E-ISAC Update

Manny Cancel, Senior Vice President, Chief Executive Officer E-ISAC
Technology and Security Committee Meeting
February 5, 2020
• Recap Member Executive Committee (MEC) Conference Call held on January 23, 2020
• E-ISAC Strategic Plan Update - Key Elements and Schedule
• Next Steps
Recap MEC Conference Call

- Member Information Sharing Initiatives
- Security Operations Staffing
- Year End Performance Metrics
- Strategic Partnerships Update
- Government Engagement
- Strategic Plan Update
• Strategic plan put in place three years ago

• Opportunity to assess plan now to:
  ▪ Confirm strategic and operational focus for both near and long term initiatives
  ▪ Evaluate and refine products and services
  ▪ Sharpen focus on resource allocation
  ▪ Identify areas to provide additional value for members
• **Key Functions**
  - Identify and analyze the security vulnerabilities, threats, and risks pervasive across the industry
  - Gather and sanitize physical and cyber security information and disseminate this information to industry and between government and industry
  - Provide platform(s) for rapid, secure information sharing and collaboration
  - Facilitate meaningful industry events, exercises, and forums

• **Stakeholders**
  - The *entire* electric industry: large, small; private, public
  - U.S. and Canadian governments
The Plan

• Operational - Near Term (1-3 Years): Focus the majority of our time and resources on improving the efficiency and quality of our current product, platform, and service offerings.

• Strategic - Longer Term (3-5 years): Enhance intelligence and analysis capabilities with a focus on mitigating operational technology risk due to cyber threats.
Analysis

- Increase frequency of valuable, in-depth analysis papers
- Improve quality and timeliness of periodic reports
- Expand CRISP coverage and data for analysis
- Leverage technology and partnerships
Information Sharing

- Establish 24x7 staffing
- Increase span, quality, and volume of voluntary shares
- Enhance the information sharing portal
- Improve and expand the automated information sharing capability
Operational: Engagement

Continuous improvement...

- Evaluate sourcing options for GridSecCon and GridEx
- Continue expansion of membership
- Increase use of products and services across segments

Engagement

Exercise(s)
Conference(s)
Industry Engagement Program
Workshops
Seminars
Schedule

Jan  
Feb  
Mar  
Apr  
May  
June  
July

Industry input gathering

MEC Meeting Apr 14

Draft plan/ draft 2021 budget

Feedback

MEC Meeting Jul 21

Final plan / final 2021 budget, 2020, 2023 projections
Next Steps

• Establish 24/7 security operations staffing
• Maximize and leverage the CRM/Salesforce tool
• Improve the value and delivery of products and services
• Continue to strengthen relationships with government and strategic partners
• Use metrics to improve our focus and execution
• Coordinate with MEC on Strategic Plan Update
• Develop 2021 budget
Questions and Answers
ERO Enterprise Information Technology Projects Update

Stan Hoptroff, Vice President, Chief Technology Officer and Director of Information Technology
Technology and Security Committee Meeting
February 5, 2020
• ERO Information Technology (IT) Projects Update
  ▪ Align Project Update
  ▪ Situation Awareness for FERC, NERC and the Regional Entities (SAFNRv3)
  ▪ Entity Registration (CORES)

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

• Priorities Looking Ahead
Why Align?

• Drive alignment and consistency in Regional Entity Compliance Monitoring and Enforcement Program (CMEP) practices to ensure more equity in outcomes for registered entities

• Improve the security of handling highly sensitive information

• Capture productivity gains
• All evidence will go into the registered entity or ERO Enterprise locker (any registered entity locker must meet certain criteria the ERO Enterprise develops for functionality, access, etc.).

• ERO Enterprise workflow and work products will be in the ERO Enterprise Align tool.

• The ERO Enterprise will enhance ERO Enterprise work products (e.g., working papers) to support conclusions without the need to store data for extended periods, avoiding a data protection risk.

**NOTE:** Achieving this will occur via training, guidance, oversight activities and other outreach.
Align - Application Security

- Consistent with cybersecurity Standards and Frameworks - National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FEDRAMP), NERC CIP
- Data identification, classification, management, and destruction
- Aggressive management of role-based credentials
- Evidence and data separation and isolation
- Control processes and auditing
Align - Application Security

- Application, patch release, and network cyber testing
- Multi-factor authentication for user access
- 24x7 monitoring and activity logging
- Cyber Risk Information Sharing Program (CRISP) monitoring for CRISP participants and NERC
- Isolated Virtual Network
• Logical Boundary Controls
• Encryption at-rest and in-transit
• Controlled encryption key management
• Integrity monitoring
• Login and Access Monitoring
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 upon submission
- Is securely isolated per entity
- Is never extracted
- Is subject to proactive and disciplined destruction policy
• Adherence to NIST security frameworks
• Outbound communications limited
  ▪ No ability to extract evidence
• Analysis environment destruction upon log out
• No direct access to the evidence
• File level permissions applied to evidence
**ERO Enterprise Data Analysis Locker**

- Entity specific lockers
- Data Loss Prevention
- Regional Encryption
- Unidirectional Data Flow

**Entity Provided Data Analysis Locker**

- Entity controls access
- Entity selects level of security
- Entity must provide defined capabilities to the ERO

**Secure Storage and Access**

**No Transfer of Possession**
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

Align Release 1: What to expect as a Regional 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, PDSs, Self-Certifications, Complaints)
- Perform Preliminary Screens, Potential Noncompliance 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

Release 1 Functionality

- 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
How do I 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 CMEP Regional workshops
• Trades meetings, as appropriate
Key Features include:

- Situational Awareness for FERC, NERC and Regions (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.
• Benefits
  ▪ One common registration tool for the ERO Enterprise
  ▪ Consistent registration experience for registered entities
  ▪ Ability to easily share registration data
  ▪ Data integration with Align
What to expect as a registered entity?

<table>
<thead>
<tr>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create and submit new registration requests</td>
</tr>
<tr>
<td>• Receive notifications when new registrations are submitted</td>
</tr>
<tr>
<td>• After Regional and NERC approval, manage the newly submitted registration record</td>
</tr>
<tr>
<td>• Manage existing registration records (those that exist today in CITS, CDMS, and CRATS)</td>
</tr>
<tr>
<td>• Manage contacts for their entity</td>
</tr>
<tr>
<td>• Receive notifications when registration changes (including new registrations) are approved</td>
</tr>
<tr>
<td>• View Coordinated Oversight Information related to their entity</td>
</tr>
</tbody>
</table>
• New customer-relationship management tool (Salesforce) in production supporting post GridEx activities along with tracking member and stakeholder contacts

• E-ISAC Portal – additional refinements underway. Focus on content publication (actionable information)

• E-ISAC Data Platform build out occurring with a heavy focus on data interfaces and data sharing. Which will enable additional improved analytics and information sharing
Priorities Looking Ahead

- Go-Live for Align Project Release 1 - 2020
- E-ISAC portal platform upgrade
- Analytical capabilities for the E-ISAC
- Accelerated adoption of Salesforce capabilities for the E-ISAC
- Development of the Geomagnetic Disturbance application
- Implementation of additional collaboration capabilities, e.g. Microsoft Teams
- Various software/hardware upgrades to NERC infrastructure
Questions and Answers
Additional Slides
### Release 2 Functionality
**Est. 2021**

- Technical Feasibility Exceptions
- Periodic Data Submittals
- 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. 2021**

- Compliance Planning (Risk, CMEP Implementation Plan, Inherent Risk Assessment, Internal Controls Evaluation, Compliance Oversight Plan)
- Compliance Audit
- Spot Check
- Compliance Investigations
- Complaints
PNC Review

Interface for Regions

### POTENTIAL NONCOMPLIANCES IN REVIEW

<table>
<thead>
<tr>
<th>MONTO... METHOD</th>
<th>UNIQUE ID</th>
<th>NCR</th>
<th>ENTITY</th>
<th>REGION AND JURISDICTION</th>
<th>STANDARD</th>
<th>REQ.</th>
<th>RECEIVED</th>
<th>VIOLATION START DATE</th>
<th>REVIEW STATUS</th>
<th>RECOMMENDATION</th>
<th>DISPOSITION</th>
<th>ASSIGNED TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Report</td>
<td>2019-00579</td>
<td>NCR99999 Test Entity</td>
<td>WECC-US</td>
<td>CIP-002-3b</td>
<td>R1.</td>
<td></td>
<td>08/13/20...</td>
<td>08/09/2019</td>
<td>IN PROGRESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-00583</td>
<td>NCR99999 Test Entity</td>
<td>WECC-US</td>
<td>CIP-002-3</td>
<td>R2.</td>
<td></td>
<td>08/14/20...</td>
<td>08/14/2019</td>
<td>IN PROGRESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-00602</td>
<td>NCR99999 Test Entity</td>
<td>WECC-US</td>
<td>VAR-005-4.1</td>
<td>R1.</td>
<td></td>
<td>08/19/20...</td>
<td>08/19/2019</td>
<td>COMPLETE</td>
<td>Dismissed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-00606</td>
<td>NCR99999 Test Entity</td>
<td>WECC-US</td>
<td>COM-005-1.1</td>
<td>R11.</td>
<td></td>
<td>08/20/20...</td>
<td>08/19/2019</td>
<td>IN PROGRESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>2019-00620</td>
<td>NCR99999 Test Entity</td>
<td>WECC-US</td>
<td>CIP-002-5.1a</td>
<td>R1.</td>
<td></td>
<td>08/23/20...</td>
<td>08/20/2019</td>
<td>IN PROGRESS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CONSOLIDATE A PNC UNDER AN OPEN ENFORCEMENT ACTION

<table>
<thead>
<tr>
<th>TY</th>
<th>UNIQUE ID</th>
<th>NCR</th>
<th>ENTITY</th>
<th>REGION AND JURISDICTION</th>
<th>STANDARD</th>
<th>REQ.</th>
<th>VIOLATION START DATE</th>
</tr>
</thead>
</table>

**INSTRUCTIONS**

This is the PNC Review Dashboard. From the top pane, you can open a PNC, review the submitted information and update it as needed.

When completed, the PNC may be processed in one of two ways:

1. It can be handled as an Enforcement Action. To do this, open the PNC from the top pane and choose “Save and Action.”

2. It can be consolidated under an existing Open Enforcement Action. To do this, open the Enforcement Action from the bottom pane, link the PNC to the EA, and save the EA.
Dispositions and Notifications Interface for Regions

### ACTIVE DISPOSITIONS

<table>
<thead>
<tr>
<th>DISPOSITION TYPE</th>
<th>UNIQUE ID</th>
<th>NCR</th>
<th>ENTITY</th>
<th>CASE FILE ID</th>
<th>NERC NOC#</th>
<th>SEND NOTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dismissal</td>
<td>2019-00887</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>sdfsdfsadfasd</td>
<td>dcdsdcfd</td>
<td>Send Dismissal Letter</td>
</tr>
<tr>
<td>Dismissal</td>
<td>2019-00885</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>sdfsdfsadfasd</td>
<td>dcdsdcfd</td>
<td>Send Dismissal Letter</td>
</tr>
<tr>
<td>Compliance</td>
<td>2019-00881</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>Aaron Test Dec 3</td>
<td>CE Letter Sent</td>
<td>Send CE Letter</td>
</tr>
<tr>
<td>Compliance</td>
<td>2019-00879</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>asa</td>
<td></td>
<td>Send CE Letter</td>
</tr>
<tr>
<td>Pending</td>
<td>2019-00888</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>test NAVAPS to CE</td>
<td>NAVAPS Sent</td>
<td>NAVAPS Sent</td>
</tr>
</tbody>
</table>

### ENFORCEMENT ACTIONS RELATED TO DISPOSITION

<table>
<thead>
<tr>
<th>TYPE</th>
<th>UNIQUE ID</th>
<th>NCR</th>
<th>ENTITY</th>
<th>STANDARD</th>
<th>REGION</th>
<th>VIOLATION START DATE</th>
<th>STATUS</th>
<th>TYPE</th>
<th>DUE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Report</td>
<td>2019-00881</td>
<td>NCR99999</td>
<td>Test Entity</td>
<td>CIP: 002-5.1a</td>
<td>R1.</td>
<td>01/01/2019</td>
<td>CEA Processing</td>
<td>Compliance Exception Letter</td>
<td>12/13/2019</td>
</tr>
</tbody>
</table>

Instructions and Help text will be provided in this area. Language still in development.
### Mitigation Management Interface for Registered Entities

#### MY MITIGATING ACTIVITIES AND MITIGATION PLANS

<table>
<thead>
<tr>
<th>TYPE</th>
<th>UNIQUE ID</th>
<th>REGION OR LRE</th>
<th>REGISTRATION</th>
<th>DATE SUBMITTED</th>
<th>STANDARD</th>
<th>REQ</th>
<th>REGION AND JURISDICTION</th>
<th>START DATE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation Plan</td>
<td>2019-00877</td>
<td>WECC</td>
<td>NCR99999 Test Entity</td>
<td>12/03/2019</td>
<td>CIP-005-5</td>
<td>R2</td>
<td>WECC-US</td>
<td>11/15/2019</td>
<td>Incomplete Returned as Incomplete</td>
</tr>
<tr>
<td>Mitigating Activities</td>
<td>2019-00481</td>
<td>WECC</td>
<td>NCR00000 Test Entity</td>
<td>08/07/2019</td>
<td>CIP-062-3jb</td>
<td>R2</td>
<td>WECC-US</td>
<td>11/01/2019</td>
<td>Active</td>
</tr>
<tr>
<td>Mitigating Activities</td>
<td>2019-00678</td>
<td>WECC</td>
<td>NCR99999 Test Entity</td>
<td>09/18/2019</td>
<td>EOP-004-4</td>
<td>R1</td>
<td>WECC-US</td>
<td>05/10/2018</td>
<td>CEA Processing due 01/24/2020</td>
</tr>
</tbody>
</table>

#### RELATED MILESTONES

<table>
<thead>
<tr>
<th>TYPE OF MILESTONE</th>
<th>UNIQUE ID</th>
<th>NAME</th>
<th>DUE DATE</th>
<th>COMPLETION DATE</th>
<th>REQUEST EXTENSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive Control</td>
<td>2019-00858</td>
<td>Address Root Cause</td>
<td>12/27/2019</td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

#### ACTIVE REQUESTS FOR INFORMATION

<table>
<thead>
<tr>
<th>DUE DATE</th>
<th>ID</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/08/2</td>
<td>2019-00424</td>
<td>UAT LS 8/7</td>
</tr>
<tr>
<td>09/08/2</td>
<td>2019-00424</td>
<td>UAT LS 8/7</td>
</tr>
<tr>
<td>09/07/2</td>
<td>2019-00435</td>
<td>Testing - L5</td>
</tr>
<tr>
<td>09/07/2</td>
<td>2019-00435</td>
<td>Testing - L5</td>
</tr>
<tr>
<td>09/07/2</td>
<td>2019-00530</td>
<td>need info</td>
</tr>
<tr>
<td>09/07/2</td>
<td>2019-00530</td>
<td>need info</td>
</tr>
<tr>
<td>09/07/2</td>
<td>2019-00530</td>
<td>for Scenario 5 RF1001 attached</td>
</tr>
</tbody>
</table>
# Findings and Enforcement Actions Interface for Registered Entities

## MY FINDINGS

<table>
<thead>
<tr>
<th>MONITORING METHOD</th>
<th>UNIQUE ID</th>
<th>REGION OR LRE</th>
<th>DATE SUBMITTED</th>
<th>REGISTRATION</th>
<th>STANDARD</th>
<th>REQ</th>
<th>START DATE</th>
<th>FINDING STATUS</th>
<th>SEND UPDATE</th>
<th>MITIGATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Report</td>
<td>2019-06552</td>
<td>TXRE</td>
<td>09/03/2019</td>
<td>NCR99999 Test Entity</td>
<td>CIP-002-5.1</td>
<td>R1.</td>
<td></td>
<td>Preliminary Screening</td>
<td>+</td>
<td>Mitigating Activities Draft</td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-06557</td>
<td>TXRE</td>
<td>08/08/2019</td>
<td>NCR99999 Test Entity</td>
<td>CIP-002-3(b)</td>
<td>R2.</td>
<td></td>
<td>PNC Review</td>
<td>+</td>
<td>Mitigating Activities Draft</td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-06728</td>
<td>TXRE</td>
<td>10/07/2019</td>
<td>NCR99999 Test Entity</td>
<td>CIP-002-5.1a</td>
<td>R2.</td>
<td></td>
<td>PNC Review</td>
<td>+</td>
<td>Mitigating Activities OEA Processing</td>
</tr>
<tr>
<td>Audit</td>
<td>2019-06827</td>
<td>TXRE</td>
<td>10/31/2019</td>
<td>NCR99999 Test Entity</td>
<td>BAL-061-TRE-1</td>
<td>R8.</td>
<td>10/01/2019</td>
<td>Preliminary Screening</td>
<td>+</td>
<td>Mitigating Activities Draft</td>
</tr>
<tr>
<td>Audit</td>
<td>2019-06500</td>
<td>SERC</td>
<td>09/19/2019</td>
<td>NCR99999 Test Entity</td>
<td>CIP-002-5.1a</td>
<td>R2.</td>
<td>09/14/2018</td>
<td>Preliminary Screening</td>
<td>+</td>
<td>Mitigating Activities Draft</td>
</tr>
<tr>
<td>Self-Report</td>
<td>2019-06400</td>
<td>WECC</td>
<td>08/07/2019</td>
<td>NCR99999 Test Entity</td>
<td>CIP-007-6</td>
<td>R2.</td>
<td>07/01/2019</td>
<td>Enforcement Processing</td>
<td>+</td>
<td>Mitigating Activities Active</td>
</tr>
</tbody>
</table>

## INSTRUCTIONS

This is your Findings dashboard. From here, you can see the status of all the potential noncompliances associated with your Registration(s). You can view those findings, and you can send a Finding Update to provide your Region with more information. You can also access your Mitigation from this screen. A summary of the process a Finding goes through is shown on the right.
ERO Enterprise Security Initiatives

Bill Lawrence, Vice President, ERO Enterprise Security Initiatives
Technology and Security Committee Meeting
February 5, 2020
• Support Region external-facing initiatives in cyber and physical security programs and awareness for registered entities, including sharing of best practices and security training
• Work with Stan Hoptroff, NERC CTO, and the Information Technology Security Group (ITSG) to set the “gold standard” of protection for ERO systems and data
• Address cyber and physical security priorities identified in the Reliability Issues Steering Committee (RISC) report with the ERO Enterprise and industry groups, including the North American Transmission Forum and North American Generator Forum

• Provide executive leadership on NERC’s EMP efforts and deliver insights on the current state-of-the art mitigation approaches, including latest scientific reports and literature

• Engage with the RISC, ITSG, and the new Reliability and Security Technical Committee (RSTC) for coordinated ERO Enterprise action on security initiatives
• Strengthen the situation awareness and infrastructure security coordination and activities of NERC and the Regions to respond to a major grid crisis, either an operational event or in a grid security emergency

• Review NERC’s Crisis Action Plan for improvements and build an ERO Enterprise CAP, with business continuity considerations

• Design and lead drills of the CAP with the ERO Enterprise, building up to major industry and government exercises
Questions and Answers