NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Stakeholder Webinar

Registered Entity Self-Built Secure Evidence Lockers

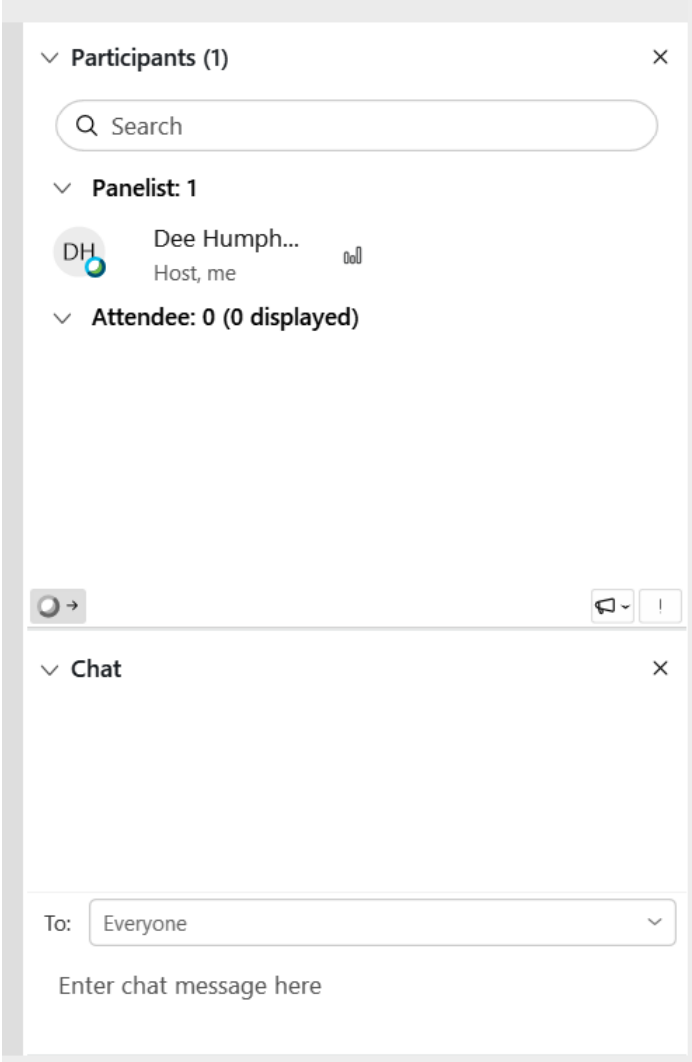
November 30, 2020

RELIABILITY | RESILIENCE | SECURITY




Meeting Logistics

- This meeting is being recorded and will be posted to NERC.com
- All lines are muted. Please submit questions via the Chat feature in WebEx



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Today's Panel

Name	Title/Role
Stan Hoptroff	Vice President, Business Technology
Mechelle Thomas	Vice President, Compliance
Andy Rodriquez	Director, Business Process Improvement
Don Prince	Director, IT Cyber Security Architecture
Jeff Hicks	Director, IT Solutions Architecture
Dee Humphries	Director, Project Management Office
Justin Lofquist	Director, Application Enterprise Architecture
Lonnie Ratliff	Senior Manager, Cyber and Physical Security Assurance
Steve Noess	Director, Regulatory Programs

Agenda: Registered Entity Self-Built Secure Evidence Lockers

- Summary: Functional Specification for Registered Entity Lockers
- What the locker is NOT
- Comparison: ERO SEL vs Registered Entity Lockers
- Validation Checklist
- Top FAQs
- Q&A

Summary: Functional Specs

- ERO Enterprise users must have remote access to interactive Microsoft Windows 10 64-bit desktop sessions
- The Windows 10 environment must have a number of productivity apps installed, as well as Check Point DiagnosticsView, OIG RAT-STATS (free), and Network Perception NP-View
- To ensure consistent navigation, files must be organized as described in the specification
- A tool capable of generating SHA3 hashes must be installed to verify file integrity

Registered Entity Self-Built Lockers: What are they NOT?

- Not just an extranet site
- Not just a SharePoint site or document repository
- Not just a secure FTP site
- Not a BCSI repository

The inclusion of the analysis environment is key to a successful implementation

Comparison Matrix

Area	ERO SEL	Registered Entity Locker
Functionality – Entity	Submit Only	Varies by Registered Entity
Functionality – ERO Enterprise	Full Analysis Environment	Full Analysis Environment
Security	NIST 800-171	Varies by Registered Entity
Scope	All Registered Entities	Varies by Registered Entity
Functional Certification	ERO Enterprise User Acceptance Testing	ERO Enterprise Certification Checklist
Cost	$$$$	Varies by Registered Entity
Implementation Level of Effort	High-Infrastructure Isolation	Varies by Registered Entity

Validation Checklist

- Registered Entity Secure Evidence Locker (SEL) Functionality Requirements Click Here
- Timeline
  - Compliance monitoring engagements vs self-report vs enforcement
- ERO Enterprise team validation of Registered Entity SEL functionality
  - Interactive Environment (Access considerations)
  - File Structure (Permissions)
    - Area for gold copies / Analysis environment
    - File permissions

Validation Checklist (cont'd)

- Additional Functionality
  - Software (Installed, current, and licensed)
  - Support minimum number of users (25)
  - 24X7 Availability
  - Manifest with file hashes
  - Timely Software updates (typically 2 days)
- Registered Entity Point of Contact
  - Software / Access / Revocation / Troubleshooting
- Procedures / Processes
  - Maintenance / Downtime (Scheduled or unscheduled)
    - Impact of extended unscheduled outages
  - Business Continuity

Validation Checklist (cont'd)

- Validation notification
  - Registered Entity
  - Regional Entity, includes Lead Regional Entity and Affected Regional Entities for Coordinated Oversight
  - NERC
- Mitigation / Follow up
  - Registered Entity will be notified of areas that failed validation
  - Option to address or use ERO Enterprise SEL
  - If addressing, must be fixed within X timeframe
  - Registered Entity SEL will be re-assessed

What goes in SEL? Compliance Monitoring

ITEMS AND WORK PAPERS IN ALIGN	NOTES
IRA Questionnaires	Sensitive information from registered entity should be uploaded in locker
IRA and COP work papers	
IRA and COP Summary	
RFIs	Sensitive information from registered entity should be uploaded in locker
RSAWs (with Auditor Notes, including Internal Controls notes)	
Preliminary Finding and Risk Harm Assessment	
Audit Report	
Self-Certification	Associated evidence in locker
Periodic Data Submittal	

Note: ERO Enterprise information will not reproduce sensitive content from the evidence lockers.

What goes in SEL? Enforcement

ITEMS AND WORK PAPERS IN ALIGN	NOTES
Self-Reports	Associated evidence in locker
Mitigation Plans	Sensitive details in locker
Mitigation review work papers, including verification	
Settlement Agreement, Notice of Confirmed Violation, Notice of Alleged Violation and Proposed Penalty or Sanction	
Noncompliance Review work papers	
Compliance Exception or FFT Notification Letter	
Filings with FERC, including Notices of Penalty, Compliance Exceptions, and FFTs	Filings may be prepared in Align, but filed through existing mechanisms outside of Align

Note: ERO Enterprise information will not reproduce sensitive content from the evidence lockers.

Frequently Asked Questions

Top FAQs

- When should an entity expect to use the ERO SEL?
  - Release 1, with certain limited exceptions (below)
- If I am building my own locker, when may I use it?
  - Only after it has been validated and only for evidence requested after validation (e.g., if an entity is currently using the ERO SEL, it may decide to build its own locker at a later date, but it may not use it until after it has received the functionality validation).
- What if an entity is definitely building its own locker that may be ready shortly after Release 1?
  - An entity that wants to go directly to using its own locker instead of the ERO SEL must be ready by Release 2 of Align: June 30, 2021. The entity must work with the Region to determine how to submit evidence in a way that is convenient for the region in the interim, and if the entity locker is not validated by June 30, 2021 the entity must use the ERO SEL.

Top FAQs

- How secure does the entity self-built locker need to be?
  - The security of a registered entity provided locker is at the discretion of the entity. NERC is not mandating or providing any security parameters. The ERO Enterprise Secure Evidence Locker provided by NERC will adhere to the NIST 800-171 security control framework.
- What is the intent of a self-built locker vs the ERO Enterprise SEL?
  - The intent is for NERC not to take physical possession of the evidence, but the evidence and analysis environment must be made available to the region and NERC to analyze and perform their duties.

Top FAQs

- What is the purpose of the functional specs? Can't I just build something secure to my own specs?
  - The intent is to ensure a uniform end-user experience for the ERO Enterprise, with common functionality, and it supports the overall mission of Align. Uniform functionality also supports security.
- Does an entity locker need to be "certified" before use?
  - A registered entity self-built locker will need to be reviewed by NERC and the regions prior to use to ensure that it meets the functional specifications. This will be a pass/fail review using the validation checklist as described. If this validation occurs after June 30, 2021, the entity will need to use the ERO SEL in the interim.
- Is the ERO SEL connected to Align in any way? Does my locker need to be connected?
  - No. There are no integrations or connections between the ERO SEL and Align. No registered entity locker will be connected to Align or the ERO SEL at this time

Top FAQs

- Is there an exception process to the functional specifications if I want to do something different with my own locker? What if I cannot afford all of the software that is listed as required?
  - There is not an exception process to the functional specifications or software required for a registered entity self-built locker, as they are the minimum requirements to allow the ERO Enterprise fully to perform the same capabilities in a registered entity locker as is possible in the ERO SEL. Providing exceptions to the functional specifications could restrict analysis capabilities and undermine the ability for a common user experience.
  - NERC is investing in a secure evidence locker with NIST 800-171 security controls and specific functional criteria to ensure a uniform user experience across ERO Enterprise staff. It is the only way that the ERO Enterprise will take possession of evidence. It will be available at no additional cost to registered entities.

Top FAQs

- What is the due date for a registered entity locker?
  - The due date is June 30, 2021, and must be validated by NERC and the Region. The entity needs to provide notification to their region that they are building their own locker by January 1, 2021.
- What if my locker is not ready by the deadline?
  - The registered entity will use the ERO SEL in the interim. Another option is to work with the Regional Entity to receive the sensitive evidence by a means at their convenience.
- Can I decide later to build a locker after I've already used the ERO SEL?
  - Yes, registered entities can decide to build a locker at a later date. They will be required to use the ERO SEL in the meantime. It will need to be reviewed and approved by NERC and the Region prior to use. NERC will not perform a transfer of evidence from one locker to another.

Supporting Material

- NIST 800-171 Control Framework

- Webinar will be posted online

- Updated Functional Specification Click Here

Questions? Submit to: AskAlign@nerc.net