



ERO Enterprise Informational Package

New Registered Entities: 101

April 7, 2023

Table of Contents

Preface iii

Welcome v

Introduction vi

 General Information for Registering a New Entity vi

Becoming a NERC Registered Entity..... 1

 Contact Region(s) 1

 Review the NERC Rules of Procedure (ROP) 1

 Read the ERO Enterprise Registration Procedure 2

 Prepare for Compliance with the NERC Reliability Standards..... 2

 Suggested Resources for Future Registered Entities 3

As a Newly Registered Entity 4

 Receive Notice of Listing on the NERC Compliance Registry 4

 Comply with NERC Reliability Standards 4

 Suggested Resources for Standards and Compliance..... 4

 Complete Entity Profile Questionnaires, Inherent Risk Assessments, and Compliance Oversight Plans 4

 Register for NERC Alerts 5

 Access Align and the Secure Evidence Locker 6

 Submit Mandatory Reporting..... 6

 Consider Joining the Coordinated Oversight Program..... 9

 Get Involved 9

 Section 1600 Application User Groups..... 9

 E-ISAC Membership 10

 Stay Informed | Training Opportunities..... 11

 Social Media 11

Appendix A: Registration Timeline Checklists..... 12

 Becoming a NERC Registered Entity 12

 As a Newly Registered Entity..... 12

Appendix B: Membership vs. Registration..... 14

Appendix C: E-ISAC..... 15

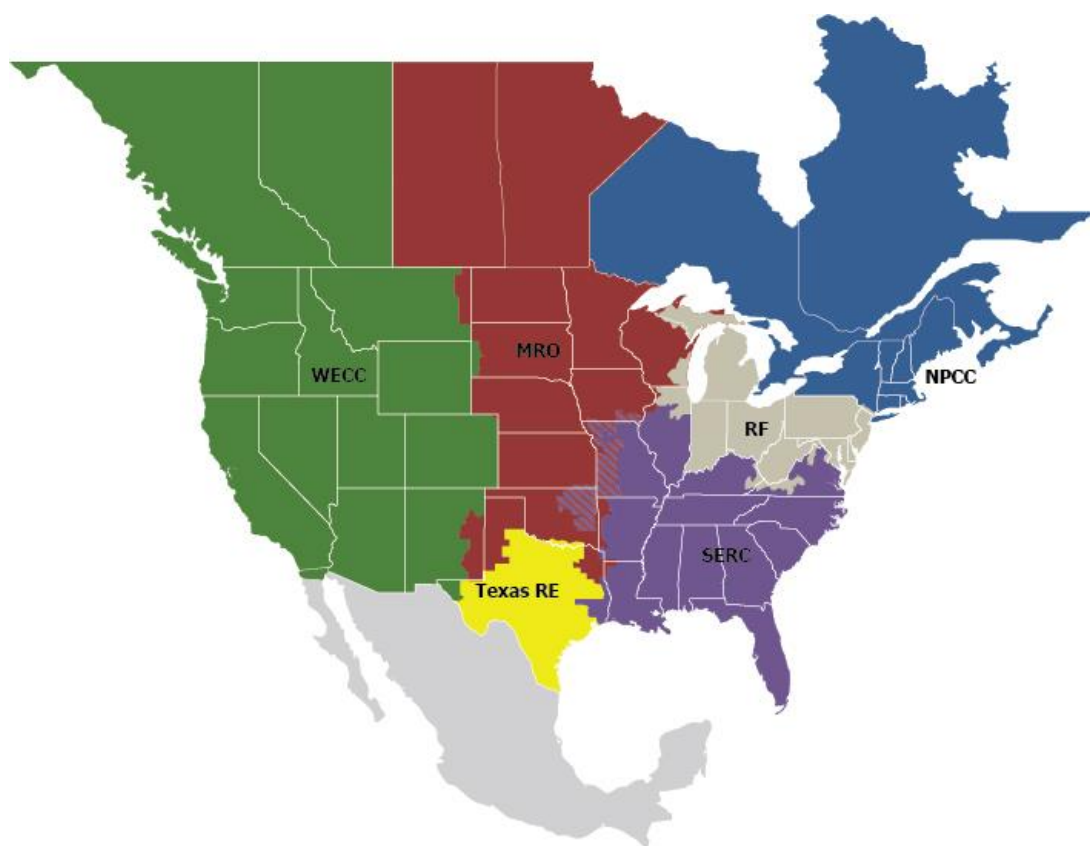
Revision History..... 17

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

In 1968, the National Electric Reliability Council (the original NERC) formed as a voluntary organization after a blackout affected 30 million people in the United States and parts of Canada. In 2003, a blackout occurred in the Northeast that affected more than 50 million people. This incident served as the impetus for the following:

- The Energy Policy Act of 2005 authorized the creation of an audited, self-regulatory ERO.
- The Federal Energy Regulatory Commission (FERC) certified NERC as the ERO, which entered into agreements¹ with the (then) eight REs in 2006.
- NERC became the North American Electric Reliability Corporation, and compliance with approved NERC Reliability Standards became mandatory and enforceable in the United States in 2007.

If you would like to learn more about NERC and the ERO Enterprise, The History of the North American Electric Reliability Corporation² is available on NERC's website. A condensed history timeline³ can also be found on the website.

NERC and the REs are committed to success by working together as one team, developing clear and consistent guidance and supporting initiatives that share best practices across the ERO Enterprise.

¹ [Agreements](#)

² [The History of the North American Electric Reliability Corporation](#)

³ [History timeline](#)

Welcome

The ERO Enterprise currently encompasses regional organizations of similar size and complexity. NERC provides industry-wide perspective and oversight, and the REs have unique features and activities that serve the needs of their regional constituents. While NERC and the REs play different roles in delivering ERO Enterprise programs, these roles are equally important and complementary, allowing the ERO Enterprise to work as one synchronous machine—effectively, efficiently, and collaboratively.

The ERO Enterprise principal activities are as follows:

- Work with industry to develop NERC Reliability Standards.
- Monitor and enforce compliance with NERC Reliability Standards.
- Assess monetary and non-monetary penalties for noncompliance.
- Evaluate the performance and future reliability of the BPS through a comprehensive set of annual assessments.
- Develop special assessments on emerging reliability and security issues as needed.
- Analyze BPS events for lessons learned.
- Help industry train and educate system operators.
- Certify system operators.
- Promote human performance improvement.
- Collect and analyze information on potential cyber and physical security threats.
- Share actionable grid security intelligence and threat indicators with BPS asset owners and operators across North America.

The ERO Golden Circle



None of the work the ERO Enterprise does would be possible without the support of stakeholders. To help you get started, this document includes actions that are necessary for getting involved and staying up-to-date on reliability matters.

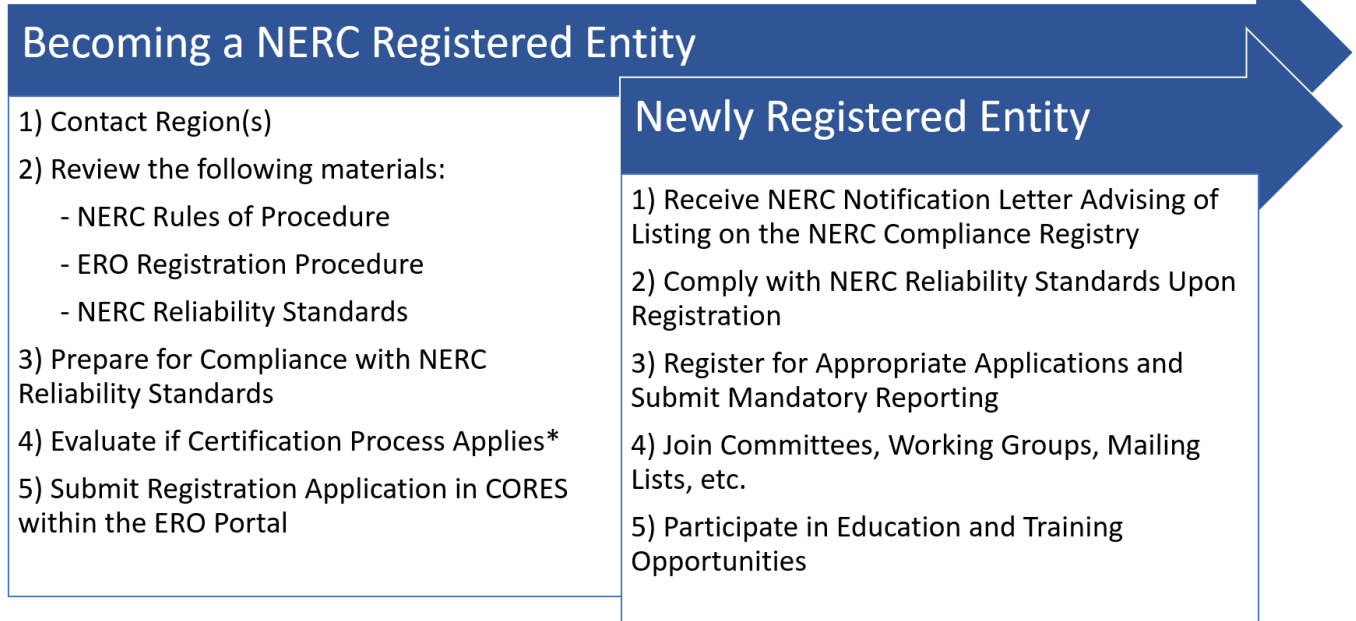
The ERO Enterprise looks forward to working with you to maintain the reliability of the BPS!

Introduction

General Information for Registering a New Entity

This package provides a framework to assist you with becoming a NERC registered entity, including the steps to complete shortly after the registration process has been completed. For those that are already registered, information regarding registration changes, compliance, and performance can be found on the RE and NERC websites.

Overview of Registration Activities: ERO 101



* Future Balancing Authorities, Reliability Coordinators, and Transmission Operators need to complete the certification process prior to registering for these specific functions.

Becoming a NERC Registered Entity

Organization registration identifies and registers BPS owners, operators, and users that are responsible for performing specified reliability functions to which requirements of mandatory NERC Reliability Standards are applicable. An entity that is required to be registered and placed on the NERC Compliance Registry can initiate the process by contacting either NERC Registration or their respective RE. Requirements and activities for the Organization Registration Program are embodied in Section 500 (Organization Registration and Certification) and Appendices 5A and 5B of the FERC-approved [NERC Rules of Procedure](#).

Contact Region(s)

The first step to becoming a NERC registered entity is to contact your applicable RE(s) regarding the Registry Criteria and the Registration process pertaining to your entity or upcoming project(s).⁴

Region Name | Registration Website | Email Address

- Midwest Reliability Organization (MRO) | [Website](#) | [Contact by Email](#)
- Northeast Power Coordinating Council (NPCC) | [Website](#) | [Contact by Email](#)
- Reliability First (RF) | [Website](#) | [Contact by Email](#)
- SERC Reliability Corporation (SERC) | [Website](#) | [Contact by Email](#)
- Texas Reliability Entity, Inc. (Texas RE) | [Website](#) | [Contact by Email](#)
- Western Electricity Coordinating Council (WECC) | [Website](#) | [Contact by Email](#)

Additionally, informative registration information can be found on NERC's Organization Registration and Organization Certification webpage.⁵

Review the NERC Rules of Procedure (ROP)

All BPS owners, operators, and users that meet criteria defined in the Statement of Compliance Registry Criteria found in Appendix 5B of the NERC Rules of Procedure⁶ are required to be NERC registered within the ERO Enterprise. The process for registration is described in Section 500 and Appendix 5A of the NERC Rules of Procedure.

Review the Rules of Procedure, including Appendices. Some topics of particular note include the following:

- **Section 100:** Applicability of Rules of Procedure
- **Section 200:** Definitions of Terms
 - **Appendix 2:** Definitions Used in the Rules of Procedure
- **Section 300:** Reliability Standards Development
 - **Appendix 3A:** Standard Processes Manual
 - **Appendix 3B:** Election Procedure for Members of NERC Standards Committee
 - **Appendix 3D:** Registered Ballot Body Criteria

⁴ It is recommended that you contact your applicable RE(s) at least 45 days prior to your requested registration activity.

⁵ Organization Registration and Organization Certification webpage

⁶ [NERC Rules of Procedure](#)

- **Section 400: Compliance Enforcement**
 - **Appendix 4B:** Sanction Guidelines
 - **Appendix 4C:** Compliance Monitoring and Enforcement Program (CMEP)
 - **Appendix 4D:** Procedure for Requesting and Receiving Technical Feasibility Exceptions (TFE) to NERC Critical Infrastructure Protection Standards
- **Section 500: Organization Registration and Certification**
 - **Appendix 5A:** Organization Registration and Certification Manual
 - **Appendix 5B:** Statement of Compliance Registry Criteria
 - **Appendix 5C:** Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of Bulk Electric System (BES)

Read the ERO Enterprise Registration Procedure

The ERO Enterprise Registration Procedure⁷ provides detailed guidance on required registration activities and criteria to become a registered entity. The procedure also provides registration activities that are either required or available for a newly registered entity. The Centralized Organization Registration ERO System (CORES)⁸ platform enables entities to manage their registration information, contact information, and functional entity mapping relationships within one application. Please review the CORES section in the ERO Enterprise Registration Procedure document for more information on how to obtain access to CORES and submit an application for registration.

Registration activities may include alternative options that entities can use to meet their registration responsibilities, such as Coordinated Functional Registration, Joint Registration Organization, and third-party agreements. It is highly recommended that you review the ERO Enterprise Registration Procedure for clarification on registration and criteria requirements.

When an entity is registering for the first time for the functions of Reliability Coordinator (RC), Balancing Authority (BA), or Transmission Operator (TOP), they must complete the Organization Certification process before their organization is officially registered. During the Certification process, the RE, with input from NERC and neighboring entities, ensures that the RC, BA, or TOP entity has procedures, processes, tools, training, and personnel in place to fulfill their responsibilities. To start the certification process, contact your applicable RE as referenced in the Contact Region(s) section.⁹

Note: This Certification requirement does not apply to those seeking to register for any function or function(s) other than RC, BA, or TOP.

Prepare for Compliance with the NERC Reliability Standards

An entity's compliance obligation begins on the day the entity is registered with NERC unless a Requirement or Reliability Standard implementation plan (or other authoritative document) specifies the date by which the entity is required to be compliant. Per the NERC Rules of Procedure (ROP), Section 400, entities are responsible for compliance with all NERC Reliability Standards that apply to each function for which they are registered. Appendix 5B, Section II identifies the functional types an entity may qualify for based on the functions the entity performs.

⁷ [ERO Enterprise Registration Procedure](#)

⁸ [Centralized Organization Registration ERO System \(CORES\) End User Guide](#)

⁹ It is recommended that you contact your applicable RE(s) about beginning the certification process, at a minimum, one (1) year in advance of your proposed effective registration date as a RC, BA, or TOP.

“An entity preparing for registration must build an effective compliance program prior to registration. It is important to develop processes, procedures, and internal controls to maintain compliance and to retain compliance evidence. The entity should be audit-ready on the day it is registered with NERC. Compliance with NERC Reliability Standards ensures reliability and security.”

A list of NERC Standards by functional applicability is available on the NERC website. Additionally, on the Standards page¹⁰ of NERC’s website you can review a list of mandatory standards¹¹ that are currently subject to enforcement. NERC publishes a complete list of Reliability Standards,¹² along with a One-Stop-Shop¹³ that provides additional helpful Reliability Standards information. It is a good idea to review the Reliability Standards under Development¹⁴ webpage to become familiar with future standards that may apply to your entity. In addition, participation in standard drafting teams is encouraged for projects that are applicable to your registered entity. Finally, all new registrants should understand that the ERO Enterprise utilizes a Risk-Based Compliance Monitoring approach. Compliance monitoring, frequency and scope, will be determined by a number of factors that focus on risk. CMEP staff will ask questions that may go beyond the requirements in the NERC Reliability Standards. This is necessary for the ERO Enterprise to fully understand the risk that may exist and how those risks are mitigated.

NERC and the REs offer educational opportunities to help you develop a strong compliance program. If you have questions about which approved NERC Reliability Standards apply to your entity, contact your applicable RE.

Suggested Resources for Future Registered Entities

- ROP Website¹⁵
- ROP, Section 500¹⁶
- Appendix 5A: Organization Registration and Certification Manual¹⁷
- Appendix 5B: Statement of Compliance Registry Criteria¹⁸
- Appendix 5C: Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of BES¹⁹
- Centralized Organization Registration ERO System (CORES) End User Guide²⁰
- NERC Standards Website²¹

¹⁰ [Standards page](#)

¹¹ [List of Mandatory Standards](#)

¹² [Reliability Standards](#)

¹³ [One-Stop-Shop](#)

¹⁴ [Reliability Standards Under Development](#)

¹⁵ [NERC Rules of Procedure \(ROP\) Website](#)

¹⁶ [ROP, Section 500](#)

¹⁷ [Appendix 5A: Organization Registration and Certification Manual](#)

¹⁸ [Appendix 5B: Statement of Compliance Registry Criteria](#)

¹⁹ [Appendix 5C: Procedure for Requesting and Receiving an Exception from the Application of the NERC Definition of BES](#)

²⁰ [Centralized Organization Registration ERO System \(CORES\) End User Guide](#)

²¹ [NERC Standards Website](#)

As a Newly Registered Entity

Receive Notice of Listing on the NERC Compliance Registry

Once the registration application is accepted by the RE and NERC in CORES, NERC will issue a NERC notification letter that advises of listing on the “NERC Compliance Registry,” including your entity’s NERC Compliance Registry ID number, the Registration effective date, and states that all registered entities are subject to compliance with all applicable NERC Reliability Standards. The current NERC Compliance Registry (NCR) listing is posted on the NERC website.¹⁸

Comply with NERC Reliability Standards

As mentioned in the “Becoming a NERC Registered Entity” section, an entity’s compliance obligation begins on the day the entity is registered with NERC, unless a requirement or implementation plan (or other authoritative document) specifies the date by which the entity is required to be compliant.

“It is important to develop processes, procedures, and internal controls to maintain compliance with the Reliability Standards and to retain compliance evidence. The entity should be audit-ready on the day it is registered with NERC.”

NERC and each RE offers educational opportunities to help you develop a strong compliance program. It is a good idea to review the Reliability Standards under the Development²² webpage to become familiar with future standards that may apply to your entity.

Suggested Resources for Standards and Compliance

- Standards Webpage²³
- Complete Set of Reliability Standards²⁴
- Standards One-Stop Shop²⁵
- Glossary of Terms²⁶
- Reliability Standards Audit Worksheets (RSAWs)²⁷
- One-Stop Shop (Compliance & Enforcement)²⁸

Complete Entity Profile Questionnaires, Inherent Risk Assessments, and Compliance Oversight Plans

Upon registering, the applicable RE will contact your entity for completion and submittal of additional information including an Entity Profile Questionnaire. This questionnaire will provide the RE with a better understanding of your

²² [Reliability Standards Under Development](#)

²³ [Standards Webpage](#)

²⁴ [Complete Set of Reliability Standards](#)

²⁵ [Standards One-Stop Shop](#)

²⁶ [Glossary of Terms](#)

²⁷ [Reliability Standards Audit Worksheets \(RSAWs\)](#)

²⁸ The [One-Stop Shop \(Compliance & Enforcement\)](#) webpage provides a consolidated and sortable listing of the pages located on the left navigation and commonly used documents related to CMEP activities, which includes information regarding the CIP Evidence Request Tool, Compliance Webinars, Checklists, etc.

company's potential vulnerabilities, risks, and characteristics (e.g., how much generation is owned by your entity, your entity's critical cyber assets, interconnectivity, and other information unique to your entity's footprint).

Inherent risk assessments (IRAs) are developed to identify and summarize the individual risk elements unique to your company and their impact and significance based on data and information obtained by REs. IRAs include performance data from Section 1600 requests, audit/compliance history, and positive performance criteria as demonstrated by your documented internal controls.

IRAs are the key input for developing an entity's Compliance Oversight Plan (COP).²⁹ A COP is a document that summarizes the entity's risk categories and oversight strategy. In addition to the inherent risks of the IRA, the COP reviews several aspects of entity performance, such as internal controls and misoperations, as inputs to oversight planning. This process is explained in the September 2020 Compliance Oversight Plan Process Enhancements Webinar that can be reviewed as an Adobe presentation³⁰ or as a recorded session³¹. The oversight strategy illustrates how often to utilize a CMEP process (compliance audit, spot check, or self-certification) plus which risks may be a focus in the CMEP process selected with associated Reliability Services.

Along with an entity's inherent risks, the RE may also focus on the ERO Enterprise risk elements (documented in the annual CMEP Implementation Plan) that are the global risks common to entities. Risk Elements are based upon threats and vulnerabilities discovered and documented in the annual NERC Reliability Issues Steering Committee reports and the annual NERC State of Reliability Report. Each Risk Element has associated areas of focus, which are standards, and requirements associated with the risk element (e.g., MOD-026-1 Requirement 2 is an area of focus for the risk element of *"Poor Quality Models Impacting Planning and Operations"* and may be chosen to be included in an oversight engagement (e.g., compliance audit) of a Generator Owner).

While an entity must adhere to all of the assigned NERC Reliability Standards applicable to its registration, the ERO Enterprise's oversight strategy is risk-based and designed to focus on the risk factors (and associated internal controls) that most impact the reliability of the BPS. Furthermore, the ERO COP Report Template³² states, "The intervals and primary CMEP Tools should not be read to preclude different intervals of CMEP Tools depending on individual registered entity facts and circumstances." Your RE will work with you individually regarding CMEP activities (planned or unplanned) to provide transparency on the risks being addressed and why. More information regarding entity profile questionnaires, inherent risk assessments, compliance oversight plans, and the CMEP Implementation Plan risk elements can be requested by contacting your RE.

Register for NERC Alerts

NERC issues NERC alerts to keep registered entities informed about information that impacts the reliability of the BPS. Generally, NERC distributes alerts broadly to owners, operators, and users of the BPS in North America based on the NERC Compliance Registry ID (NCR ID). Alerts may be targeted to groups of entities based on their registered function(s) (e.g., BAs, Planning Authorities, GOs, etc.). As a result, it is imperative that all registered entities contact NERC via email at NERC.Alert@nerc.net to enroll or revise its listing for the NERC alert system, as applicable. Alternately, an entity may call the NERC Alerts Hotline at 404-446-9797. Instructions to enroll for NERC alerts are also included within the NERC notification letter provided at the time of registration.

²⁹ [COP](#)

³⁰ [Adobe presentation](#)

³¹ [recorded session](#)

³² [ERO COP Report Template](#)

Besides signing up for future NERC alerts, previous alerts can be reviewed on the NERC alerts site.³³ Entities should review all previous NERC alerts that apply to their registration function(s).

For more information, visit NERC's About Alerts³⁴ webpage.

Access Align and the Secure Evidence Locker

The ERO Enterprise collaborated with industry to develop Align and the Secure Evidence Locker (SEL). Align is an ERO Enterprise common platform developed to support CMEP activities and business processes. The tool provides a standardized and consistent interface for REs conducting CMEP activities. The SEL is a highly secure, isolated, encrypted environment that is subject to file destruction policies and serves as a temporary repository to upload sensitive information associated with CMEP activities in Align. As a newly registered entity, you will need to be familiar with these applications and how compliance and enforcement activities will be managed by you and the ERO Enterprise. An ERO Portal account is required to access both applications.³⁵ Below is a list of tools that will help with navigating both systems:

- ERO Portal End User Guide³⁶
- NERC Multi-Factor Authentication Quick Start Guide³⁷
- Align Training Videos³⁸
- Registered Entity Request Access Process³⁹

Submit Mandatory Reporting

In accordance with Section 1600 of the NERC ROP, NERC may request data or information that is necessary to meet its obligations under Section 215 of the Federal Power Act as authorized by Section 39.2(d) of the FERC regulations. Under the Performance Analysis program, NERC currently collects data from registered entities that meet reporting requirements for demand response, generation, transmission, protection system operations, and geomagnetic disturbances.

Each Section 1600 application has associated data reporting instructions that are available through the Performance Analysis section⁴⁰ of NERC's website. The data reporting instructions were developed by NERC with RE and industry support. Other helpful materials, such as user guides and FAQs, are available through each of the associated web pages on NERC's website as well.

Questions regarding each Section 1600 application can be sent to the respective NERC e-mail address shown in the table below.

³³ [NERC Alerts Site](#)

³⁴ [About Alerts](#)

³⁵ Activities may include compliance audits, spot checks, self-certifications, complaints, periodic data submittals, compliance investigations, self-reports, and self-logs.

³⁶ [ERO Portal End User Guide](#)

³⁷ [NERC Multi-Factor Authentication Quick Start Guide](#)

³⁸ [Align Training Videos](#)

³⁹ [Registered Entity Request Access Process](#)

⁴⁰ [Performance Analysis section](#)

Section 1600 Reporting Requirements Listed by Function

Reporting Type ⁴¹	Description	Required Reporting 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	BA, 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	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, 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 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

In addition to Section 1600 reporting, the Compliance Enforcement Authority (CEA)⁴² requires periodic data submittals in accordance with the schedule stated in the applicable Reliability Standards as established by the CEA or as needed in accordance with the NERC ROP, Appendix 4C Section 3.6.

Periodic Data Submittal Reporting Requirements

Reporting Type	Description	Required Reporting For
Periodic Data Submittals	The ERO Enterprise Periodic Data Submittal Schedule is posted ⁴³ on the NERC website to provide registered entities a consistent periodic data submittal schedule throughout the ERO Enterprise by eliminating the regional schedule variations.	See the Periodic Data Submittals Schedule ⁴⁴

⁴¹ Solar and BESS facilities do not currently have GADS reporting obligations.

⁴² CEA is defined in Appendix 2A as follows: "NERC or the RE in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards."

⁴³ [posted](#)

⁴⁴ The current schedule is located on the [One-Stop Shop \(Compliance Monitoring & Enforcement Program\) website](#) under the Compliance section.

Finally, NERC Reliability Standards EOP-004⁴⁵ and CIP-008⁴⁶ also require reporting of system events and incidents. These standards are aligned with NERC ROP Section 800, specifically sections 807 and 808 regarding the analysis of events and disturbances.

Event Reporting Requirements		
Reporting Type	Description	Required Reporting For
EOP-004	<p>EOP-004 is an Operations and Planning Reliability Standard that requires an entity to have an operating plan in accordance with Attachment 1 of EOP-004. Attachment 1 specifies event types and criteria by registration, which must be reported to NERC and other organizations (e.g., the applicable RE(s)). Upon recognition of a triggering event, the report (Attachment 2 of EOP-004) must be submitted by the later of 24 hours or by the end of the responsible entity's next business day. It is important to train and educate staff on this requirement to ensure timely reporting.</p> <p>Events, whether they meet the EOP-004 criteria or not, are generally addressed through the Event Analysis Program (EA Program). The goals of the EA Program are undertaking appropriate levels of analysis to determine the causes of the events, promptly assuring tracking of corrective actions to prevent recurrence, and providing lessons learned to the industry. The EA Program also provides valuable input for training and education, reliability trend analysis efforts, and, possibly, Reliability Standards development. For more information on the ERO Events Analysis Program, including process documents, cause-coding, categorization of events, and lessons learned, see the Event Analysis Program⁴⁷ on the NERC website.</p> <p>Keep in mind that the Department of Energy (DOE) has similar reporting requirements⁴⁸ as the EOP-004 process. Because of this alignment, NERC and the Regional Entities will accept a DOE-417 form in lieu of an EOP-004 form if the entity prefers to use that form for reporting. A copy of the DOE-417 can be submitted in the same manner as an EOP-004 form (Attachment 2) with the same directions as indicated in the EOP-004 standard (e.g., email systemawareness@nerc.net⁴⁹ plus additional applicable organizations).</p>	BA, DP, GO, GOP, RC, TO, TOP
CIP-008	<p>Effective January 1, 2021, applicable NERC registered entities must comply with the expanded incident reporting requirements in revised Reliability Standard CIP-008-6. Reports must be submitted to the E-ISAC⁵⁰ and, for those entities subject to the jurisdiction of the United States, the U.S. Department of Homeland Security Cybersecurity, and Infrastructure Agency (DHS CISA). Staff should work with their compliance departments on their entity's specific requirements and obligations.</p> <p>The E-ISAC is providing this information for situational awareness. If you have specific questions about the revised CIP-008-6 Reliability Standard applicability, or guidance, contact NERC's Compliance Assurance or your respective RE compliance or enforcement Staff.</p>	BA, DP, GO, GOP, RC, TO, TOP

⁴⁵ [EOP-004](#)

⁴⁶ [CIP-008](#)

⁴⁷ [Event Analysis Program](#)

⁴⁸ [similar reporting requirements](#)

⁴⁹ systemawareness@nerc.net

⁵⁰ If you have questions about submitting a CIP-008-6 report to the E-ISAC, contact operations@eisac.com or call 202-790-6000.

Consider Joining the Coordinated Oversight Program

The purpose of the Coordinated Oversight Program is to increase efficiency and eliminate unnecessary duplication of compliance monitoring and enforcement activities for Multi-Region Registered Entities (MRREs). A registered entity operating in or owning assets in two or more REs' jurisdictions with one or more NCR identification numbers is a potential candidate for inclusion in the Coordinated Oversight Program; the program is voluntary. In connection with the program, the ERO Enterprise takes into account reliability considerations, such as— but not limited to— a registered entity's registered functions, load and generation capacity, transmission assets, and transmission and generation control centers. Please refer to the following for more information on joining the Coordinated Oversight Program:

- ERO Enterprise Guide for the MRRE Coordinated Oversight Program⁵¹
- Coordinated Oversight MRRE FAQ⁵²

Get Involved

This section pertains to governance information and available voluntary committees, groups, standard drafting, and membership opportunities. Below are links to the ERO governance structure as well as links to various membership committees for those interested in being involved in governance.

Getting Involved with NERC and Regional Entities			
Organization	Board	Various Committees/Groups	Membership ⁵³
NERC	NERC Board	NERC MRC NERC Committees Standard Drafting Team Vacancies	NERC Membership
MRO	MRO Board	MRO Organizational Groups	MRO Membership
NPCC	NPCC Board	NPCC Reliability Coordinating Committee NPCC Committees	NPCC Membership
RF	RF Board	RF Committees	RF Membership
SERC	SERC Board	SERC Committees	SERC Membership
Texas RE	Texas RE Board	Texas RE MRC CIPWG NSRF	Texas RE Membership
WECC	WECC Board	WECC Committees	WECC Membership

Section 1600 Application User Groups

User groups for the GADS,⁵⁴ MIDAS,⁵⁵ and TADS⁵⁶ applications provide entities with an opportunity to meet with other users of the applications to share ideas, make suggestions for application enhancements, suggest updates to the data reporting instructions, and contribute to the development of application training. The user groups typically meet virtually on a monthly basis.

⁵¹ [ERO Enterprise Guide for the Multi-Region ERO Enterprise Guide for the Multi-Region Registered Entity Coordinated Oversight Program](#)

⁵² [Coordinated Oversight MRRE FAQ](#)

⁵³ An overview that explains the difference in registration and membership is listed within this document under Appendix B.

⁵⁴ [GADS](#)

⁵⁵ [MIDAS](#)

⁵⁶ [TADS](#)

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). Join the E-ISAC for free access to cyber and physical security bulletins, webinars, and events. The E-ISAC⁵⁷ provides around-the-clock situational awareness and expert analysis to reduce cyber and physical security threats to the North American electricity industry. E-ISAC membership is open to all electricity asset owners and operators (AOOs) as well as select government and cross-sector partners, national laboratories, international AOOs, and select security vendors with a demonstrated need to access E-ISAC security information. The E-ISAC is operated by NERC but maintains physical and network separation from NERC's CMEP processes. NERC and the E-ISAC adhere to a code of conduct.⁵⁸

The E-ISAC offers its membership a variety of products and services:

- The E-ISAC Portal,⁵⁹ where members and partners can securely exchange voluntarily shared cyber and physical security threat information
- Reports and bulletins on current and emerging industry threats and trends, featuring insights from experts in the E-ISAC and its partners in the electricity industry and government
- Access to special topic webinars and monthly security briefings
- Participation in GridEx⁶⁰ (biennial grid security exercise) and GridSecCon⁶¹ (annual conference), and the Industry Engagement Program (member engagement program)
- The Cybersecurity Risk Information Sharing Program (CRISP⁶²)— a collaboration between the E-ISAC, the Department of Energy, and the Pacific Northwest National Laboratory

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. To join the E-ISAC, visit www.eisac.com⁶³ and click on “Request Account.”

For more information about membership, send an email to E-ISAC membership services.⁶⁴

⁵⁷ [E-ISAC](#)

⁵⁸ [Code of Conduct](#)

⁵⁹ [E-ISAC Portal](#)

⁶⁰ [GridEx](#)

⁶¹ [GridSecCon](#)

⁶² [CRISP](#)

⁶³ www.eisac.com

⁶⁴ [E-ISAC membership services](#)

Stay Informed | Training Opportunities

The ERO Enterprise promotes a culture of reliability excellence by facilitating ongoing educational opportunities that deliver relevant compliance guidance and encourage stakeholder engagement. The Communications and Training departments use a variety of mediums to communicate important and timely information, coordinates with a wide range of industry organizations, and ensures public content conveys effective messages.

Staying Informed with NERC and Regional Entities				
Organization	About Us	Newsletters	Event Calendars	Outreach Training
NERC	About NERC	NERC News	NERC Calendar	NERC Training
MRO	About MRO	MRO Newsroom	MRO Calendar	MRO Training
NPCC	About NPCC	NPCC News	NPCC Calendar	NPCC Training
RF	About RF	RF Newsroom	RF Calendar	RF Training
SERC	About SERC	SERC Newsroom	SERC Calendar	SERC Training
Texas RE	About Texas RE	Texas RE News	Texas RE Calendar	Texas RE Training
WECC	About WECC	WECC Announcements	WECC Calendar	WECC Training

Social Media

Most areas post information about upcoming events (webinars, workshops) plus important announcements (reliability assessments, papers and publications, NERC alerts) on social media using primarily LinkedIn and Twitter. Key subject matter experts, including both operations and planning and cyber-security professionals, may be interested in these announcements of targeted workshops and opportunities to get involved in committee work and initiatives. Under the discretion of your own social media use policies, consider encouraging employees to follow NERC and the REs on LinkedIn and Twitter.

Social Media	
Available LinkedIn Websites	Available Twitter Websites
NERC LinkedIn	https://twitter.com/NERC_Official
MRO LinkedIn	
NPCC LinkedIn	
RF LinkedIn	https://twitter.com/RFirst_Corp
SERC LinkedIn	https://twitter.com/SERCReliability
Texas RE LinkedIn	https://twitter.com/Texas_RE_Inc
WECC LinkedIn	https://twitter.com/WECCReliability

Appendix A: Registration Timeline Checklists

Below is a brief list of required and recommended actions to take during the various registration phases.

Becoming a NERC Registered Entity

Becoming a NERC Registered Entity		
Complete	Task	Activity Description
<input type="checkbox"/>	Contact Region(s) ⁶⁵	Contact your applicable RE(s) to discuss upcoming registration activities. Email MRO Email NPCC Email RF Email SERC Email Texas RE Email WECC
<input type="checkbox"/>	Read NERC and ERO Documents ⁶⁶	NERC ROP Appendix 5A Organization Registration & Certification Manual Appendix 5B Statement of Compliance Registry Criteria ERO Enterprise Registration Procedure Standards Webpage
<input type="checkbox"/>	Prepare for Compliance w/ NERC Standards	Standards Webpage Reliability Standards Under Development
<input type="checkbox"/>	Evaluate if Certification Process Applies	Appendix 5A Section IV Organization Registration and Certification Manual
<input type="checkbox"/>	Submit Registration Application in CORES	CORES Video Library CORES End User Guide

As a Newly Registered Entity

As a Newly Registered Entity		
Complete	Task	Activity Description
<input type="checkbox"/>	Receive NCR letter	Entity is registered on the NERC Compliance Registry Matrix .
<input type="checkbox"/>	Comply w/ NERC Standards	RSAWs One-Stop Shop (Compliance & Enforcement)

⁶⁵ It is recommended that you contact your applicable RE(s) at least 45 days prior to your requested registration activity.

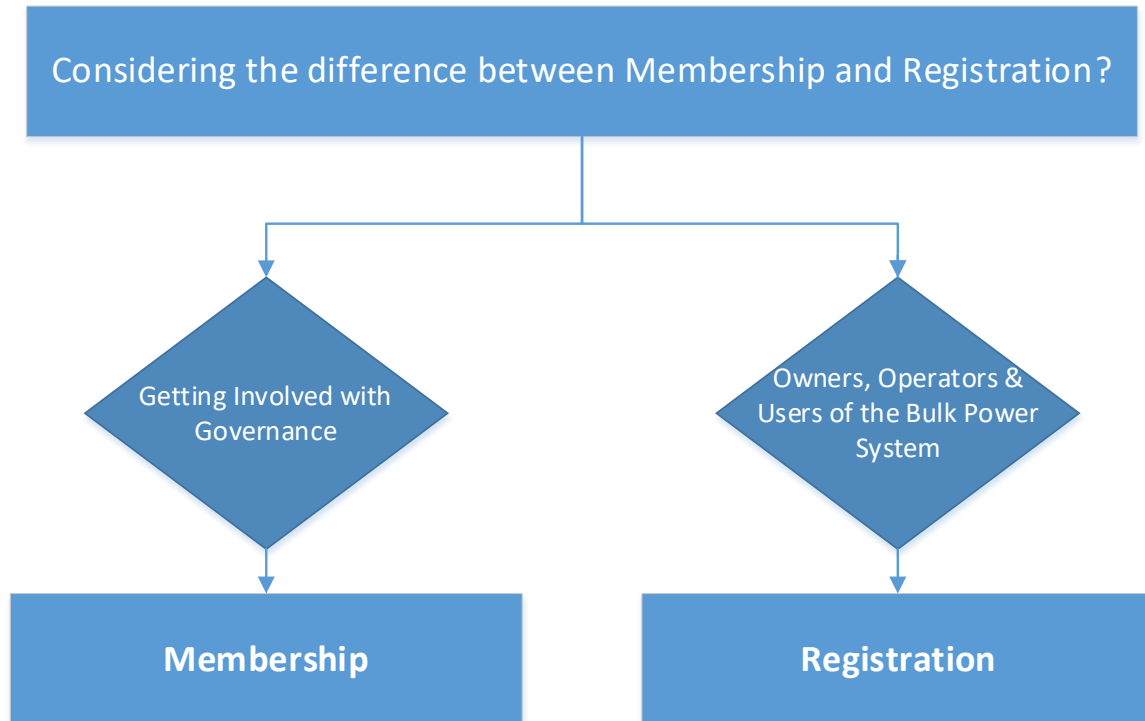
⁶⁶ Appendix 5A and Appendix 5B include information regarding which organizations are required to register for by Functional Entity type.

As a Newly Registered Entity		
Complete	Task	Activity Description
<input type="checkbox"/>	Complete Entity Risk Profile	Contact applicable RE(s). MRO NPCC RF SERC Texas RE WECC
<input type="checkbox"/>	Register for NERC Alerts	Visit NERC's About Alerts webpage. Previous Alerts can be reviewed here .
<input type="checkbox"/>	Access Align & SEL	ERO Portal End User Guide Align Training Videos
<input type="checkbox"/>	Submit Mandatory Reporting	DADS GADS GADS Wind GMD MIDAS TADS Periodic Data Submittals The current schedule is located on the One-Stop Shop (Compliance Monitoring & Enforcement Program) website under the Compliance section. EOP-004 CIP-008 Event Analysis Program
<input type="checkbox"/>	Consider Joining the Coordinated Oversight Program	A registered entity operating in or owning assets in two or more REs' jurisdictions with one or more NERC Compliance Registry (NCR) identification numbers is a potential candidate for inclusion in the Coordinated Oversight Program. ERO Enterprise Guide for the Multi-Region Registered Entity Coordinated Oversight Program Coordinated Oversight MRRE FAQ
<input type="checkbox"/>	Get Involved	NERC MRO NPCC RF SERC Texas RE WECC NERC Board MRO Board NPCC Board RF Board SERC Board Texas RE Board WECC Board NERC Membership MRO Membership NPCC Membership RF Membership SERC Membership Texas RE Membership WECC Membership The Electricity Information Sharing and Analysis Center (E-ISAC) provides its members and partners with resources to prepare for and reduce cyber and physical security threats to the North American electricity industry.
<input type="checkbox"/>	Stay Informed	About NERC About MRO About NPCC About RF About SERC About Texas RE About WECC NERC News MRO Newsroom NPCC News RF Newsroom SERC Newsroom Texas RE News WECC Announcements NERC Calendar MRO Calendar NPCC Calendar RF Calendar SERC Calendar Texas RE Calendar WECC Calendar NERC Training MRO Training NPCC Training RF Training SERC Training Texas RE Training WECC Training

Appendix B: Membership vs. Registration

Membership

NERC and RE membership is a way to engage with the governance process. Membership provides privileges for participating with the ERO Enterprise through Board, Committee and Standards balloting. There is a simple distinction between NERC Registration⁶⁷ and Membership⁶⁸ (see the chart below).



⁶⁷ All BPS owners, operators, and users that meet criteria defined in the Statement of Compliance Registry Criteria found in Appendix 5B of the NERC ROP are required to be NERC registered within the ERO Enterprise.

⁶⁸ Membership is voluntary.

Appendix C: E-ISAC



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.

E-ISAC**RELIABILITY | RESILIENCE | SECURITY**

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.

Revision History

Revision Table		
Revision Number	Date	Description
0	11/5/2021	Original Date
1	4/7/2023	Updated logos Corrected broken links Added Appendix C: E-ISAC