ERO Enterprise Information Technology Projects Update

Stan Hoptroff, Vice President, Chief Technology Officer and Director of Information Technology
Technology and Security Committee Meeting
November 1, 2019
• ERO Information Technology (IT) Projects Update
  ▪ Align Project Update
  ▪ Situation Awareness for FERC, NERC and the Regional Entities (SAFNRv3)

• Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
  ▪ Salesforce customer relationship management (CRM)
  ▪ E-ISAC Portal
  ▪ Data Analysis

• Priorities Looking Ahead
• Industry stakeholder engagement focused on securing evidence and data
• Industry cyber expertise has been very helpful to our efforts
• Evidence locker design and engineering underway
• Release 1 Schedule development underway
• Data identification, classification, management and destruction
• Aggressive management of role-based credentials
• Control processes and auditing
• Cybersecurity Standards and Frameworks (National Institute of Standards and Technology, Federal Risk and Authorization Management Program, Critical Infrastructure Protection)
• Data and document encryption at-rest and in-transit
• Application and network cyber testing
• Multi-factor authentication for user access
• Cyber Security Risk Information Sharing Program Monitoring
• Application and data isolation
• Evidence isolation
• 24x7 monitoring activity logging
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, as appropriate
Key Features include:

- SAFNR v3 will deploy improved underlying technologies to increase system robustness
- Ability to control views for ERO Enterprise, FERC, and Reliability Coordinators
- Leverages the same real-time data on facilities (>200kV and >500W)
- User dashboard with drill-down capability into data
- Administrator tools that facilitate system updates, topology changes and control access levels
- Visualization of environmental conditions impacting reliability, such as weather, fires, and space weather.
- Overlays of GeoMAC wildfire data to aid in tracking wildfires and associated threats to Bulk Power System facilities.
• Interchangeable base maps
• Commercially available imagery
• Zoom and pan similar to Google Maps controls
• Generators icons signify fuel type
• Substation icons signify per-unit voltage
• Commercially available geolocation (e.g., Platts, ABB Ventyx)
• Radar, temperature (number field or contour), wind speed field
• National Weather Service Watch-Warning – Advisory areas
• Space weather overlay (Geomagnetic Disturbance)
• Esri, GIS user type Fire map overlay
Situation Awareness for FERC, NERC and the Regional Entities (SAFNR)
• Boolean logic and comparisons to administrator (BPSA) defined constants
  ▪ Lines and generators in or out of service
  ▪ ACE or frequency outside bands for associated times
  ▪ Hourly load more than xx% over or under forecast
  ▪ Data sources changing available status

• Rolling 168-hour history, equivalent to data sent by Reliability Coordinators
- Separate window in application able to be displayed alongside map
• New customer-relationship management tool (Salesforce) in production
• E-ISAC Portal – additional refinements underway. Focus on content publication (actionable information)
• Data gathering, management and analysis
Priorities Looking Ahead

- Go-Live for Align Project Release 1 - 2020
- SAFNR v3 go live and retirement of SAFNR v2
- E-ISAC portal platform upgrade
- Analytical capabilities for the E-ISAC
- Outreach capability via a customer-relationship management solution (Salesforce) for the E-ISAC
Questions and Answers
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
Align Release 1: What to expect as a registered entity?

Stakeholder Group

Registered Entities

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 Standards and Requirements applicable to your entity
- Manage user access for your specific entity
### Stakeholder Group

#### Regional Entities

#### 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 Standards and Requirements applicable to a registered entity
Align Release 1: What to expect as NERC?

**Stakeholder Group**

- **NERC Users**
  - Perform oversight of the Regional Entities’ activities
  - View dashboards on new/open action items
  - Create reports required by FERC related to Enforcement and Mitigation activities
  - Generate report of Standards and Requirements applicable to a registered entity
### Align Future Releases: What to expect?

#### Release 2 Functionality
**Est. Q2 2020**

- Technical Feasibility Exceptions
- PDSs
- Self-Certifications

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

#### Release 3 Functionality
**Est. Q4 2020**

- Compliance Planning (Risk, CMEP Implementation Plan, Inherent Risk Assessment, Internal Controls Evaluation, Compliance Oversight Plan)
- Compliance Audit
- Spot Check
- Compliance Investigations
- Complaints
- 10/03/2019 Member Executive Committee (MEC) meeting
- GridSecCon 2019 Recap
- GridEx V Update
- Recommended 2020 Performance Metrics
- Member Information Sharing Initiatives
• Strategic Plan – Key Activities
  ▪ Initiatives to Increase Member Information Sharing
  ▪ Strategic Partnerships Update
    o Financial Systemic Analysis and Resilience Center
    o IESO Collaboration
    o MS-ISAC Collaboration
  ▪ Government Engagement Update
    o DOE Engagement – Memorandum of Understanding
    o Increased Collaboration with the DHS, NSA, DOD
  ▪ Security Operations Staffing
    o 24/5 by 12/31/2019
    o 24/7 by Q3 2020
  ▪ Endorsed Proposed 2020 Performance Metrics
Co-hosted with SERC in Atlanta, GA, October 22-25, 2019

More than 600 Attendees

Keynote speakers:
- Karen S. Evans, Brian M. Harrell, Tom Fanning, Brian Thumm
- Emphasis on increased government-industry collaboration and information sharing

Women’s Networking Breakfast

Expert Panels and Training Sessions

Classified and Unclassified Threat Briefings

Positive feedback from participants and attendees

Evaluating outsourcing options for some functions in 2020
• Simulates a severe cyber-physical attack on electricity and other critical infrastructures across North America
• 420 participating utilities (an increase from 206 in GridEx IV)
• Increased participation from distribution utilities, natural gas, government, and law enforcement
• New approach to Executive Tabletop focusing on extraordinary operational measures and centered on NPCC region
• CEO “Hotwash” call and staff secure video teleconference on November 15
• Metrics designed to align with goals and key supporting activities in the Long-Term Strategic Plan
• Expected to evolve over time as processes and data sources mature
• Reviewed with and reflecting input from the MEC Working Group
• Endorsed by the MEC at the October 3 meeting
• Seeking Technology Security Committee endorsement
• Subject to final review by Corporate Governance and Human Resources Committee
What’s changed since the last TSC meeting?

- Refined the metric definitions
- Refined the method and approach for calculation and data collection
- Identified metric owners and data sources
- Started measurement for a subset of the metrics
- Discussion regarding development of future targets (2020 and beyond)
- MEC review and endorsement
<table>
<thead>
<tr>
<th>Engagement</th>
<th>Information Sharing</th>
<th>Analysis</th>
<th>Staffing and Attrition</th>
</tr>
</thead>
<tbody>
<tr>
<td>% increase in prospective member organizations engaged.</td>
<td>Member Portal Sharing:</td>
<td>% increase of content enriched by E-ISAC analysts</td>
<td>Annual employee attrition rate</td>
</tr>
<tr>
<td>% increase in prospective member organizations that sign up to use the E-ISAC portal.</td>
<td>% increase in number of portal posts by member organizations</td>
<td>Unclassified Threat Workshop content survey results (relevant, timely, unique, actionable)</td>
<td>Total staff and period over period net change</td>
</tr>
<tr>
<td>Frequency of member user interactions by channel</td>
<td>Total Information Shares:</td>
<td>% increase in joint analytical products with partners</td>
<td></td>
</tr>
<tr>
<td>Elapsed time since last member interaction (e.g. share or contact)</td>
<td>% increase in number of information shares by source, channel, and event type</td>
<td>E-ISAC Data Platform project implementation variance from plan</td>
<td></td>
</tr>
<tr>
<td>% increase in diversity of types of member organizations participating in Industry Engagement Program and E-ISAC led workshops</td>
<td>Partner Information Sharing:</td>
<td>% increase in volume of information shares received from partner organizations</td>
<td></td>
</tr>
<tr>
<td>% increase in Canadian member organizations</td>
<td>% increase in quality of information shares received from partner organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canadian Electricity Association support of 2021 budget</td>
<td>Member Information Sharing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% increase in GridEx participation</td>
<td>Volume of member organization information sharing within predefined peer groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% increase in cross-sector participation in GridEx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% increase in state government participation in GridEx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality and usefulness of CRM tool and data: actual results compared to business case assumptions</td>
<td>Security Watch Operations coverage:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On Duty – Core Hours Head Count</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On Call – Off Hours Head Count</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On Duty – Off Hours Head Count</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Watch Operations sharing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IOCs loaded into external sharing platform.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Metric Example – Engagement

Metric: Diversity of types of member organizations participating in Industry Engagement Program (IEP) and E-ISAC-led workshops

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Member Companies</td>
<td>19</td>
<td>17</td>
</tr>
<tr>
<td>Investor-Owned</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Cooperative</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>State/Municipality</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>Federal/Provincial</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Canadian</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total Participants (people)</td>
<td>24</td>
<td>22</td>
</tr>
</tbody>
</table>

More cooperatives engaged in IEP during 2019 than in the prior year.
Diversity measurement only includes IEP participation and does not include other E-ISAC-led workshops.
Canadian asset owner and operators (AOO) membership uses Canadian Electricity Association data as the basis for target Canadian AOO population.
Metric: Member Portal Sharing - increase in number of Portal posts by member organizations

- Includes both cyber and physical security bulletins posted to the E-ISAC Portal
- Information reported via channels outside the Portal (such as bulk reporting) is **not** included
Metric: Enriched content posted by E-ISAC analysts

Enriched content:
- Information shares and open source intelligence that has been evaluated and synthesized by E-ISAC
- Either additional or combined content has been added to the originally shared information, or filtering of information has occurred
• Critical to enhancing the E-ISAC’s products and services
• Scorecard developed and shared with industry CEOs
• Developed a short guide for information sharing
  ▪ Provides examples of what and how members should share
• Task group of MEC Working Group focusing on issue
  ▪ Documenting findings on mechanism to increase sharing
  ▪ Developing a data standardization document
Priorities Ahead

- 24/5 and 24/7 security operations staffing
- Maximize and leverage the value of the CRM/Salesforce tool
- Improve the value and delivery of products and services
- Information sharing by industry and our strategic partners
- Quality and timeliness of the products and services provided to members
- Continuing to strengthen relationships with government and strategic partners
- Using metrics to improve our focus and execution
Questions and Answers