ERO Enterprise Entity Onboarding Checklist

The Electric Reliability Organization (ERO) Enterprise is looking forward to working with you to maintain the reliability and security of the bulk power system (BPS). Ensuring electric reliability is no small task. To help you get started, the ERO Enterprise has created a short checklist of action items that will help you get involved and keep you up to date on BPS reliability and security matters!

The purpose of this checklist is to help new Primary Compliance Contacts (PCCs), Primary Compliance Officers (PCOs), and Alternate Compliance Contacts (ACCs) with signing up for the applications and communications provided by the ERO Enterprise. To learn more specific details about initial steps for new entities and new entity contacts, please review the ERO Enterprise 101 Informational Package and the ERO Enterprise Registration Procedure.

Required Action Items for Registered Entity Contacts

☐ **Set up an ERO Portal account.** The ERO Portal is used to access the Centralized Organization Registration ERO System (CORES), which is used across the ERO Enterprise for all registration activities, as well as to access Align and the ERO Secure Evidence Locker (SEL), which are used for compliance and enforcement activities.

☐ **Update contact roles in CORES.** Review the CORES Video Library and Chapter 2 of the CORES User Guide.

☐ **Manage ERO Portal application permission rights in the ERO Portal.** Review Chapter 5 of the ERO Portal User Guide.

☐ **Submit Section 1600 Reporting based on NERC Function.** See Table 1.1.

Table 1.1: Section 1600 Reporting

Reporting Type[1]	Description	Required For	Access Needed	Contact E-mail
Demand Response Availability Data System (DADS)	Mandatory semi-annual reporting for entities with dispatchable demand response programs over 10 MW and in service over 12 months	Balancing Authority (BA), Distribution Provider (DP)	OATI NERC Web Portal	dads@nerc.net
Generation Availability Data System (GADS)	Mandatory quarterly reporting of generator performance and outage data for conventional generating units that are 20 MW and larger, including smaller units that are aggregated	GO	OATI NERC Web Portal	gads@nerc.net
Generation Availability Data System Wind (GADS Wind)	Mandatory quarterly reporting of generator performance data for wind plants that are 75 MW and larger	Generator Operator (GOP)	ERO Portal, GADS Wind Data Submission Access	gadswind@nerc.net
Geomagnetic Disturbance Data (GMD)	Mandatory annual reporting of GMD device information and GMD event data or indicating that the entity does not have GMD equipment	GO, Transmission Owner (TO)	ERO Portal, GMD permission(s)	gmd@nerc.net
Misoperations Information Data Analysis System (MIDAS)	Mandatory quarterly reporting of protection system operation and misoperation data for Bulk Electric System (BES) elements or indicating that the entity does not have MIDAS equipment	DP, GO, TO	ERO Portal, MIDAS permission(s)	midas@nerc.net
Transmission Availability Data System (TADS)	Mandatory quarterly reporting of transmission line and transformer outage data for BES elements 100 kV or greater	TO	OATI NERC Web Portal	tads@nerc.net

[1] Solar and BESS facilities do not currently have GADS reporting obligations.

Required Action Items for Registered Entity Contacts (Continued)

☐ **Send an email to nerc.alert@nerc.net to sign up for NERC Alerts.** The email request should read: "*My name is _____, and I am the Primary Compliance Contact for _____ (NCR_____). I would like to register with the NERC Alert System. Please send an email to _____@.com or contact me at ___-___-____ when I have been registered, or if further information is needed.*"

☐ **Submit Periodic Data Submittals based on NERC Function.** Review the ERO Enterprise Periodic Data Submittals Schedule located under the Compliance section on the One-Stop Shop (Compliance Monitoring & Enforcement Program) web page.

☐ **Provide reporting of system events and incidents** (EOP-004 | CIP-008 | Event Analysis Program).

Recommended Action Items for All Registered Entities

☐ **Join the Electricity Information Sharing and Analysis Center (E-ISAC) for free access to cyber and physical security bulletins, webinars, and events.** More information about E-ISAC is available on pages 3–4 of this document.

☐ **Participate in the biennial grid security exercise, GridEx, and the annual grid security conference, GridSecCon.**

☐ **Review past NERC announcements and newsletters on this page.**

☐ **Sign up for the weekly Standards, Compliance, and Enforcement Bulletin.**[2]

☐ **Attend free training events.** Check the NERC calendar to see what's coming up. For Regional Entity training, review the "Stay Informed | Training Opportunities" section in the ERO Enterprise 101 Informational Package.

☐ **Submit a NERC Helpdesk ticket for assistance with any ERO technical support.**

Additional Recommended Action Items Based on Regional Entity

Table 1.2: Region-Specific Applications

Region	Application Names
MRO	**File Transfer Protocol (FTP) sites:** FTP1 - Reliability Analysis | FTP2 - Compliance | FTP3 - Risk Assessment and Mitigation (RAM) | FTP4: Enforcement
NPCC	
ReliabilityFirst	MK Insight
SERC	SERC Compliance & Committee Portal
Texas RE	Texas RE Extranet
WECC	British Columbia | Baja California, Mexico

[2] **REGISTRATION:** If you would like to receive this bulletin or be added to a NERC distribution list, you must first register an account in the ERO Portal. Once you have registered your ERO Portal account, authenticated your credentials with DUO, and completed your profile, please submit a ticket through the Help Desk by selecting the "NERC Email Distribution List" option under the Applications menu. In the Description Box, please specify which lists you would like your email address to be added to. This bulletin is distributed to several lists, including the Standards distribution list (Standards-specific announcements) and the NERC-info distribution list.

TLP:WHITE - Disclosure is not limited

The Electricity Information Sharing and Analysis Center (E-ISAC)

The Electricity Information Sharing and Analysis Center (E-ISAC) reduces cyber and physical risk to the North American bulk power system (BPS) by providing around-the-clock situational awareness and expert analysis. The E-ISAC serves as a trusted source of security information for its North American asset owner and operator (AOO) members and a select group of partner organizations across government and industry.

Created in 1999 and located in Washington, D.C., the E-ISAC is operated by the North American Electric Reliability Corporation (NERC). Both adhere to a strict code of conduct that reinforces the E-ISAC's organizational isolation from NERC's enforcement activities.

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.

The E-ISAC seeks to inform its members and partners through analysis, engagement, and information sharing.

Analysis

The E-ISAC offers the electricity industry quality analysis and rapid sharing of security information on how to mitigate complex, constantly evolving threats to the grid.

At the heart of the E-ISAC's analysis efforts is the 24/7 Watch and a team of analysts who monitor the BPS for incidents as they emerge and provide expert assessments as situations warrant.

Members and partners have access to a suite of analytical products and services, including:

- Real-time incident bulletins
- Reports on current and emerging industry threats, with insights from E-ISAC industry members and government partners
- Monthly reports and webinars on the latest security updates, trends, and news

Additional benefits include the Cybersecurity Risk Information Sharing Program (CRISP), an E-ISAC collaboration with the U.S. Department of Energy and the Pacific Northwest National Laboratory.

TLP:WHITE - Disclosure is not limited

Engagement

As a membership-based organization, the E-ISAC places a premium on building strong relationships with its AOO members and forging strategic partnerships with government agencies, international allies, private sector organizations, and trade associations. The E-ISAC provides engagement opportunities through its events, programs, and workshops.

These include:

- **E-ISAC Monthly Briefings:** Learn about the latest cyber and physical security threats and trends during this monthly webinar. Takes place the first Tuesday of the month; holiday exceptions.
- **Industry Engagement Program:** Industry members participate in virtual and in-person programs to learn about the E-ISAC, build relationships with industry colleagues, and exchange best practices.
- **GridEx:** An exercise that allows participants to engage remotely, GridEx simulates a cyber and physical attack on the North American BPS and other critical infrastructure.
- **GridSecCon:** This conference features world-class training sessions, cutting-edge discussions, and presentations on emerging cyber and physical threats, policy updates, and lessons learned.

The E-ISAC also participates in regional events, speaking engagements, industry conferences, and working groups. To request a speaker for your event, contact speakerrequests@eisac.com.

Information Sharing

The E-ISAC's secure online Portal serves as the central information hub for members and partners. Through the Portal, members can voluntarily exchange information about cyber and physical incidents with full control of how they share this information. They also receive customized access to the latest products and services such as incident bulletins, white papers, webinars, and workshops. Information shared with the E-ISAC are threats that include, but are not limited to, those that do not meet the threshold of mandatory reporting.

To share information with the E-ISAC:

- Post to the E-ISAC Portal: www.eisac.com
- Contact Watch Operations: operations@eisac.com
- Call us: 202-790-6000 (24/7)

Membership

E-ISAC membership is available to North American AOOs and select partner organizations, and there is no cost to join. The E-ISAC encourages security officers, general managers, and other individuals with cyber, physical, or operational technology security responsibilities to apply for membership.

Contact Us

We look forward to hearing from you. Contact memberservices@eisac.com.