NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Registered Entity Maintained Secure Evidence Lockers

Functional Specification
November 3, 2020 Rev 8

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

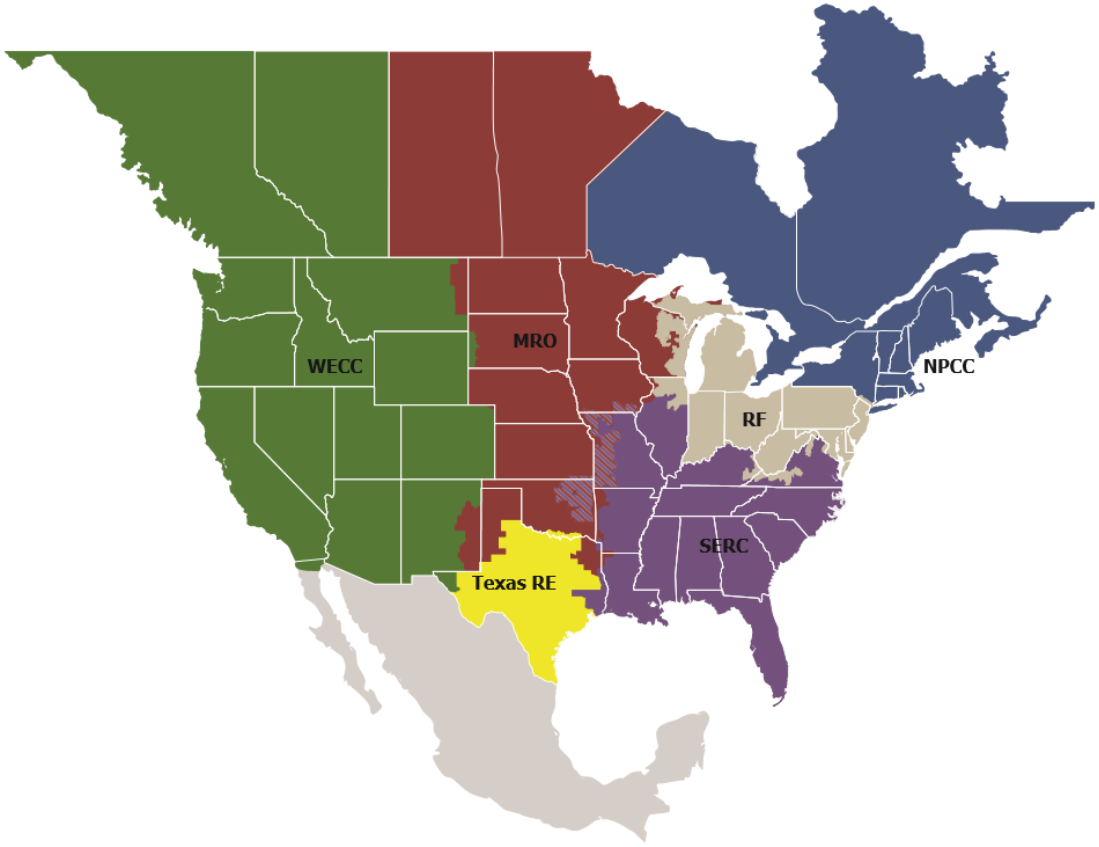
Preface

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 Region 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	Western Electricity Coordinating Council

Introduction: Purpose and Audience

The ERO Enterprise[1] 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. In collaboration with stakeholders, the ERO Enterprise has proposed the concept of Secure Evidence Lockers (SEL). These lockers would implement the principle of least privilege, with the goal of ensuring that only those with a need to see information would be able to do so. Additionally, the architecture of the SEL would be such that it would reduce the likelihood of data loss.

There are two different types of SELs:

- An ERO Enterprise SEL, provided and maintained by the ERO Enterprise, and used by registered entities to submit such information to the ERO Enterprise, and
- A registered entity SEL, provided and maintained by a registered entity, and used by the registered entity to submit information to the ERO Enterprise.

[1] The ERO Enterprise is comprised of those employees and contractors of NERC, Texas RE, SERC, NPCC, WECC, MRO, or RF.

Key Functional Requirements

Access to Registered Entity Maintained SELs

Upon Primary Compliance Contact or Alternate Compliance Contact receipt of an email request from the ERO Enterprise, Registered Entities maintaining their own previously ERO Enterprise validated SEL shall provide the following:

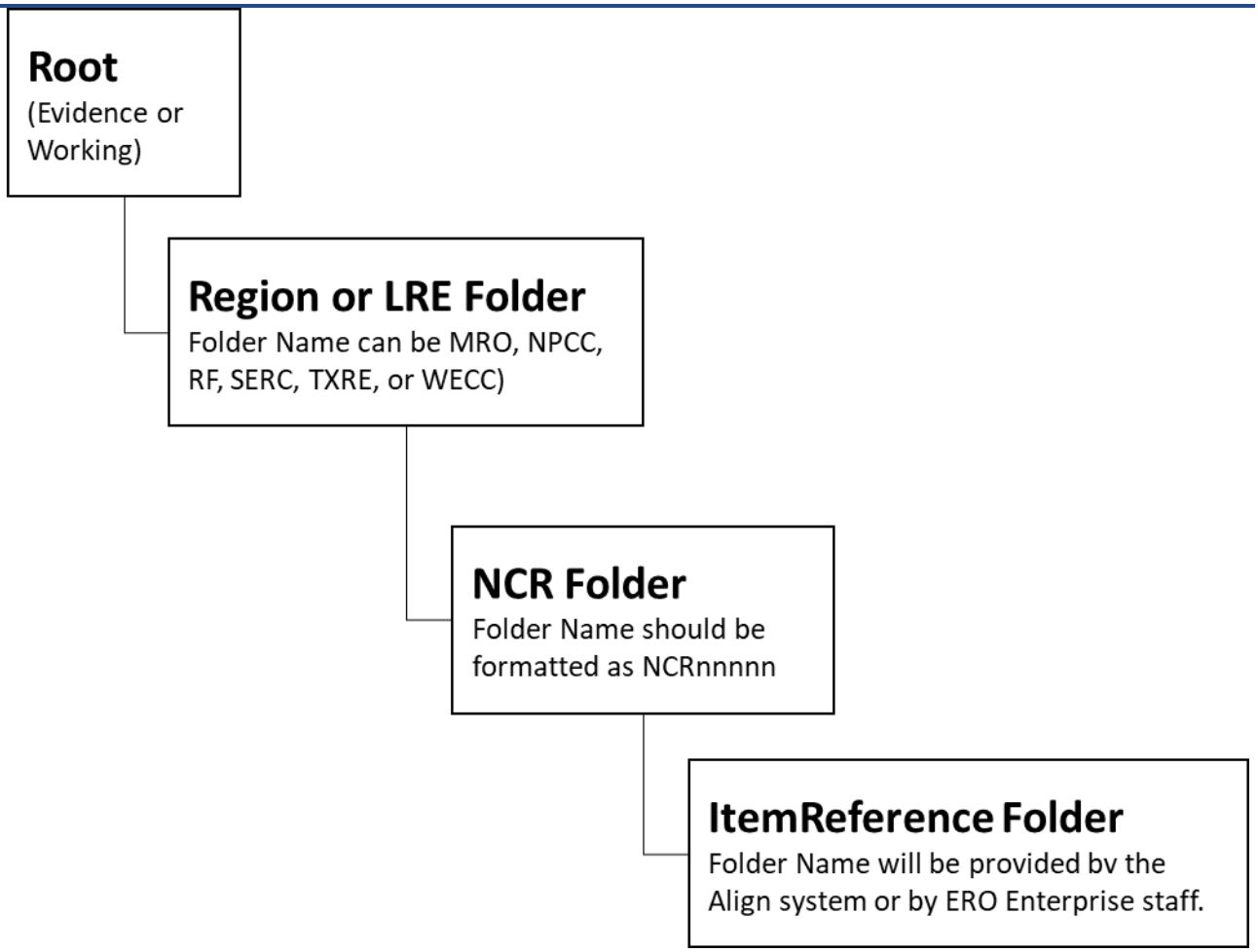
1. ERO Enterprise access to the SEL within five (5) business days, unless otherwise agreed to by the ERO Enterprise.
2. Notification to the requestor and user being granted access (if different from requestor), and must include:
    a. Instructions for how to access the SEL environment.
    b. The specific name and location of the Evidence and Working areas ,and
    c. Contacts for access, software, and/or troubleshooting issues.
3. A process and a registered entity point of contact to ensure timely revocation of ERO Enterprise staff access upon approval of the ERO Enterprise designated point of contact.
    a. The process shall require a confirmation to the ERO designated point of contact that the revocation request was complete.

Information Organization of Registered Entity Maintained SELs

1. Registered entity maintained SELs must store provided files in logical areas named “Evidence” and “Working”. Permissions applied to “Evidence” area files must be configured with read/write access for all registered entity authorized users, and read-only for ERO Enterprise users. The intent of this area is to provide a single master copy of any submitted evidence so that it can be viewed as submitted (i.e., without the potential of ERO Enterprise user modifications). ***The system should not allow overwriting or individual deletion of these files by the ERO Enterprise users, but may support versioning.***

2. Registered entity maintained SELs must have the ability to create and store working copies (i.e., convenience copies) of submitted files in a logical or virtual “Working” area. Files permissions must ensure registered entity users do not have access to these working copies, and must provide read/write/delete access for ERO Enterprise users. The intent of this area is to provide working copies of any submitted evidence so that it can be analyzed and annotated by ERO Enterprise staff as needed. ERO Enterprise users may need to create folders under this structure. ERO Enterprise users must have the ability to copy files from the “Evidence” area to the “Working” area.

3. Registered entity maintained SELs must organize files within the “Evidence” and “Working” areas into the following areas:



Functional Requirements for Registered Entity Maintained SELs

1. Registered entity maintained SELs must provide ERO Enterprise users an interactive Microsoft Windows 10 64-bit environment, or other Microsoft Operating System if agreed upon by ERO Enterprise staff and the required applications are functional. Each ERO Enterprise user should be able to have their own concurrent Windows session.

2. Registered entity maintained SELs must provide ERO Enterprise users access to a logical file structure within the Microsoft Windows environment configured as described in the "Information Organization" section of this document.

3. Registered entity maintained SELs must provide ERO Enterprise users fully licensed and current versions of the following applications and utilities installed in their default configuration. This list may be subject to modification over time as needs change:

    - All Standard Windows installed utilities and tools, including Notepad, Windows Media Player, Microsoft Windows Event Viewer, Paint, Snipping Tool, and Windows Command Line Interface
    - Ubuntu Linux (running within Windows using the built-in Windows Subsystem for Linux)
    - Microsoft Office Professional (including Outlook, Visio, and Access)
    - Adobe Acrobat Reader

- Check Point DiagnosticsView
- OIG RAT-STATS (free)
- Network Perception NP-View
- PowerWorld Viewer (free)
- Notepad++
- Java (In support of NP-View)

4. The registered entity maintained SEL shall provide a manner for ERO Enterprise staff to upload templates into the "Working" area for evidence analysis assistance.

5. In certain cases, ERO Enterprise staff may request software updates or additional tools; the registered entity must implement such updates within two (2) business days of the request, unless otherwise agreed to by the ERO Enterprise staff requestor.

Additional Requirements for Registered Entity Maintained SELs

1. Prior to storing files in the SEL, registered entities maintaining their own SELs must generate a SHA3 hash for each file and submit that hash to the ERO Enterprise SEL. Hashes must be recorded in a plain text file named as follows:

   <original file name>.SHA3

   The steps for this process should be similar to the following:
   1.) Begin the appropriate process in Align (e.g., submit Self-Report, respond to RFI, etc.)…).
   2.) Identify the file to be stored in the SEL.
   3.) Using a corporate PC, generate the hash file.
   4.) Upload the hash file(s) to the ERO Enterprise SEL, using the reference number generated by Align.
   5.) Create the appropriate file structure in your SEL environment (e.g. Region, NCR, Reference Number).
   6.) Place your file in the Evidence area.

2. If a registered entity chooses to take its registered entity maintained SEL offline when no active requests for access are in progress and the locker is not in use, it must be returned to online and available status within five (5) business days of an ERO Enterprise request to access the SEL.

3. When a registered entity maintained SEL is online and providing access to ERO Enterprise users, it may only be offline for scheduled maintenance periods. With the exception of ERO Enterprise requested software updates, ERO Enterprise users that have active access to the SEL must be notified of scheduled maintenance outages potentially affecting their usage no less than five (5) business days prior to the scheduled outage. Scheduled outages should occur between the hours of 7 p.m. and 7 a.m., Central Prevailing Time. Unscheduled outages must be remedied as quickly as possible, with a goal of service returning in no more than twenty-four (24) hours after the start of the unscheduled outage, unless otherwise agreed to with the ERO Enterprise designated point of contact.

4. Registered entities must have the capability to generate a manifest of all files uploaded to the SEL within two (2) business days of uploading files, and shared with the ERO Enterprise designated point of contact.

5. Non-functional Requirements:
   a. Minimum Number of Users - Registered entity maintained SELs must be able to support (without performance degradation) a minimum of 25 concurrent user logins and 25 accounts.

b. Availability - During the times that ERO Enterprise users have access to the registered entity's SEL, the registered entities maintained SEL must operate with a goal of 24X7 availability.
c. Support - Registered entities' support staff must be available to respond to support requests 24X7 when the SEL is in use.

ERO Enterprise Functionality Verification of Registered Entity Maintained SELs

The ERO Enterprise ***must verify the functionality and approve the SEL*** prior to the registered entity usage as an acceptable alternative to the ERO Enterprise SEL. A registered entity seeking to implement its own SEL must coordinate with its CEA prospectively and before the initiation of any CMEP activity. For any CMEP activities already underway before coordination with the CEA, the registered entity is expected to use the ERO Enterprise SEL.

1. **Initial Notification**
   When the registered entity maintained SEL is configured and ready for ERO Enterprise verification, the registered entity must notify its Regional Entity or Lead Regional Entity in the case of a multi-region registered entity (MRRE) participating in the Coordinated Oversight Program. Once notified, the Regional Entity is responsible for notifying the ERO Enterprise verification team for a joint functionality assessment engagement.
   a. Timing – The Regional Entity must receive a notification at least 60 days before the scheduled engagement (compliance monitoring engagement, etc.).
   b. For unscheduled engagements (e.g. Self-Reports, etc.), late requests, and if the registered entity maintained SEL has not been previously verified, then the ERO Enterprise SEL shall be used.

2. **Functionality Testing**
   The ERO Enterprise will use **Appendix A: Functionality Testing Checklist** to verify that the registered entity's SEL meets the minimum functionality criteria.

3. **Verification Notification**
   The ERO Enterprise verification team will notify the registered entity of the results of the functionality testing.

4. **Follow-up / Mitigation**
   If the results of functionality testing show the registered entity's SEL does not meet the minimum functionality criteria, the ERO Enterprise verification team will provide the registered entity with the specific items that failed functionality testing. The registered entity has the option to address the failed item(s) or agree to use the ERO Enterprise SEL. For instances where the registered entity chooses to mitigate the issues, the ERO Enterprise verification team is responsible for re-assessing the environment, but the registered entity SEL must be validated prior to using for any CMEP activities. If the registered entity's SEL fails verification and the registered entity chooses not to mitigate, the registered entity has the option to build an acceptable SEL in the future and have it reassessed by the ERO Enterprise verification team.

5. **Periodic Testing / Validation**
   Periodic validation and/or testing shall be required to ensure continuity of processes. If a registered entity maintained SEL is inactive, the registered entity and Regional Entities shall follow the "Access to Registered Entity Maintained SELs" section above. In addition, the registered entity will provide to the ERO Enterprise verification team a change log including a verification and validation of the functional requirements of the entity provided SEL on an annual basis, or when needed (i.e. CMEP engagements conducted in timeframes less than one year).

6. Revocation

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]. In the possible rare cases of usability issues, the CEA and/or NERC may revoke a registered entity's validated SEL. For example, a registered entity experiences prolonged system outages where the ERO Enterprise CMEP staff cannot perform its assessment in a timely manner, and the CEA has concerns about carrying out the CMEP activity as outlined in the NERC Rules of Procedure. The registered entity's SEL validation may be revoked and it would be expected that the registered entity use the ERO Enterprise SEL. System downtime may not be the only reason a Registered Entity's SEL validation may be revoked (other reasons may include, but are not limited to, access issues, functionality, licensing issues).

[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

Appendix A: Functionality Testing Checklist

Access

1. Has the registered entity provided access to the SEL within five (5) business days upon request? Did the response include:
    a. Instructions for how to access the SEL?
    b. The specific name and location of the storage and analysis area?
    c. Contacts for access, software, and troubleshooting issues?
    d. Revocation process and point of contact in the case of ERO Enterprise users that may need access revoked?
        i. Conduct revocation test.
2. Has the team verified that requested ERO Enterprise verification members can access the registered entity SEL?
    a. Is there additional information needed for access? For example, multifactor authentication?
3. Verify the SEL supports a minimum of 25 concurrent user logins and 25 accounts.
    a. Configurations (Network, server, memory, etc.)
    b. Policies / Procedures
4. Verify the availability of the SEL environment.

File Structure / Permissions

1. The team should verify that files are stored in the two different locations on the SEL: (This will require the registered entity to upload test files including a hash file.)
    a. Master copy area ("Evidence" drive):
        i. Verify the drive is only read access for ERO Enterprise users.
        ii. Verify the system will not allow addition, overwriting, or deletion of files.
        iii. Verify the system will support versioning of the files in the case of ERO Enterprise asks for multiple versions of the same document.
    b. Working copy area ("Working" drive):
        i. Verify that registered entity staff does not have access to these files.
        ii. Verify ERO Enterprise team has read/write access to both the working copies of the files, as well as the underlying file structure to create CMEP temporary work papers.
        iii. Verify that under no circumstance can ERO Enterprise staff download files to their system (laptop, external drive, etc.)
    c. File structure:
        i. Has the registered entity organized the file structure in the format as described in the functional document?
            1. Root area / Region or LRE Area / NCR Area (Primary NCR for Entities under Coordinated Oversight) / Item Reference Area

Environment

1. Does each ERO Enterprise verification team member have an interactive Microsoft Windows 10 64-bit environment upon logging in?
    a. While Windows 10 is preferred, other versions of the Microsoft Windows Operating System may be acceptable if there is no impact to tool functionality.

2. Can the verification team members view and navigate the file structure as described in the File Structure / Permissions section?
3. Can users copy files from the Evidence area to the Working copy area successfully?
    b. Do other users have read/write to this working copy?
4. Has the registered entity installed fully licensed and current versions of the required applications and utilities as outlined in the Functional Requirements for registered entity maintained SELs section above?

Updates / Software Installation / Downtime

1. Has the registered entity provided a point of contact for software upgrades and/or additional software requests?
2. Has the registered entity provided its process for updating the applications or installing additional software within two (2) business days of being requested, or longer if otherwise agreed to by the ERO Enterprise requestor?
3. Has the registered entity provided its expected scheduled maintenance periods?
    a. Are those scheduled maintenance times between the hours of 7pm and 7am, Central Prevailing Time, or other time agreed upon by ERO Enterprise requestor.
4. Does the registered entity have a process to notify ERO Enterprise staff for scheduled maintenance outages?
    a. Does that process outline that the ERO Enterprise should be notified of scheduled outages at least five (5) business days prior to the scheduled maintenance outage?
5. Does the registered entity have a process to address unscheduled outages and an ERO Enterprise notification process?
    a. NOTE: In the event of extended excessive scheduled or unscheduled outages of the registered entity SEL, the compliance monitoring activity may be extended or the registered entity may be expected to use the ERO Enterprise SEL.

File Integrity / Notifications

1. Has the registered entity demonstrated that for each file uploaded, it can generate a SHA3 hash that can be stored within the SEL and uploaded to the ERO Enterprise SEL? The filename should be <original file name>.SHA3
    a. Verify the registered entity notifies ERO Enterprise staff when files are uploaded for review.
2. Has the registered entity demonstrated that it can generate a manifest for all uploaded documents, upon upload of files?
    a. Verify the registered entity can provide a manifest of all documents that the registered entity uploaded.

Business Continuity

1. In the case of hardware failure, has the registered entity provided its business continuity plan for recovery of the SEL?
2. Has the Registered Entity provided a process for retrieval of evidence in an unaltered fashion (Hash verification) upon request?
3. What controls are in place for data retention by the Registered Entity?