E-ISAC Operations Update

Manny Cancel
Technology and Security Committee Meeting
November 4, 2020
• Operations Update

• Threat Landscape

• Strategic Partnerships

• GridEx VI

• Policy Input
  - Feedback
  - Outreach
  - Next Steps
Operations Update

- E-ISAC continues to operate remotely and develop responsible return plans
- Organization changes
- ESCC activities
- Executive Order 13920
- Cross-sector coordination with other ISACs, Analysis and Resiliency Center (ARC)
- 20% increase in membership and 37% increase in portal users
- Portal Upgrade scheduled for January 2021
- CIP-008 reporting goes into effect on January 1, 2021
• Key Advanced Persistent Threat (APT) groups tracked:
  ▪ Russia: Sandworm Team and associated APT28
  ▪ China: APT10 and APT41

• Trends and Observations
  ▪ Potential for Ransomware impact to OT systems
  ▪ Emotet malware not seen in sector, prevalent in SLTT and elections
• Trends
  ▪ 29% increase in intrusions
  ▪ 103% increase in vandalism
  ▪ 55% increase in gunfire incidents
  ▪ Civil unrest
  ▪ Increased surveillance activities using unmanned aircraft systems (drones)

• Products
  ▪ Physical Security Reports
  ▪ Wind Farm Security White Paper
  ▪ Protective Measures Index Tool
  ▪ Security vulnerability assessment workshop (VISA Workshop)
  ▪ E-ISAC Situational Awareness Summary: 2020 Election
• DOE
  ▪ Coordinating on OT initiatives, CRISP OT pilot, Essence OT pilot
  ▪ ESCC unclassified threat briefing
  ▪ GridEx VI

• DHS
  ▪ Intelligence reports derived from E-ISAC Portal posts
  ▪ Advance notifications on Malware Analysis Reports
  ▪ Update CISA on outages and threats to the bulk power system to support 2020 elections

• MS-ISAC/EL-ISAC
  ▪ Coordinating with MS/El-ISAC to inform industry election security
- Canadian Partnerships
  - Canadian Electricity Association
  - Canadian Security Establishment’s EnerSEcCC
  - IESO
- Analysis & Resilience Center (formerly FSARC)
  - Developing formal collaboration agreement
  - Participated in Energy Risk Committee meeting
• Exercise the resilience of the North American electricity system in the face of a coordinated attack from a state-sponsored adversary
  - Distributed Play - November 16-17, 2021
  - Executive Tabletop - November 18, 2021

• Hagerty Consulting awarded contract

• Potential scenarios include kinetic attacks, social engineering, supply chain, insider threat, cross-sector impacts, etc.
• Stakeholders are generally supportive of strategy

• Common themes:
  ▪ Support Canadian objectives
  ▪ Minimize duplication of efforts with other initiatives and programs
  ▪ Ensure fiscal responsibility and cost efficiency
  ▪ Operate within E-ISAC mandate/scope
  ▪ Clarify objectives and deliverables of major programs
  ▪ Ensure extension of services does not erode services to electricity industry or increase costs
  ▪ Evaluate implementation timeframes
  ▪ Evaluate cross-sector activities
• Contacted respondents for clarification and ensured no additional concerns needed to be addressed

• Outreach to Trade Associations and NERC Member Representatives Committee
• Update strategic plan to address feedback
• Update NERC Board
• Continue outreach to membership, trade associations and regions
• Track progress on strategic plan initiatives on quarterly basis
Questions and Answers
Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
November 4, 2020
Agenda

• ERO Business Technology Projects Update
  ▪ Geomagnetic Disturbance (GMD) application
  ▪ Microsoft TEAMS Collaboration Platform
• Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
  ▪ Salesforce customer relationship management (CRM)
• Security Advisory Group
• Priorities Looking Ahead
• Section 1600 Data Request; FERC Order 830
• October 1, 2020 released to production
• Data reporting mechanism for GMD data
• Key users: transmission owners and generator owners
• Developed, hosted and secured by NERC’s xRM platform
• Stakeholders will have access to GMD data via NERC.com
Welcome to the NERC Geomagnetic Disturbance (GMD) Data System. Below is a list of entities you are authorized to view or submit data on behalf of. If you would like to request access to a registered entity, you may do so on the application access request page.

<table>
<thead>
<tr>
<th>NCR</th>
<th>Entity Name</th>
<th>GMD Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCR11664</td>
<td>4C Acquisition LLC</td>
<td>GMD Submitter</td>
</tr>
<tr>
<td>NCR11826</td>
<td>54KR 8ME LLC</td>
<td>GMD Submitter</td>
</tr>
<tr>
<td>NCR55555</td>
<td>Test Company 2-1</td>
<td>GMD Submitter</td>
</tr>
</tbody>
</table>

**Menu**

- **GIC Monitor Devices**
  View, create, manage or bulk import GIC monitor devices

- **Magnetometer Devices**
  View, create, manage or bulk import magnetometer devices

- **GIC Monitor Data Reporting**
  View and submit GIC monitor data reporting submissions

- **Magnetometer Data Reporting**
  View and submit magnetometer geomagnetic data reporting submissions

- **Missing Data Report Imports**
  Bulk import missing data reports

- **GMD System Reports**
  View GMD Submission Reports

- **GMD Events**
  View GMD events that require reporting
Training

- Regional registration teams will be encouraged to train entity users on Centralized Organization Registration ERO System changes
- Two types of GMD training - one for reporting entities and the other for data researchers
- Training and user documentation is complete
- Data reporting training sessions are in progress – October 2020
- Data Researcher training will be delayed until 2021 to allow for a period of data collection in Q4 2020
• Unified communications and collaboration platform
• Enables secure remote collaboration
• Access, share and edit documents, PowerPoints and spreadsheets
• Strategic investment for NERC, ERO Enterprise and registered entities in a post-coronavirus world
• 80M global users
Welcome to the team!

Here are some things to get going...

Add more people  Create more channels  Open the FAQ

Alan Redd has added Brice Blocker to the team.
Alan Redd has added Dee Humphries to the team.
Alan Redd has added LaCreasia Smith to the team.
Alan Redd changed team description.

Dee Humphries has added Denise Lafantaisie to the team.

Brice Blocker  7/14 1:14 PM
Dee Humphries LaCreasia Smith might be a good idea to discuss we’d like to setup projects in TEAMS in our next team meeting. They can be separate teams or setup as channels within another team, etc. I suspect it will be a case by case basis...

Start a new conversation. Type @ to mention someone.
• CRM tool (Salesforce) in production, saving time and increasing accuracy of member tracking and stakeholder contacts
• E-ISAC Portal – Platform replacement to Salesforce underway; expected go live in Q4 2020
• E-ISAC Data Platform (EDP) – Converting to a robust, reliable, secure production platform in Atlanta data center; continue to expand analytical capabilities
• Advisory body established by NERC Management
• Represents all industry sectors; engagement at the Chief Information Security Officer level
• Will interface with NERC IT Leadership
• Supports NERC Management with expertise and advice on data confidentiality, integrity and security
• Sensitive industry information stored or processed by NERC
Priorities Looking Ahead

• Analytical capabilities for the E-ISAC under the EDP
• Accelerated adoption of Salesforce capabilities for the E-ISAC
• Implementation of Microsoft Teams
• Regional focus on cyber security with new cyber security director
• Various software/hardware upgrades to NERC infrastructure
Questions and Answers
GMD Application Screen Shots
Geomagnetic Disturbance Data System

Welcome to the NERC Geomagnetic Disturbance (GMD) Data System. Below is a list of entities you are authorized to view or submit data on behalf of. If you would like to request access to a registered entity, you may do so on the application access request page.

<table>
<thead>
<tr>
<th>NCR</th>
<th>Entity Name</th>
<th>GMD Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>NCR11664</td>
<td>4C Acquisition LLC</td>
<td>GMD Submitter</td>
</tr>
<tr>
<td>NCR11826</td>
<td>54KR 8ME LLC</td>
<td>GMD Submitter</td>
</tr>
<tr>
<td>NCR55555</td>
<td>Test Company 2-1</td>
<td>GMD Submitter</td>
</tr>
</tbody>
</table>

List of entities for which ERO Portal user has permission to report data

Menu

- **GIC Monitor Devices**
  View, create, manage or bulk import GIC monitor devices

- **Magnetometer Devices**
  View, create, manage or bulk import magnetometer devices

- **GIC Monitor Data Reporting**
  View and submit GIC monitor data reporting submissions

- **Magnetometer Data Reporting**
  View and submit magnetometer geomagnetic data reporting submissions

- **Missing Data Report Imports**
  Bulk import missing data reports

- **GMD System Reports**
  View GMD Submission Reports

- **GMD Events**
  View GMD events that require reporting
GIC Monitor Device Screen Displays Existing Devices and Provides Ability to Create or Edit, Manually or via Import File

Below are the registered GIC monitor devices for currently selected registered entity. If you wish to view GIC monitors for a different entity, you must change the entity in the top right-hand corner of the page.

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Device Status</th>
<th>Device Serial Number</th>
<th>Geographic Latitude (North)</th>
<th>Geographic Longitude (West)</th>
<th>Status Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>10069</td>
<td>AV</td>
<td>s-988</td>
<td>45.0</td>
<td>105.0</td>
<td>7/2/2020</td>
</tr>
<tr>
<td>10068</td>
<td>AV</td>
<td>s-1239</td>
<td>50.0</td>
<td>60.0</td>
<td>7/2/2020</td>
</tr>
<tr>
<td>10067</td>
<td>AV</td>
<td>s-12354</td>
<td>32.0</td>
<td>132.0</td>
<td>7/1/2020</td>
</tr>
<tr>
<td>10065</td>
<td>AV</td>
<td>s-09876</td>
<td>14.0</td>
<td>114.0</td>
<td>6/30/2020</td>
</tr>
<tr>
<td>10064</td>
<td>AV</td>
<td>s-55555</td>
<td>23.0</td>
<td>123.0</td>
<td>6/30/2020</td>
</tr>
<tr>
<td>10062</td>
<td>AV</td>
<td>s-5555</td>
<td>44.0</td>
<td>74.0</td>
<td>6/10/2020</td>
</tr>
<tr>
<td>10061</td>
<td>AV</td>
<td>s-9998</td>
<td>16.0</td>
<td>113.0</td>
<td>6/24/2020</td>
</tr>
<tr>
<td>10060</td>
<td>AV</td>
<td>s-00009</td>
<td>12.0</td>
<td>112.0</td>
<td>6/10/2020</td>
</tr>
</tbody>
</table>
## GIC Monitor Data Reporting

### GIC Monitor Device Import Validation Results

<table>
<thead>
<tr>
<th>GMD Event</th>
<th>Successful Records</th>
<th>Failed Records</th>
<th>Submission Status</th>
<th>Earliest Data Interval</th>
<th>Earliest Data Interval Seconds</th>
<th>Latest Data Interval</th>
<th>Latest Data Interval Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019E01</td>
<td>0</td>
<td>1</td>
<td>Processing Complete with Errors</td>
<td>8/25/2018 15:00</td>
<td>0</td>
<td>8/27/2018 00:00</td>
<td>0</td>
</tr>
<tr>
<td>2018E01</td>
<td>31</td>
<td>0</td>
<td>Successfully Processed</td>
<td>8/25/2018 12:00</td>
<td>0</td>
<td>8/26/2018 12:05</td>
<td>0</td>
</tr>
<tr>
<td>2018E01</td>
<td>61</td>
<td>0</td>
<td>Successfully Processed</td>
<td>8/25/2018 20:00</td>
<td>0</td>
<td>8/25/2018 20:10</td>
<td>0</td>
</tr>
<tr>
<td>2017E03</td>
<td>11,881</td>
<td>0</td>
<td>Successfully Processed</td>
<td>9/27/2017 15:00</td>
<td>0</td>
<td>9/29/2017 00:00</td>
<td>0</td>
</tr>
<tr>
<td>2017E03</td>
<td>11,881</td>
<td>0</td>
<td>Successfully Processed</td>
<td>9/27/2017 15:00</td>
<td>0</td>
<td>9/29/2017 00:00</td>
<td>0</td>
</tr>
<tr>
<td>2017E03</td>
<td>0</td>
<td>1</td>
<td>Processing Complete with Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2017E03</td>
<td>0</td>
<td>11,881</td>
<td>Processing Complete with Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2017E01</td>
<td>61</td>
<td>0</td>
<td>Successfully Processed</td>
<td>5/27/2017 16:00</td>
<td>0</td>
<td>5/27/2017 16:10</td>
<td>0</td>
</tr>
</tbody>
</table>
### GIC Monitor Missing Data Reporting

- **Missing Data Reports** Document Gaps in GMD Event Data

#### Active GIC Monitor Missing Data Reports

<table>
<thead>
<tr>
<th>GMD Event</th>
<th>Device ID (GIC Monitor)</th>
<th>Missing Data Start Date and Time (UTC)</th>
<th>Missing Data Start Seconds</th>
<th>Missing Data End Date and Time (UTC)</th>
<th>Missing Data End Seconds</th>
<th>Missing Data Reason</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017E02</td>
<td>10065</td>
<td>9/7/2017 22:00</td>
<td>0</td>
<td>9/8/2017 04:00</td>
<td>0</td>
<td>3-Data Recording Device Malfunction</td>
<td>6/26/2020 16:44</td>
</tr>
<tr>
<td>2017E01</td>
<td>10062</td>
<td>5/27/2017 16:00</td>
<td>0</td>
<td>5/27/2017 16:10</td>
<td>0</td>
<td>1-GIC Monitor Malfunction</td>
<td>6/11/2020 12:30</td>
</tr>
<tr>
<td>2015E06</td>
<td>10064</td>
<td>12/20/2015 15:00</td>
<td>10</td>
<td>12/20/2015 17:00</td>
<td>0</td>
<td>1-GIC Monitor Malfunction</td>
<td>6/17/2020 18:55</td>
</tr>
<tr>
<td>2015E06</td>
<td>10064</td>
<td>12/20/2015 07:30</td>
<td>0</td>
<td>12/20/2015 15:00</td>
<td>0</td>
<td>1-GIC Monitor Malfunction</td>
<td>6/17/2020 18:54</td>
</tr>
</tbody>
</table>
Magnetometer Devices

- Magnetometer Device Screen Displays Existing Devices and Provides Ability to Create or Edit, Manually or via Import File

### Magnetometer Devices

Below are the registered magnetometer devices for the currently selected registered entity. If you wish to view magnetometer devices for a different entity, you must change the entity in the top right-hand corner of the page.

#### Summary Device List

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Device Status</th>
<th>Geographic Latitude (North)</th>
<th>Geographic Longitude (West)</th>
<th>Status Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>50086</td>
<td>AV</td>
<td>74.0</td>
<td>74.0</td>
<td>6/25/2020</td>
</tr>
<tr>
<td>50084</td>
<td>AV</td>
<td>65.0</td>
<td>135.0</td>
<td>6/10/2020</td>
</tr>
<tr>
<td>50083</td>
<td>AV</td>
<td>77.0</td>
<td>77.0</td>
<td>6/11/2020</td>
</tr>
<tr>
<td>50082</td>
<td>AV</td>
<td>15.0</td>
<td>115.0</td>
<td>6/10/2020</td>
</tr>
<tr>
<td>50081</td>
<td>AV</td>
<td>67.0</td>
<td>67.0</td>
<td>6/29/2020</td>
</tr>
<tr>
<td>50076</td>
<td>AV</td>
<td>64.0</td>
<td>124.0</td>
<td>6/3/2020</td>
</tr>
<tr>
<td>50075</td>
<td>AV</td>
<td>84.0</td>
<td>84.0</td>
<td>6/3/2020</td>
</tr>
<tr>
<td>50074</td>
<td>AV</td>
<td>45.0</td>
<td>84.0</td>
<td>6/3/2020</td>
</tr>
</tbody>
</table>
Magnetometer Data Reporting

- Magnetometer Device Import Validation Results

### Magnetometer Data Reporting

<table>
<thead>
<tr>
<th>GMD Event</th>
<th>Successful Records</th>
<th>Failed Records</th>
<th>Submission Status</th>
<th>Earliest Data Interval</th>
<th>Earliest Data Interval Seconds</th>
<th>Latest Data Interval</th>
<th>Latest Data Interval Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019E01</td>
<td>0</td>
<td>4</td>
<td>Processing Complete with Errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2018E01</td>
<td>31</td>
<td>0</td>
<td>Successfully Processed</td>
<td>8/26/2018 12:00</td>
<td>0</td>
<td>8/26/2018 12:05</td>
<td>0</td>
</tr>
<tr>
<td>2018E01</td>
<td>61</td>
<td>0</td>
<td>Successfully Processed</td>
<td>8/25/2018 20:00</td>
<td>0</td>
<td>8/25/2018 20:10</td>
<td>0</td>
</tr>
<tr>
<td>2018E01</td>
<td>38</td>
<td>0</td>
<td>Successfully Processed</td>
<td>8/25/2018 18:00</td>
<td>0</td>
<td>8/25/2018 18:03</td>
<td>0</td>
</tr>
<tr>
<td>2017E02</td>
<td>102</td>
<td>0</td>
<td>Successfully Processed</td>
<td>9/7/2017 21:35</td>
<td>10</td>
<td>9/7/2017 21:52</td>
<td>0</td>
</tr>
<tr>
<td>2017E02</td>
<td>0</td>
<td>1</td>
<td>Processing Complete with Errors</td>
<td>9/7/2017 21:00</td>
<td>0</td>
<td>9/7/2019 21:34</td>
<td>50</td>
</tr>
<tr>
<td>2017E02</td>
<td>210</td>
<td>0</td>
<td>Successfully Processed</td>
<td>9/7/2017 21:00</td>
<td>0</td>
<td>9/7/2017 21:35</td>
<td>0</td>
</tr>
<tr>
<td>2017E02</td>
<td>210</td>
<td>0</td>
<td>Successfully Processed</td>
<td>9/7/2017 21:00</td>
<td>0</td>
<td>9/7/2017 21:35</td>
<td>0</td>
</tr>
</tbody>
</table>
Missing Data Reports Document Gaps in GMD Event Data

### Magnetometer Missing Data Reporting

<table>
<thead>
<tr>
<th>GMD Event</th>
<th>Device ID (Magnetometer)</th>
<th>Missing Data Start Date and Time (UTC)</th>
<th>Missing Data Start Seconds</th>
<th>Missing Data End Date and Time (UTC)</th>
<th>Missing Data End Seconds</th>
<th>Missing Data Reason</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017E02</td>
<td>50059</td>
<td>9/8/2017 10:30</td>
<td>0</td>
<td>9/8/2017 22:00</td>
<td>0</td>
<td>3-Data Recording Device Malfunction</td>
<td>6/26/2020 16:55</td>
</tr>
<tr>
<td>2015E06</td>
<td>50084</td>
<td>12/20/2015 18:00</td>
<td>0</td>
<td>12/20/2015 20:00</td>
<td>0</td>
<td>2-Magnetometer Malfunction</td>
<td>6/17/2020 20:19</td>
</tr>
<tr>
<td>2015E06</td>
<td>50084</td>
<td>12/20/2015 15:00</td>
<td>10</td>
<td>12/20/2015 17:00</td>
<td>0</td>
<td>2-Magnetometer Malfunction</td>
<td>6/17/2020 18:57</td>
</tr>
</tbody>
</table>
Submission Status Report Shows Device Reporting for an Event

The GMD Submission Status Report provides information about whether data was reported for each device by Event, Calendar Year, or Reporting Collection Period (April - March).

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Device ID</th>
<th>Data Start Date and Time</th>
<th>Data End Date and Time</th>
<th>Has Missing Data Report?</th>
<th>NCR</th>
<th>Is Data Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015E02</td>
<td>10037</td>
<td>06/22/2015 12:16:00</td>
<td>06/22/2015 12:20:00</td>
<td>No</td>
<td>NCR55555</td>
<td>No</td>
</tr>
<tr>
<td>2015E02</td>
<td>10064</td>
<td>06/22/2015 12:16:00</td>
<td>06/22/2015 12:20:00</td>
<td>No</td>
<td>NCR55555</td>
<td>No</td>
</tr>
<tr>
<td>2015E02</td>
<td>10065-Confidential</td>
<td>06/22/2015 12:00:00</td>
<td>06/22/2015 23:59:50</td>
<td>No</td>
<td>NCR55555</td>
<td>No</td>
</tr>
<tr>
<td>2015E02</td>
<td>10065-Confidential</td>
<td>06/23/2015 00:00:00</td>
<td>06/23/2015 00:55:20</td>
<td>No</td>
<td>NCR55555</td>
<td>No</td>
</tr>
<tr>
<td>2015E02</td>
<td>50070</td>
<td>06/22/2015 12:16:00</td>
<td>06/22/2015 12:20:00</td>
<td>No</td>
<td>NCR55555</td>
<td>No</td>
</tr>
</tbody>
</table>
• Data Search and Download Allows Researchers to Specify Criteria

GMD Data Search and Download

Event
2015E02 (06/22/2015 03:00:00 - 06/23/2015 15:00:00)

Device Type
- Magnetometers
- GIC Monitors

Min Latitude
10

Max Latitude
80

Min Longitude

Max Longitude

Device ID

Selected Devices
No devices selected
GMD Data Submitters Also Can Search by Entity NERC Compliance Registry ID
• Data Search and Download Results Displayed; User Selects Data Files to Download

<table>
<thead>
<tr>
<th>Event Name</th>
<th>NCR</th>
<th>Device Type</th>
<th>Device ID</th>
<th>Number of Data Records</th>
<th>Latitude</th>
<th>Longitude</th>
<th>Data Sample Start Date and Time</th>
<th>Data Sample End Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015E02</td>
<td>NCR55555</td>
<td>Magnetometer</td>
<td>50070</td>
<td>25</td>
<td>32.00</td>
<td>132.00</td>
<td>06/22/2015 12:16:00</td>
<td>06/22/2015 12:20:00</td>
</tr>
<tr>
<td>2015E02</td>
<td>NCR55555</td>
<td>Magnetometer</td>
<td>50086-Confidential</td>
<td>4320</td>
<td>74.00</td>
<td>74.00</td>
<td>06/22/2015 12:00:00</td>
<td>06/22/2015 23:59:50</td>
</tr>
<tr>
<td>2015E02</td>
<td>NCR55555</td>
<td>Magnetometer</td>
<td>50086-Confidential</td>
<td>333</td>
<td>74.00</td>
<td>74.00</td>
<td>06/23/2015 00:00:00</td>
<td>06/23/2015 00:55:20</td>
</tr>
</tbody>
</table>

Confidential data files only provided to entities who report those devices
ERO Enterprise Align
Project Update

Stan Hoptroff, Vice President, Business Technology
Dee Humphries, Director, Project Management Office
Technology and Security Committee Meeting
November 4, 2020
• Major/New Topics
  ▪ Release 1 Timeline Overview and Upcoming Milestones
  ▪ Align Governance Model Update
  ▪ Canada
  ▪ Challenges
  ▪ Change Management
  ▪ How to Stay Informed
Align Timeline and Milestones
(As of October 2020)

**R1 Regional Adoption Workshops**
(August – October)
Workshops focused on preparing the Regions for R1

**R1 Initial Regional Training**
(November – January)
Regions begin to conduct initial training for staff on use of Align focused on the changes to internal Regional business processes

**R1 Go/No-Go Process**
(December – April)
Series of checkpoints to monitor production readiness

**R1 Regional and Registered Entity Training – Align and ERO SEL**
(February - April)
Regions continue to conduct training for regional staff and entities

**R1 TTT – Align Refresher and ERO SEL**
(January – February)
Walk through TTT materials for ERO SEL and provide Align refresher

**R1 Final Data Validation**
(January – February)
Regional SMEs validate standards and entity data

**R2 QA Testing**
(November/December)
Core team performs QA testing for R2

**R2 UAT**
(Q1)
R2 SMEs perform UAT for R2

**R2 Training Materials**
(Q1/Q2)
Development of R2 training materials

**Cycle 6 Process Harmonization**
(August - November)
Harmonization of compliance planning processes (e.g., IRA, COP)

**In progress**

**Complete**
OLT: Provide executive leadership and oversight

Product Management Team: Risk Performance and Monitoring Group, Enforcement Group and NERC representation; project-level engagement

User Committee: Regional experts and registered entity experts representation; Compliance and Certification Committee and Alignment Working Group provides input and expertise
Transition to this model will take place during 2021
• In progress to:
  - Determine which provinces will use the U.S. instance
  - Define use cases by Region and province
  - Identify roadblocks (agreements, data sovereignty, etc.)
  - Define rollout strategy for each province
• **Resources:** Multiple parallel efforts (R1 training/rollout, R2 development, R3 requirements, ongoing stakeholder engagement)

• **Budget pressure:** Balance in-scope efforts with continuous improvement requests (i.e., 50 enhancements from stakeholders)

• **Rollout approach:** Data supports “whole Region” vs. segmentation by groups of entities; management across multiple systems during rollout
Change Management

• Change Readiness Assessment will take place in November
  ▪ Will measure business readiness for Release 1 go-live
  ▪ Will reach registered entities
  ▪ Will be benchmarked against baseline survey conducted in 2019

• Go-Live Deployment Readiness
  ▪ Will measure technical and operational readiness
How To Stay Informed

Key communication vehicles

• Align newsletter for Regions and registered entities
• Regional Change Agent Network
• Dedicated project page on NERC.com: [Click Here](#)
• Upcoming Compliance Monitoring and Enforcement Program (CMEP) Regional workshops
• Trades meetings
• NERC News
• Social media
Comments from TVA

1. The ALIGN Project Team has done an INCREDIBLE job!
2. The new ALIGN system looks very impressive, as do the training videos!
3. I am really looking forward to using the new ALIGN system.
4. It will improve the current processes, for the registered entities as well as the Regional Entities and NERC.
5. The training videos provided are excellent! They are short, yet convey a lot of information.
6. The narrator in the training videos does a great job explaining and demonstrating, without making it confusing or too detailed.
7. The new ALIGN system provides a number of enhancements and upgrades, which will make things easier to understand, input, and track.
8. The new ALIGN system screens are much cleaner and easier to follow, along with excellent help text to guide you.

David Abdalla
Senior Program Manager
NERC O&P Compliance

Tennessee Valley Authority
Questions and Answers
Background and Reference Material
Align Release 1:
What to expect as a registered entity?

**Release 1 Functionality**

- Create and submit Self-Reports and Self-Logs
- Create and manage mitigating activities (informal) and Mitigation Plans (formal)
- View and track Open Enforcement Actions (EAs) resulting from all monitoring methods
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Generate report of NERC Standards and Requirements applicable to your entity
- Manage user access for your specific entity
**Release 1 Functionality**

- Receive Self-Reports and Self-Logs from entities
- Manually create findings that result from any monitoring method (Audits, Spot Checks, Investigations, Periodic Data Submittals (PDSs), Self-Certifications, Complaints)
- Perform Preliminary Screens, Potential Noncompliance (PNC) Reviews, and disposition determinations for each PNC/EA
- Send and received responses to RFIs
- Trigger notifications such as Notice of Alleged Violation(s) and Proposed Penalty or Sanction, Notices of Confirmed Violation(s), Compliance Exception Letter(s), Find, Fix, Track & Report Letter(s), and Settlement Agreements
- Receive, review, and approve mitigating activities (informal) and Mitigation Plans (formal)
- Receive notifications and view dashboards on new/open action items
- Generate report of NERC Standards and Requirements applicable to a registered entity
Align Future Releases: What to expect?

**Release 2 Functionality**
**Est. 2021**

- Technical Feasibility Exceptions
- Self-Certifications
- PDSs

*Note: A strategy is being developed for how these monitoring methods will be managed in the gap between Releases*

**Release 3 Functionality**
**Est. 2021**

- Compliance Planning (Risk, CMEP Implementation Plan, Inherent Risk Assessment, Internal Controls Evaluation, Compliance Oversight Plan)
- Compliance Audit
- Spot Check
- Compliance Investigations
- Complaints
Moving to a common platform will provide:

- Alignment of **common** & CMEP **business processes**, ensuring consistent practices and data gathering
- A **standardized interface** for registered entities to interact with the ERO Enterprise
- **Real-time access to information**, eliminating delays and manual communications
- **Consistent application** of the CMEP
- **More secure** method of managing and storing CMEP data
ERO Enterprise Secure Evidence Locker Update

Stan Hoptroff, Vice President, Business Technology
Justin Lofquist, IT Director
Technology and Security Committee Meeting
November 4, 2020
• What is the ERO Enterprise Secure Evidence Locker (ERO SEL)?
• Solution Overview
  ▪ ERO SEL - How Will It Work?
  ▪ National Institute of Standards and Technology (NIST) Standard
  ▪ Security Controls
• Registered Entity Experience Screen Shots
• Regional Entity Experience Screen Shots
• ERO SEL Potential Risks
A highly secure, isolated environment

- Purpose-built to collect and protect evidence
- Enables submission by authorized and authenticated entity users
- Provides compartmentalized analysis of evidence in temporary, isolated, disposable environments
- No interfaces with any other systems

Evidence

- Is encrypted immediately upon submission
- Is securely isolated per entity
- Is never extracted
- Is never backed up
- Is subject to proactive and disciplined destruction policies
Solution Overview
ERO SEL - How will it work?
Technical Implementation

ERO Enterprise Evidence Analysis
Locker

- Secure File Transfer
  - Encryption: Regionally Specific
  - Routing Rules

- Enterprise Content Management
  - Locker

- Analysis Environment
  - Auditor Session
    - Auditor tools
    - Disposable
  - Enforcement Session
    - Auditor tools
    - Disposable

Management Utilities

- Privileged Session Server
- MFA
- System Administrator

Registered Entity User

MFA Authentication

Authorized CMEP Personnel

MFA Authentication
• Applicability: Federally-authored for non-governmental agencies handling Controlled Unclassified Information (CUI)

• Contains 110 controls in 14 key areas including:
  ▪ Access Control
  ▪ Physical Protection
  ▪ System and Information Integrity
  ▪ Personnel Security
  ▪ Incident Response
  ▪ Risk Assessment
• Proxies for all incoming and out-bound traffic – inspection of all HTTPS traffic
• In-process Virus / malware protection
• Micro-segmentation with Next-Gen firewalls
  ▪ Restricted communications within environment
• Geo-blocking
• Forensic endpoint monitoring and Network Traffic Analytics
• Enterprise Vulnerability Scanning
• Integrated, key-based authentication (PKI)
  ▪ Encryption of all traffic and data
  ▪ NERC possession and rotation of all encryption keys
• Auditing of all activities and file actions
• Privileged Access Management Service
Registered Entity Experience
Users will log into the Secure Evidence Locker through a URL and be authenticated using their ERO Portal account with Multi-Factor Authentication (MFA).
• Enter reference ID and click Validate
• Upload Files(s)
• Click Submit
Multiple files can be uploaded at once

Receive email confirmation of submission, including “Hash Value,” to ensure submission integrity
• Authenticated through MFA
• No ability to view submitted information (data loss prevention control)
• Ability to request current inventory of evidence per entity
Regional Entity Experience
• Users will log into the Secure Evidence Locker through a URL and be authenticated using their ERO Portal account with MFA.
• Once logged in, users will be presented with a workspace, which will provide the ability to launch an ERO Analysis Environment.
• Once the user clicks on ‘ERO Analysis Environment,’ a new desktop environment will launch.
• This environment is a fully-functioning Windows environment, loaded with all the applications required to analyze submitted evidence, including MS Office, Adobe Acrobat, NP-View, etc.

• Clicking on the ‘Secure Evidence Locker’ icon will launch the Locker within the desktop environment.
ERO SEL - Regional Entity Experience

[Image of a computer interface showing a secure evidence locker]

[Details of the interface include:
- Browser:
  - Secure Evidence Locker
  - MKO
  - NPCC
  - RF
  - SERC
  - TXRE
  - WECC
  - NCR12345
- Document List:
  - Raw Notes.txt
  - Entity Submissions
  - Sample Config.xml
  - Imhosts.txt
  - Assets.csv
  - Working Copies
  - Network Overview.vsd
  - AOC Notes.docx
  - Positive Obs Notes.docx
  - Finding Notes.docx
  - Listing.csv
- Properties:
  - Name: Raw Notes.txt
  - Object ID: 090x4558004459a
  - Version: 1.0, CURRENT
  - Content Size: 177B
  - Content Type: text/plain
  - Owner Name: dadmin
  - Optional Metadata
- Virtual Metadata
- Location: 2020-04511
- Versions
- Renditions
- Workflow Tasks
- Workflows
- History]
• All files are wiped from the Analysis Environment when the user logs out
• No ability to remove evidence from Analysis Environment, e.g., copy / paste (data loss prevention control)
• Access restricted to Regional Corporate networks
• Support of new technologies
• Delays created by the COVID-19 pandemic
  ▪ Professional Services (travel and collaboration)
  ▪ Testing and in-person training
Questions and Answers