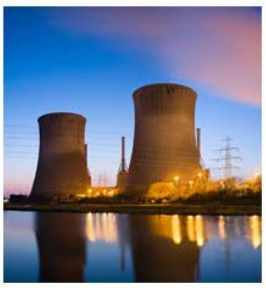
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise CMEP Process

Bulk Electric System (BES) Artifact Submittal Exception Process

April 26, 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

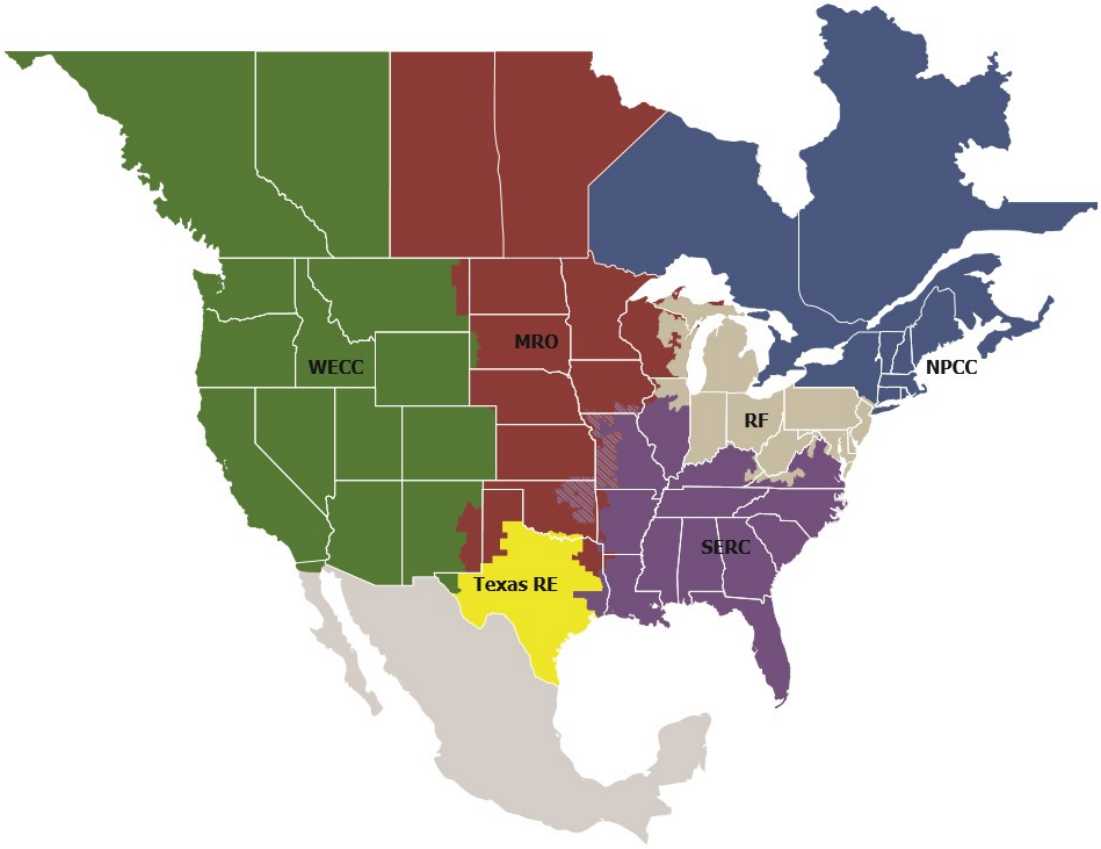
Table of Contents

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 divided into 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 (TOs)/Operators (TOPs) 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

ERO Enterprise Bulk Electric System (BES) Artifact Process

Purpose

The ERO Enterprise at times must review information owned or produced by Registered Entities that could be useful to a person looking to negatively impact the Bulk Power System. This information often includes evidence Registered Entities must provide to demonstrate compliance with NERC and Regional Reliability Standards and Requirements. The ERO Enterprise has designed and is implementing the Secure Evidence Locker (ERO SEL), provided and maintained by the ERO Enterprise, for use by Registered Entities to submit such information (also known as artifacts). This process provides an alternative framework for the Compliance Enforcement Authority (CEA) and a Registered Entity to collaborate on effective and secure evidence submittal in certain cases when a Registered Entity prefers to take additional measures, at its own expense, to submit certain sensitive information outside of the ERO SEL.[1] This provides clarity on the ERO Enterprise process for obtaining certain compliance monitoring and enforcement artifacts in a manner that enables the ERO Compliance Monitoring and Enforcement Program (CMEP) staff to carry out its statutory and regulatory responsibilities.

ERO Enterprise Practice

Pursuant to the NERC Rules of Procedure, the ERO Enterprise has the authority to collect evidence in a manner it deems most appropriate from a Registered Entity to carry out the CMEP.[2] To maintain consistency and to provide enhanced security in evidence collection among Regional Entities, the ERO Enterprise is in the process of implementing the ERO SEL to support effective data and information handling security practices.

The ERO Enterprise developed the ERO SEL for temporary storage of all Registered Entity artifacts. The ERO SEL is a highly secure, isolated, and on-premises at NERC environment designed to protect submitted Registered Entity artifacts. The ERO SEL enables a Registered Entity to securely submit evidence through an encrypted session. The artifacts are encrypted immediately upon submission, securely isolated per Registered Entity, never extracted, never backed up, and subject to proactive and disciplined destruction policies. Additionally, using the ERO SEL provides security advantages over several decentralized platforms to ensure proper protection and chain-of-custody management. The ERO SEL will provide the necessary functionality to allow the evidence to be reviewed by ERO CMEP staff in a manner that enables them to perform their responsibilities.[3]

---

[1] The use of an alternative framework is limited to highly sensitive information as identified on the Bulk Electric System (BES) Cyber Security Artifact list, attached to this process as Appendix A.

[2] The NERC Rules of Procedure, Appendix 4C, Section 3.0, states: "The Compliance Enforcement Authority has authority to collect Documents, data and information in the manner it deems most appropriate, including requesting copies of Documents, data and information to be made and removing those copies from the Registered Entity's location in accordance with appropriate security procedures conforming to Section 1500 of the Rules of Procedure and other safeguards as appropriate in the circumstances to maintain the confidential or other protected status of the Documents, data and information, such as information held by a governmental entity that is subject to an exemption from disclosure under the United States Freedom of Information Act, or a comparable state or provincial law, that would be lost of the information were placed into the public domain." NERC Rules of Procedure, Appendix 4C, available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx

[3] Owners, operators, and users of the Bulk Power System registered on the NERC Compliance Registry shall comply with authorized requests for data and information. In the event a Reporting Entity within the United States fails to comply with an authorized request for data or information under Section 1600 of the Rules of Procedure, NERC may request the Commission to exercise its enforcement authority to require the Reporting Entity to comply with the request for data or information and for other appropriate enforcement action by the Commission.

The ERO SEL architecture and operational model will adhere to the National Institute of Standards and Technology (NIST) 800-171 security control framework, which is established to protect Controlled Unclassified Information (CUI) in nonfederal systems (Critical Energy Infrastructure Information (CEII) is classified as CUI). The ERO SEL is thus designed to significantly reduce risk of evidence loss and exposure.

A Registered Entity may choose to develop its own SEL. In such instances, the SEL must be in accordance with the functionality criteria outlined on NERC's website, and verified and approved by the ERO Enterprise prior to being used.[4] As such, a Registered Entity maintained SEL may be used to submit artifacts identified in Appendix A and neither requires nor prohibits the use of this alternative method process.

While the ERO Enterprise anticipates that the majority of Registered Entities will use the ERO SEL and a few will use their own SEL, some Registered Entities indicated that they would prefer coordinating additional measures for their submission of certain artifacts. As such, Registered Entities, with ERO Enterprise input, created a BES Cyber Security Artifacts list, Appendix A, that refers to those artifacts that some Registered Entities may consider highly sensitive such that they would be willing to coordinate additional measures and/or expense to provide them for CEA review outside of the ERO SEL (or outside of their own SEL, as applicable).[5]

In consultation with its CEA, a Registered Entity may request to make certain information identified in Appendix A available via means other than the ERO SEL. The information must be provided in a manner that is agreed upon by the CEA. Further, this alternative may require additional time and resource commitments by the Registered Entity. In the event a Registered Entity fails to make requested evidence available, the CEA may execute the steps described in the NERC Rules of Procedure, including Attachment 1 of Appendix 4C, Process for Non-submittal of Requested Data.[6]

[4]Registered Entity Provided Secure Evidence Lockers, Functional Specification, April 29, 2020 Rev 6, available at https://www.nerc.com/ResourceCenter/Align%20Documents/1-Align-Registered%20Entity%20SEL%20Functional%20Requirements%20Updated%20April%2029%202020.pdf.

[5]Registered Entities that choose to coordinate alternate means according to this process must separately coordinate with NERC and any applicable governmental authorities to provide the evidence in a manner convenient to NERC and AGAs should NERC or the AGA determine it needs to review evidence, as it will not be available in the ERO SEL (e.g., as part of NERC's regular oversight of REs or in support of reviewing enforcement actions). Also, since NERC is coordinating read-only access to the ERO SEL to FERC staff members when they are participating as observers or when they otherwise need to review Registered Entity evidence, entities that choose to coordinate for alternate means according to this process are individually responsible for all aspects of coordinating with FERC for the delivery of any of the artifacts to them.

[6]Pursuant to section 3.0 of the CMEP, the CEA has authority to collect Documents, data and information. Attachment 1 of Appendix 4C details the steps the CEA may take if a Registered Entity fails to produce requested data or information. NERC Rules of Procedure, Appendix 4C, available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

Alternative means for submitting artifacts identified in Appendix A are subject to the planning, scheduling, and personnel considerations of the CEA. To ensure ERO CMEP staff have sufficient time and capabilities to effectively review all artifacts, this could include, and is not limited to:

- Additional hardware, (e.g., laptops, secure removable media, etc.), provided by the Registered Entity at its own expense.
- Additional travel expenses of Registered Entity personnel. For example, Registered Entity personnel may be required to travel to the CEA's location with the evidence.
- Longer on-site compliance monitoring engagements to ensure adequate time to review the evidence, either concurrently or as separate on-site visits before an audit. This includes all coordination for conference room space and staff availability at the Registered Entity. For example, rather than reviewing the evidence in the ERO SEL, the CEA may expand the on-site portion of a given engagement (such as by adding one, two, or more weeks to the engagement, etc.)

Exception Process Overview

A Registered Entity seeking to coordinate additional measures under this process must coordinate with its CEA before the initiation of a CMEP activity. This process does not apply to a CMEP activity after a Registered Entity receives notice, pursuant to the NERC Rules of Procedure, of such activity.

Step 1 – Registered Entity Submittal

The Primary Compliance Contact for the Registered Entity must submit, at a minimum, the following information to its CEA to begin coordination under this process:

1. Entity name (MRRE Group Name (if applicable))
2. Entity NCR#(MRRE Group Name (if applicable))
3. Entity contact name and information
4. Description of Artifacts from Attachment A for which Registered Entity is requesting to coordinate alternate means of submission (please do not include sensitive information).
5. Description of alternate means of submission

Submittals must be sent to the Registered Entity's CEA (if in the Coordinated Oversight Program, to the Lead Regional Entity).

Step 2 – CEA Coordination

Within 15 calendar days, the CEA will electronically acknowledge receipt of the submittal by the Registered Entity. The CEA may request further information or request follow up coordination with Registered Entity staff to discuss alternate means that may be available.

Step 3 – CEA Review and Registered Entity Notification

The CEA will then perform a review of the Registered Entity's exception submittal request with consideration of CEA resources and staffing, and it will coordinate with the Registered Entity to provide applicable evidence to the submittal process. The Registered Entity may also choose to submit the evidence via the ERO SEL, or its own SEL, if it is unable to provide the evidence via the alternative means described by the CEA.

The CEA will complete this review within 45 calendar days or provide notification to the submitting entity

that it is extending the time needed for review.

If the Registered Entity disagrees with a decision by the CEA about its exception submittal request, the Registered Entity may have its decision reviewed by the Vice President (or designee) at the CEA who is responsible for Compliance Monitoring. The decision from such review for purposes of this process is final.[6]

[6] The review of the exception submittal request determination is not to be confused with the reasonableness of a request for Documents, data or information. See NERC Rules of Procedure, Appendix 4C, §3.0, available at: https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

Appendix A: List of Registered Entity Bulk Electric System (BES) Cyber Security Artifacts

1. Vulnerability Assessments
2. Electronic Security Perimeters, including Firewall Rules
3. Electronic Access Control and Monitoring Systems
4. Network Device Configuration Files
5. BES Cyber Systems and Configurations
6. Enabled Ports and Services
7. Physical Access Control Systems
8. Physical Security Perimeters
9. One line diagrams
10. Protected Cyber Assets
11. Generic or Default Accounts
12. Cabling and Communication Components
13. Security Plans or Programs
14. TFE Details
15. Device Password Restrictions
16. Information Secure Handling Procedures