NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Data Handling in Align and the SEL

August 2021

RELIABILITY | RESILIENCE | SECURITY




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

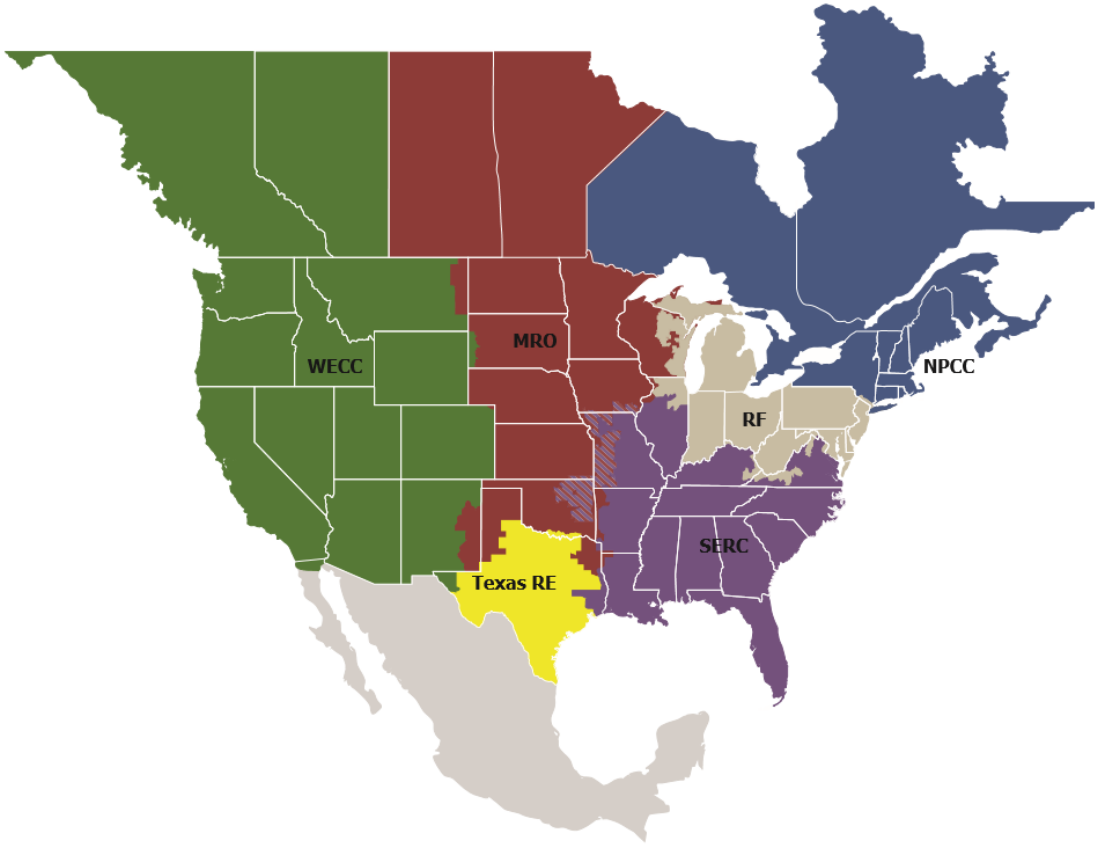
Table of Contents

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

Data Handling in Align and SEL

Purpose

The ERO Enterprise at times must review information owned or produced by registered entities that relates to Bulk-Power System (BPS) operations and planning. This information often includes evidence registered entities must provide to demonstrate compliance with NERC and Regional Reliability Standards and Requirements, as well as information to determine the risk on the BPS. The ERO Enterprise has implemented the Secure Evidence Locker (SEL), provided, and maintained by the ERO Enterprise, for use by registered entities to submit evidence (also known as artifacts) for assessment. This guidance provides clarity regarding the storage and maintenance of registered entity and ERO Enterprise-created or -provided information related to Compliance Monitoring and Enforcement Program (CMEP) activities in Align and the SEL. This guidance is to provide general principles to support ERO Enterprise program alignment, but individual facts and circumstances, as well as experience with the Align and SEL systems, may shape ERO Enterprise actions. Based on the guiding principles[1] in the Align and SEL development, the ERO Enterprise collects, assesses, and temporarily stores all registered entity-provided artifacts in the SEL. In addition, the ERO Enterprise develops and maintains its own workflows and work products within the ERO Enterprise Align tool. Through the ERO Enterprise Align tool, registered entities may provide responses, narratives, descriptions, and other information that do not require an attached document.

ERO Enterprise Systems

Align Overview

As the ERO Enterprise continues to mature to a risk-based approach in its regulatory posture, a more comprehensive system to manage and analyze all aspects of ERO Enterprise compliance monitoring and enforcement processing has been implemented. The CMEP Technology Project began in 2014 to meet that need with the goal of improving and standardizing processes in the Compliance Monitoring and Enforcement Program (CMEP) across the ERO Enterprise. The project has positioned the core CMEP business processes of NERC and the Regional Entities on a single, secure platform that allows improved documentation, sharing, and analysis of compliance work activities. This project was designed to assist the ERO Enterprise achieve its mission to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Align Benefits

The Align tool provides:

- Alignment of common CMEP business processes, ensuring consistent practices and data gathering across the ERO Enterprise.
- A secure standardized interface for registered entities to interact with the ERO Enterprise.
- A secure, efficient communications channel providing real-time access to information.
- A capability for a more consistent application of the CMEP.

The ERO Enterprise uses the Align tool to inquire about specific information to perform specific CMEP activities, as well as to request artifacts that are then submitted in the SEL environment. However, ERO

[1] https://www.nerc.com/ResourceCenter/Align%20Documents/March%2023%202020%20Stakeholder%20Align%20and%20Locker%20Meeting.pdf

Enterprise staff must use caution to include sufficient information in a request for information but without including verbatim language from SEL-submitted artifacts. Appendix A of this document contains specific examples of how to handle that.

SEL Overview

To maintain consistency and to provide enhanced security in evidence collection among Regional Entities, the ERO Enterprise implemented the ERO SEL to support effective data and information handling security practices. The ERO Enterprise SEL is designed to protect submitted registered entity artifacts; it is secure, isolated, and on-premises in the NERC environment.

Registered entities submit artifacts in the SEL environment for ERO Enterprise staff to view and analyze (or their own SEL, where approved).[2] ERO Enterprise staff cannot extract these artifacts, nor do they have the ability to cut and paste information from an artifact to a supporting work paper outside of the SEL environment.

SEL Benefits

The ERO Enterprise developed the ERO SEL to safeguard temporary storage of all registered entity artifacts. The ERO SEL:

- Enables a registered entity to securely submit artifacts through an encrypted session.
- Immediately encrypts artifacts upon submission.
- Securely isolates artifacts per registered entity; the artifacts cannot be extracted, are not backed up, and are subject to proactive and disciplined destruction policies.

The ERO SEL securely holds all registered entity artifacts associated with CMEP processes for registered entities and provides the necessary functionality to allow ERO Enterprise staff to review the artifacts in a reliable and consistent manner.

Align and/or SEL Access

Regional staff is responsible for controlling access to the Align and SEL environments. For example, regional data custodians will only allow NERC staff access to specific data within the SEL, typically based on oversight engagements. In short, NERC staff does not have unfettered access to the ERO Enterprise SEL environment. In addition, regional staff may use contractors to assist in CMEP activities, and should follow access processes in determining the appropriate level of access and controls to Align and the SEL.

Artifact Retention

The retention period for artifacts in the ERO SEL will vary based on circumstance and will adhere to the Rules of Procedure (RoP). Artifacts that are associated with possible noncompliance will remain in the ERO SEL for no more than two years after the completion of FERC's approval of the filed/submitted noncompliance, at which time they will be deleted from the ERO SEL. For Canadian entities using the SEL,

[2] ERO Enterprise BES Artifact Submittal Exception 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. That process is available at https://www.nerc.com/ResourceCenter/Align%20Documents/ERO%20Enterprise%20BES%20Artifact%20Submittal%20Exception%20Process_04262021_v2_CLEAN.pdf.

the retention period will be that specified by the applicable Canadian governmental authority. The registered entity has an obligation to retain its own copy of the submitted artifact(s) for the five-year retention period associated with CMEP data and evidence, and they must be able to resubmit it to the ERO SEL upon request (e.g., NERC/FERC future oversight engagements, etc.).

Any files created by the CEA that reside within the ERO SEL (such as auditor notes, calculations, and sampling) will be subject to the same retention and destruction process as registered entity-submitted artifacts.

CEA staff is responsible for the implementation of this retention policy, and is subject to NERC oversight.

ERO Staff Documentation

ERO Enterprise staff documentation is an essential element of the CMEP quality. ERO Enterprise staff use the Align tool to store their supporting work papers. ERO Enterprise staff documentation, e.g., work papers, should record the work performed and evidence examined to support significant findings and conclusions, including descriptions and records examined; however, the supporting documentation should not recreate the registered entities documentation submitted via a SEL. In other words, ERO Enterprise staff must create work product to support conclusions without the need to store the registered entity data for extended periods or recreate registered entity SEL artifacts. For example, Align will not store registered entity submitted artifacts; however, it must store the CMEP created work papers that contain sufficient information to support the CMEP engagement findings and conclusions, and risk information. Appendix A of this document provides specific examples.

Appendix A – Align and SEL Examples

CIP Examples
Example 1 – Questions concerning a registered entity firewall ruleset

During a review of a registered entity firewall configuration artifact within the ERO Enterprise SEL, CMEP staff has a concern around a ruleset that allows overly broad access to BES Cyber Systems. The ruleset has all the IP addresses to the critical systems as well as the ports and services allowed.

For example, the artifact states on line 222 that anyone outside the ESP can access the internal network (192.168.1.1/255.255.0.0) through HTTP and HTTPS (ports 80 and 443). ERO Enterprise staff may ask the registered entity to provide more information around the rule and may use the request for information workflow within the Align tool.

ERO Enterprise staff may want to ask the registered entity, "Line 222 of the firewall configuration file appears to be providing overly broad access on several ports, please provide further explanation on why the ports may be open to the all the allowed hosts." This line of questioning does not specify the actual IP address nor the ports.

While this is only an example of the question that may be asked, a verbal conversation with the registered entity could also be used to clarify the request if needed, but the conclusion reached by ERO Enterprise staff should be documented in the appropriate work papers.

Example 2 – ERO Enterprise Work papers

In a continuance of example 1, how should ERO Enterprise staff document their concerns in work papers in Align? Based on example 1's questions, one method would be to capture that "the registered entity has an overly broad firewall ruleset that allows access on two specific ports from all IP addresses outside the ESP to all BES Cyber Assets within the ESP".

Typically, the facility and/or location are used to determine the possible risk, therefore, ERO Enterprise staff could state the impact rating of the affected BES Cyber Systems and not provide the exact location and/or IP address. Additionally, device types and/or functions, and potential access to the EMS would be used to determine the risk of a non-compliance. This information should be captured in work papers in Align.

O&P Examples
Example 3 – Questions concerning initial training on three-part communication (COM-002-4 R2)

During a review of evidence in the ERO SEL of a registered entity's training program concerning three-part communication when issuing Operating Instructions, it was not apparent; 1) that training was provided to each member of its operating personnel and 2) what controls are in place to provide the training to new operating personnel. The list of current operating personnel contains full operator names, their work phone numbers, and their personal phone numbers. Their current procedure shows that onboarding training for new operators includes three-part communication training.

For example, the training log is named “Three-Part Training Log.pdf” and is dated March 2018 and includes records for 5 employees with personally identifying information such as work numbers, personal numbers, home addresses, and social security numbers. The log lists Peter Peterson who left the company in June 2018, and does not contain Rick E. Xample who started working in an operating capacity on March 2019.

ERO Enterprise staff may ask the registered entity, by use the request for information workflow within the Align tool, to provide more information about how the entity decides who is operating staff and what controls are in place to ensure new hires are given the three-part communication training. A verbal conversation with the registered entity could be used as well, but the conclusion reached by ERO Enterprise staff should be documented in the appropriate work papers. ERO Enterprise staff may want to ask the entity, “This file “Three-Part Training Log.pdf” seems to only be accurate for March 2018, and does not appear to have been updated. How can you be sure on an ongoing basis you are fulfilling the requirement? Also, what evidence is available to show that Rick E. Xample has received the training required by COM-002-4 R2?”

Example 4 - ERO Enterprise Work papers

In a continuance of example 3, how should ERO Enterprise staff document their concerns in work papers in Align? Based on example 3’s questions, one method would be to capture that the registered entity has provided a file, “Three-Part Training Log.pdf”, dated March 2018 that is a snapshot of who received training, but is not updated on an ongoing basis as evidenced by it not capturing personnel changes since March 2018. It does not reflect an employee left the entity in June 2018 and another joined in March 2019, and does not show the new employee received training. The ERO Enterprise staff has requested documentation or explanation of controls that would ensure new employees designed as operating staff receive the required training, and in particular, whether Rick E. Xample received the training. This information should be captured in work papers in Align.

Appendix B – Data Examples

Align is a secure platform that is used by the ERO Enterprise to review and document information related to CMEP activities. If the registered entity has questions about whether certain information may be shared in Align, the registered entity should contact its CEA to discuss where the information should be provided.

Align should be used to submit narrative information, while the SEL should be used to submit evidence and attachments. However certain information, such as that identified in the list below, should be uploaded into the SEL.

1. Location information (with detailed vulnerabilities, IP addresses, etc.)
2. Details of one-line diagrams
3. IP addresses
4. Details of ESP diagrams
    a. IP addresses
5. Details of network configurations
    a. IP addresses
    b. Ports and services
    c. All network rules
6. Ports and services
    a. IP addresses
    b. Network accessible ports and services
7. Inventory of enabled default or other generic accounts
8. Details of baseline configurations
    a. IP addresses
    b. Ports and services
9. Details of PSP diagrams
10. Vulnerability assessment results
    a. IP addresses
    b. Ports and services
    c. Examples of cyber or physical vulnerabilities
11. Security information regarding BES Cyber Assets
    a. BES Cyber System names if tied to other information such as IP addresses, location, vulnerability, etc.
    b. Specifics of protections in place such as detailed explanation of how the two-factor authentication works in their system

c. BES Cyber Asset names if tied to other information such as IP addresses, location, vulnerability, etc.