

A DIVISION OF NERC



# E-ISAC

ELECTRICITY  
INFORMATION SHARING AND ANALYSIS CENTER

# E-ISAC Update

Manny Cancel

Technology and Security Committee Open Session

February 9, 2022

**TLP:WHITE**

**RELIABILITY | RESILIENCE | SECURITY**



- Membership Outreach – Member Executive Committee (MEC)
- Threat Landscape
- Operational Technology (OT) Visibility and Joint Cyber Defense Collaborative (JCDC) support
- Other Activities
- Grid Ex VI Recap

## Member Executive Committee

- Established by the ESCC to serve as a customer advisory board to the E-ISAC and provide senior industry leadership expertise and guidance to inform the strategic direction of the E-ISAC and increase value to the electricity sector
- Provides strategic-level input on:
  - E-ISAC's strategic plan
  - Operational focus areas
  - Budget development
  - Performance metrics

MEC Member	Company
Bill Fehrman (Chair)	Berkshire Hathaway
Ann Delenela	Entergy
Eóin Cooke	AltaLink
Jim Jones	Great River Energy
Jim Robb	NERC
Margaret Hopkins	Puget Sound Energy
Mike Fish	Salt River Project
Scott Smith	City of Bryan Texas
Steve Swick	AEP
Tom O'Brien	PJM
Tom Wilson	Southern

- Outreach conducted to discuss expectations for E-ISAC
  - Information sharing and curated analysis
  - Support for key programs (e.g., CRISP, OT Visibility, Automated Information Sharing)
  - Additional collaboration with Natural Gas Sector
- Other observations
  - What is status of E-ISAC Long-Term Strategic Plan?
  - Cadence and value of MEC Meetings
  - Enhance value by driving increased engagement and action

## Next Steps

- Reduce number of MEC Meetings
  - April 2022 meeting will be canceled
- Work with MEC members to identify opportunities to increase the value of meetings and engagement, and improve overall content
- Engage members on strategic topics

## Long-Term Strategic Plan

- Provide timely and actionable information and facilitate increased information sharing
  - 48% increase in E-ISAC products in 2021
  - Supply chain, ransomware, critical vulnerabilities
  - Automated information sharing pilot (ESSIX)
- Enhance the E-ISAC's analytical capabilities
  - OT Visibility (Dragos/Essence) and CRISP OT Pilot
  - Project Lighthouse
  - Joint Cyber Defense Collaborative (JCDC) support
- Increase focus on operational technology risks
  - OT Visibility and CRISP/Essence OT Pilot

## Long-Term Strategic Plan (cont'd)

- Enhance the E-ISAC's capability to leverage classified and other critical threat and intelligence information
  - Increased participation in classified briefings
  - New threat intelligence sources
- Explore extending services to other sectors
  - Increased collaboration with natural gas and other critical infrastructure sector
    - Log4j
    - Ransomware
    - Geopolitical tensions



- Geopolitical tension
- Log4j vulnerability
- Conti ransomware
- Domestic violent extremists threats
- Geopolitical tensions
- Insider Threat



- Operational Technology (OT) Visibility
  - Deployments continue across the sector
  - E-ISAC CTI team monitoring Neighborhood Keeper
  - Coordinating with DNG-ISAC on gas related queries
- CRISP OT Dragos/Essence pilots
- Joint Cyber Defense Collaborative (JCDC) support
  - Coordination with DOE and DHS

- CRISP Expansion
- E-ISAC Portal
- ESSIX (Automated information sharing)
- Membership outreach and industry engagement
- 2023 Business Plan and Budget development

## GridEx VI Distributed Play Participation

Participating organizations: 293

Planners: 766

Participating organizations by sector:

Chemical	Government Facilities
Commercial Facilities	Information Technology
Communications	Natural Gas
Critical Manufacturing	Nuclear Reactors
Dams	Oil
Electricity	Transportation Systems
Emergency Services	Water and Wastewater Systems
Financial Services	

- Send out planning materials earlier
- Encourage greater collaboration between utilities and reliability coordinators
- Continue to allow/encourage planners to customize the exercise (MSEL, scenario, injects, etc.) to meet their objectives
- Expand NERC's participation in GridEx VI by testing alternative communications to simulate email being compromised
- Continue to host website with planner documents; provide greater clarity on access and troubleshooting



- Key themes:
  - Operational coordination Telecommunications and Gas
  - Government authorities (e.g. Grid Security Emergency Orders)
  - Security of inverter-based resources
  - Narrative warfare/mis-information

- Continue current activities:
  - Build effective communications mechanisms
  - Build on the shared consensus regarding Grid Security Emergency Orders
  - Coordinate between the electricity and natural gas providers
  - Reinforce relationships between governments in the United States and Canada
- Clarify ESCC/government roles with crisis communications
- Strengthen operational coordination between electricity and communications



- Finalize after action report
- Identify action items and identify individuals to support
- Conduct briefing in March/April to summarize report and action plan



A stylized map of North America is shown in the background. The United States and southern Canada are filled with a dark blue color, while Mexico is shown in a light grey color. A horizontal band of a lighter blue color runs across the middle of the map, behind the title text.

## Questions and Answers

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

Agenda Item 3

# ERO Enterprise Align Project

Stan Hoptroff, Vice President, Business Technology  
LaCreacia Smith, Senior PMO Manager, ERO PMO  
Technology and Security Committee Open Meeting  
February 9, 2022

**RELIABILITY | RESILIENCE | SECURITY**



- Align Release 3 Functionality
- Align Release 3 Lessons Learned
- Align Release 4 Functionality
- Align Project Timeline
- Canadian Update
- Current Challenges
- How to Stay Informed

## **Release 3 Functionality**

- Audit Scope
- Audit Notification Package
  - Audit Notification Letter
  - Pre-Audit survey
- CMEP Staff Working Papers
  - Secure Evidence Locker Reference Number
  - Status
  - Actions (Potential Noncompliances, Areas of Concern, etc.)
- Regional Notes
  - Compliance Culture
- Findings Created for Enforcement
- Final Audit Report Generation

## FULL YEAR SCHEDULE

YEAR	NCR/CO GROUP #	ENTITY NAME(S)	FUNCTIONS	R / ...	ENGAG... SCOPE	ST... DATE	END DATE	ANP DATE	ASSIGNED RESOU...	OBSERVERS
2021	NCR00303	Municipal Energy Agency Of Nebraska	RP	R	CIP	08/03/20	08/14/20		Sophie Gommers	
2021	NCR00102	Basin Electric Power Cooperative	DP, GO, GOP, RP, TO, TP	R	O&P	11/29/20	12/03/20		MRO Editor 1	
2021	NCR00961	Alliant Energy - East	BA, DP, GO, GOP, RP	R	Both	08/16/20	08/21/20		Andy Rodriquez, Caroline Bommel, Dan	ERO 1, ERO 2, ERO 3,
2021	NCR00674	Minnesota Power (Allele, Inc.)	BA, DP, GO, GOP, RP, TO,	R	O&P	09/06/20	09/20/20		Admin Admin, align tester 3, Andy	Aviance Clay
2021	NCR00818	Madison Gas And Electric Company	BA, DP, GO, GOP, RP	R	CIP	08/16/20	08/20/20		Brenton Matthews, MRO Editor 1	
2021	NCR11823	Red Pine Wind Project, LLC	GO, GOP	R	CIP	08/18/20	08/25/20		Caroline Bommel, Dan Chanda	
2021	NCR01081	City Utilities Of Springfield, MO	DP, GO, GOP, RP, TO, TOP,	R	CIP	08/06/20	09/06/20		Andy Rodriquez, Jochem Tolk	
2021	NCR00860	Omaha Public Power District	DP, GO, GOP, RP TO, TOP	R	CIP	08/24/20	08/28/20		Caroline Bommel, MRO Editor 1	

TEST DATA

SCHEDULED ENGAGEMENTS					
SCHEDULE ID▲	REGISTRATION	START DATE	END DATE	TYPE NAME	EDIT ENGAGEMENT
SH21-00370	NCR01015 - Montana-Dakota Utilities Company in MRO	10/06/2021	10/15/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00370	NCR01143 - Southwest Power Pool, Inc. in MRO	10/06/2021	10/15/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00363	NCR00381 - Hennepin County, MN in MRO				<a href="#">Edit</a>
SH21-00352	NCR11880 - Upstream Wind Energy, LLC in MRO	09/17/2021	11/26/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00350	NCR00303 - Municipal Energy Agency Of Nebraska in MRO	09/13/2021	09/15/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00349	NCR00102 - Basin Electric Power Cooperative in MRO	09/13/2021	09/14/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00339	NCR00961 - Alliant Energy - East in MRO	09/30/2021	01/01/2022	Spot Check	<a href="#">Edit</a>
SH21-00338	NCR00961 - Alliant Energy - East in MRO	09/01/2021		Compliance Audit	<a href="#">Edit</a>
SH21-00337	NCR00961 - Alliant Energy - East in MRO	09/01/2021	09/03/2021	Spot Check	<a href="#">Edit</a>
SH21-00336	NCR00962 - Alliant Energy - West in MRO	09/13/2021	09/15/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00335	NCR00102 - Basin Electric Power Cooperative in MRO				<a href="#">Edit</a>
SH21-00327	NCR00961 - Alliant Energy - East in MRO	08/27/2021	08/31/2021	Compliance Audit	<a href="#">Edit</a>
SH21-00323	NCR11778 - Thunder Ranch Wind Project, LLC in MRO			Spot Check	<a href="#">Edit</a>

TEST DATA

General Working Papers Issues ANP Findings Report						
Working Papers						
SUBJECT	ASSIGNED TEAM MEMBERS	RSAW STATUS	REVIEW STATUS	SEL REFERENCE	ACTION	
NCR00086 - Boise-Kuna Irrigation District in WECC				WECC NCR00086 ME21-00011 ME21-00011		
CIP-002-5.1a R1. for NCR00086-WECC	WECC Editor 1	Not Started	In Progress	WECC NCR00086 ME21-00011 ME21-00011 CIP-002-5.1a R1.		
CIP-002-5.1a R2. for NCR00086-WECC	Assign Team Member	Not Started	Not Started	WECC NCR00086 ME21-00011 ME21-00011 CIP-002-5.1a R2.		
CIP-003-8 R1. for NCR00086-WECC	WECC Editor 1	Internal Review Complete	PNC	WECC NCR00086 ME21-00011 ME21-00011 CIP-003-8 R1.		
CIP-003-8 R2. for NCR00086-WECC	WECC Editor 1	In Progress	Not Applicable	WECC NCR00086 ME21-00011 ME21-00011 CIP-003-8 R2.		
CIP-003-8 R3. for NCR00086-WECC	WECC Editor 1	Internal Review Complete	Not Applicable	WECC NCR00086 ME21-00011 ME21-00011 CIP-003-8 R3.		

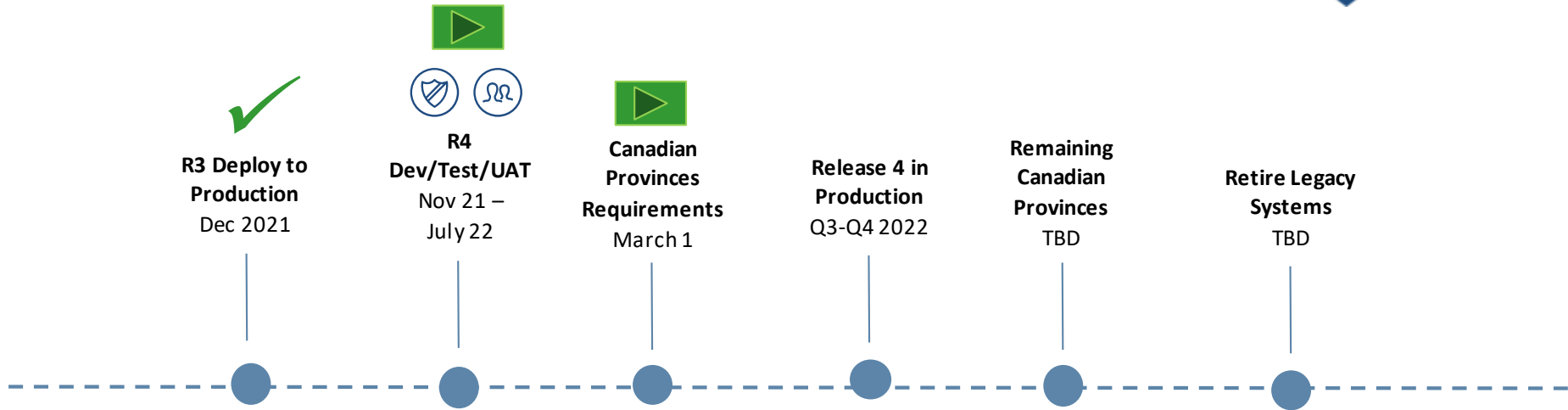
Page 1 of 1



- Our performance testing program was inadequate
- The migration of historical records impacted Periodic Data Submittals and Self-Certification, both of which are bulk processes
- Software updates deployed separately from additional functionality

- Audit Enhancements
- Scheduling Enhancements
- Inherent Risk Assessment
- Compliance Oversight Plan

- Requirements Gathering in Progress
- Implementation Plan (under review)
  - Manitoba & Saskatchewan (MRO) – Q2 2022
  - Alberta & British Columbia (WECC) – Q3 2022
  - Nova Scotia (NPCC) – Q4 2022



**AUDIENCE IMPACT KEY**




Registered Entities    ERO Enterprise Staff

 *In progress*

 *Complete*

- **Project Fatigue:** Maintaining team and stakeholder engagement
- **People:** Parallel efforts (R1-R3 performance and stability efforts; R4 development)
- **Technical:** Finding the right balance between our unique business needs and the platform (extensions and future upgrades)
- **Cost Management:** Balancing available funds and business requirements (enhancements)

## Key communication vehicles

- Align newsletter for Regions and registered entities
- Regional Change Agent Network
- Dedicated project page on NERC.com: [Click Here](#)
- CMEP Regional workshops
- NERC News
- Social media



# Questions and Answers

Moving to a common platform has provided:

- **A more secure** method of managing and storing Compliance Monitoring and Enforcement Program (CMEP) data
- Alignment of **common 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
- **Ease of Access:** Ability to download all standards and requirements for use in other systems



# **Background and Reference Material**

## 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 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

## Stakeholder Group

### Registered Entities



## Release 2 Functionality

- Create, submit, and modify Technical Feasibility Exceptions
- Create, manage and respond to Periodic Data Submittals
- Create and manage Self-Certifications
- Receive and respond to RFIs
- Receive notifications and view dashboards on new/open action items
- Manage user access for your specific entity

## Stakeholder Group

### Registered Entities



## Release 3 Functionality

- Use Align for compliance monitoring engagements (Audit, Spot Checks, and Investigations)
- Ability to review audit report details
- Expand RFIs for Audits

## Stakeholder Group

### Registered Entities



## Release 4 Functionality

- Enhanced Audit and Scheduling functionalities
- Compliance Planning (Inherent Risk Assessment and Compliance Oversight Plan)
- Expand RFIs for Compliance Planning

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

Agenda Item 4

# ERO Enterprise Business Technology

Stan Hoptroff, Vice President, Business Technology  
Technology and Security Committee Open Meeting  
February 9, 2022

**RELIABILITY | RESILIENCE | SECURITY**



- Program Area Technologies
- Shared Services Technologies
- Business Technologies (IT)

- Current Investments
  - E-ISAC Portal migration to Salesforce: February 2021
- Future Investments
  - Centralized Organization Registration ERO System Enhancements
  - Generation, Transmission and Event Management tracking enhancements (previously deferred)
  - Reliability Assessment Data System
  - Situation Awareness FERC, NERC and Regions enhancements (additional data points, forced oscillation and visibility for >200kV facilities)



- Current Investments
  - DC Office Buildout in support of NERC 2.0
    - Huddle Rooms
    - Conference Rooms
    - Team Rooms
    - Watch Operations (E-ISAC)
    - Extra Large Conference Rooms (75" displays)
- Future Investments
  - Integrated Human Resources and Finance & Accounting systems
  - Internal Audit and Risk Management system

- Current Investments
  - Mobile Device Management (MDM)
  - Identity Access Management (7K client base)
  - Privileged Access Management (system administration)
  - Data Loss Prevention (inadvertent disclosure)
- Future Investments
  - Enhanced Cyber Security Capabilities
  - Disaster Recovery Implementation (backup data center)
  - Selected Core Infrastructure to off-premise (enhanced support, security and functionality not available on premise)



# Questions and Answers