out announcements and webinar information about this important data request to affected registered entities. The webinar will provide you with important information about the data request and a demonstration of the ERO Portal tool that will be used to submit your responses to NERC. *RF recommends that all Generation and Transmission entities attend this important webinar.* The webinar is now scheduled to be held Tuesday, Nov. 7 at 2:00-3:00 p.m. Eastern. Pre-registration is required. Read the attached notification for more details and registration information.

Important NERC Registration Information You Need to Know

Notification of Additional Changes in 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 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 be liable 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 Bob Folt, Principal Analyst, RAM and NERC Registration, with any questions at bob.folt@rfirst.org.

E-ISAC Membership

As a registered entity, it is important, and expected, that you will join the Electricity Information Sharing and Analysis Center (E-ISAC). E-ISAC membership is available to North American asset owners and operators (AOOs) and select partner organizations, and there is no cost to join. The E-ISAC encourages security individuals with cyber, physical, or operational technology security responsibilities to apply for membership.

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.

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. Alternately, 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.

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.

Monthly Technical Talk with RF Call

The next Tech Talk with RF will be held on Monday, Nov. 13, from 2 to 3:30 p.m. EST.

November 2023 Technical Talk with RF
State Policy Edition

Monday, Nov. 13, 2023, 2:00 PM | (UTC-04:00) Eastern Time (US & Canada)
Join link:
https://reliabilityfirst.webex.com/reliabilityfirst/j.php?MTID=m2037d5cdc5dc3ea6c6b1c2985ff26bad
Webinar number:2307 840 8073
Webinar password: 0123456 (0123456 from phones and video systems)
Join by phone:1-650-479-3207 Call-in toll number (US/Canada)
Access code: 230 784 08073
Please join us on Slido.com using #TechTalkRF as the event code

Intended Audience
- State lawmakers, commissioners, and staff
- Policy makers engaged in state energy regulation
- National associations of regulatory commissioners
- Utility regulatory and government affairs personnel
- Transmission planners plus anyone interested in transmission transfer studies and/or advanced technologies that may enhance reliability on the grid of the future

Agenda Topics

We will be discussing **NERC's Interregional Transfer Capability Study, the aspects of the clean energy transition and emerging technologies**.

John Moura, Director, Reliability Assessment and Performance Analysis – North American Electric Corporation (NERC)
- John Moura will provide an overview, discuss the scope, and proposed timeline for completion of NERC's Interregional Transfer Capability Study (ITCS). As directed by Congressional action, NERC is working on this study, in conjunction with the Regional Entities and industry stakeholders. The study focuses on the reliable transfer of electric

power between neighboring transmission planning areas. The results of and details of the study will be filed with FERC on or before Dec. 2, 2024.

Shane Watts, Sr. Lead Trainer – PJM Interconnection

- Shane Watts will be discussing various emerging technology and tools being developed and used to maintain reliable operation of the electric system. In addition, he will highlight Renewable Portfolio Standards (RPS) and goals within the PJM footprint.

For all Technical Talk with RF calls: WebEx dial-in details will be posted on a monthly basis to the RF website. Please contact Michelle Cross, Manager External Affairs, with any questions, suggestions, or topics of interest for future calls.

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 current always. **Please periodically verify the names, addresses, phone numbers (cell) and email addresses for each Primary Compliance Contact (PCC), Primary Compliance Officer (PCO) and Alternate Compliance Contact (ACC) in the ERO Portal/CORES system.**

NERC Align Training Resources

In addition to the RF Align page, the NERC Align Project page and FAQ document also contain helpful information. 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 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.

UPDATE! Cybersecurity Training for the Utility Workforce

Starting in late October this year, the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), in partnership with Idaho National Labs (INL) will host a series of six cybersecurity training events for our industry. Each event will be three days designed of training for technical practitioners in electric utilities. All utility employees that have a responsibility for managing grid operations and the digital infrastructure of U.S. based electric utilities, including cooperative, public power, tribal, and investor-owned utilities, are encouraged to attend.

This is a DOE sponsored event, and as such there is no cost to attend. There will be one session in six different locations over the next 6 months, with each session covering the same material. The list of locations and dates follows:
- Orlando, FL – Nov. 28 - 30, 2023
- Kansas City, MO – Dec. 5 - 7, 2023
- San Diego, CA – Jan. 17 - 19, 2024
- Dallas, TC – Jan. 23 - 25, 2024
- Buffalo, NY – Apr. 23 - 25, 2024

See agenda below:

Day 1

DOE CyberStrike (Full Day)

Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

OR

ICS Foundations (Full Day)

This course serves the purpose of introducing people into the field of industrial control systems (ICS) / operational technology (OT) and the cybersecurity considerations unique to securing these environments.

Day 2 Morning

CHOOSE 1 Morning Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

OR

DOE CyberStrike (Full Day)
Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.

Day 2 Afternoon

CHOOSE 1 Afternoon Session:

CTI in times of conflict
Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.

Defending Against State Sponsored Attacks
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk, evidence-based approach.

ICS Security for Leaders and Managers
The session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control system OT/ICS environments.

OSINT-Practical Open-Source Intelligence Techniques For Defense
The talk will cover key OSINT skills that analysts can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

Day 3

Red Team / Blue Team Challenge Competition

Participants will work through a series of interactive learning scenarios that enable Operational Technology security professionals to develop and master the real-world, in-depth skills they need to defend real-time systems. It is designed as a challenge competition and is split into separate levels so that advanced players may quickly move through earlier levels based on their expertise. The Grid Netwars experience has been themed for the electricity industry and the scenario has been coordinated to align with industry exercise events.

2023 Upcoming Standards Subject to Future Enforcement - NONE

2024 Upcoming Standards Subject to Future Enforcement		
CIP-004-7	Cyber Security – Personnel & Training	Jan. 1, 2024
CIP-011-3	Cyber Security – Information Protection	Jan. 1, 2024
FAC-001-4	Facility Interconnection Requirements	Jan. 1, 2024
FAC-002-4	Facility Interconnection Studies	Jan. 1, 2024
TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events (Requirements R7, 7.1–7.3, 7.3.1–7.3.2, 7.4, 7.4.1–7.4.3, 7.5, 7.5.1., R11, 11.1–11.3, 11.3.1–11.3.2, 11.4, 11.4.1–11.4.3, 11.5, and 11.5.1)	Jan. 1, 2024
FAC-003-5	Transmission Vegetation Management	April 1, 2024
FAC-011-4	System Operating Limits Methodology for the Operations Horizon	April 1, 2024

FAC-014-3	Establish and Communicate System Operating Limits	April 1, 2024
IRO-008-3	Reliability Coordinator Operational Analyses and Real-time Assessments	April 1, 2024
PRC-002-3	Disturbance Monitoring and Reporting Requirements | Implementation Plan	April 1, 2024
PRC-023-5	Transmission Relay Loadability | Implementation Plan	April 1, 2024
PRC-026-2	Relay Performance During Stable Power Swings | Implementation Plan	April 1, 2024
TOP-001-6	Transmission Operations	April 1, 2024
EOP-012-1	Extreme Cold Weather Preparedness and Operations (Requirements 1–2 effective 4/1/28; Requirement 4 effective 10/1/29)	Oct. 1, 2024

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

Periodic Data Submittals Due in November 2023			
11/30/2023	PRC-004	GO, TO, DP	Protection System Misoperations - Section 1600 data request for Q3, 2023 (July 1 – Sept. 30). **Submit in MIDAS portal.**

Periodic Data Submittals Due in December 2023 - NONE