Agenda
Technology and Security Committee
Open Meeting

February 15, 2023 | 10:15-11:00 a.m. Mountain Zone

JW Marriott Tucson
3800 W Starr Pass Blvd.
Tucson, AZ 85745

Conference Room: Tucson Salons E-F

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines*

Agenda Items

1. **Minutes*** – **Approve**

   a. November 7, 2022 Open Meeting

2. **E-ISAC Operations*—** **Update**

   a. **Threat Briefing (Cyber, Physical)**

   b. **Intelligence Projects**

   c. **Vendor Affiliate Program**

3. **ERO Enterprise Business Technology*** **— Update**

   a. **Business Continuity Program**

   b. **Align Project**

4. **Annual Review of Committee Mandate*** **— Update**

5. **Other Matters and Adjournment**

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.

- Discussions of a participant's marketing strategies.

- Discussions regarding how customers and geographical areas are to be divided among competitors.

- Discussions concerning the exclusion of competitors from markets.

- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.

- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.

- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

DRAFT Minutes
Technology and Security Committee Meeting

November 7, 2022 | 2:30-3:30 p.m. Eastern

Conference Call

Call to Order

Ms. Jane Allen, Chair, called to order a duly noticed open meeting of the Technology and Security Committee (the Committee) of the Board of Trustees (Board) of the North American Electric Reliability Corporation (NERC) on August 17, 2022 at approximately 9:15 a.m. Pacific, and a quorum was declared present.

Present at the meeting were:

Committee Members	Board Members
Jane Allen, Chair	James B. Robb, NERC President and Chief Executive Officer
Colleen Sidford	Robert G. Clarke
Jim Piro	Susan Kelly
Robin E. Manning	Larry Irving
Suzanne Keenan	George S. Hawkins
Kenneth W. DeFontes, *ex officio*	Roy Thilly

NERC Staff

Andy Sharp, Vice President and Chief Financial Officer
Bryan Preston, Vice President, People and Culture
Janet Sena, Senior Vice President, External Affairs
Justin Lofquist, Director, Enterprise Application Architecture
Howard Gugel, Vice President, Engineering and Standards
Kelly Hanson, Senior Vice President and Chief Administrative Officer
Mark Lauby, Senior Vice President and Chief Engineer
Matthew Duncan, Director, Intelligence, E-ISAC
Mechelle Thomas, Vice President, Compliance
Sônia Mendonça, Senior Vice President, General Counsel, and Corporate Secretary
Stan Hoptroff, Vice President, Business Technology
Tina Buzzard, Assistant Corporate Secretary

NERC Antitrust Compliance Guidelines

Ms. Buzzard directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda, and indicated that all questions regarding antitrust compliance or related matters should be directed to Ms. Mendonça.

RELIABILITY | RESILIENCE | SECURITY

Introduction and Chair's Remarks

Ms. Allen welcomed everyone to the meeting and reviewed the agenda. She provided a summary of the Committee's November 1, 2022 closed meeting, noting that the Committee received an update on the threat landscape, the ERO Enterprise Cyber Posture, as well as the results of a phishing test conducted with the NERC Trustees.

Minutes

Upon motion duly made and seconded, the August 17, 2022 meeting minutes were approved as presented at the meeting.

E-ISAC Operations

Mr. Duncan provided an update on E-ISAC operations, focusing on the E-ISAC's 2022 accomplishments, 2023 priorities and work plan, the threat landscape and cyber threat mitigation. The Committee discussed recent increases in CRISP membership and steps the E-ISAC and industry are taking to get ahead of cyber threats.
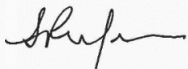
ERO Enterprise Align Project

Mr. Hoptroff and Mr. Lofquist provided an update on the NERC applications roadmap for 2023. They discussed NERC's plans for the following applications: NERC Alerts, Generating Availability Data System (GADS) Wind, GADS Solar, Reliability Coordinator Information System, and the Enterprise Data Analytics Center. They also highlighted the work of the NERC Applications Development and Support Team and provided an update on the status of the Align project, including Release 4.5 and Align governance model.

The Committee discussed the size of facilities included in GADS Solar, the investments for these applications, efforts to ensure data integrity for the analytics initiative, and including the Regional Entities in the discussions related to Finance and Human Resources applications.

Adjournment

There being no further business, the meeting was adjourned.

Submitted by,

Sônia Mendonça
Corporate Secretary

Electricity Information Sharing and Analysis Center (E-ISAC) Operations

Action
Update

Background

Management will provide the Technology and Security Committee an update regarding E-ISAC operations. The update will include a discussion of the security threat landscape, intelligence projects, and the Vendor Affiliate Program.

- <u>Threat Landscape</u>: Management will discuss E-ISAC's tracking of potential threats to the electric sector, including from nation state actors and physical security incidents.

- <u>Intelligence Projects</u>: Management will provide an update on the Cybersecurity Risk Information Sharing Program (CRISP) and participation in the Energy Threat Analysis Center (ETAC).

- <u>Vendor Affiliate Program</u>: Management will provide an update on the Vendor Affiliate Program, including its launch in 2022 and plans for 2023.

- 2022 Review

- Threat Briefing

- Cybersecurity Risk Information Sharing Program (CRISP)

- Vendor Affiliate Program

RELIABILITY | RESILIENCE | SECURITY

- Complex Geopolitical Landscape
  - Russian Ukraine conflict presents unique challenges
  - China remains active
  - Iran, North Korea, and others look for opportunities
- E-ISAC Response
  - Tri-Sector Coordination (Energy, Finance, and Communications)
  - "SHIELDS UP"
  - ERO Crisis Action Plan

- Protecting Physical Infrastructure
  - Security Incidents in Q3 2022
  - U.S. midterm elections
  - Drones a major challenge

- E-ISAC Response
  - All-Points Bulletins
  - Special topic briefings and training
  - Physical Security Advisory Group
  - Quarterly and Monthly reports
  - Physical Security Resource Guide
  - Future webinars

E-ISAC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER
A DIVISION OF NERC

- Cyber Security Threats
  - Emergence of new IT and OT threats
    - Industroyer2
    - Incontroller/Pipedream
    - BadVIBE(s) Vmware
    - European wind turbine cyber events
- E-ISAC Response
  - Energy Threat Analysis Center (ETAC) Participation
  - New Cyber Security Advisory Group (CSAG)

RELIABILITY | RESILIENCE | SECURITY

- 2022 activities focused on membership expansion, outreach across the E-ISAC community, and improved information sharing
  - GridEx VI Lessons Learned Report
  - CRISP growth
  - New E-ISAC Portal
  - Vendor Affiliate Program
  - Industry Engagement Program
  - GridSecCon 2022

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

- 3% of physical security incidents shared with E-ISAC between 2020-2022, resulted in outages or other grid impacts

- Notable increase in Q3-Q4 2022 compared to baseline trends over the past 18 months

- Recent increase in ballistic damage, intrusion/tampering, vandalism

- Notable increase in repeat and clustered incidents

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

- Sharing information in a timely manner, with consent from the affected member

- Tracking incidents for further analysis

- Providing recommendations and analyst comments - enhancing lessons learned for other members
    - TLP:GREEN - Physical Security Resource Guide for Electricity Asset Owners and Operators

- When applicable, coordinating with federal, state, and local partners
    - National Counter Terrorism Center (NCTC)
    - FBI Joint Terrorism Task Force (JTTF)
    - Threat briefings
    - Member group calls

- Improve partnership with state/local law enforcement and regulators

- Encourage all entities to share data regarding physical security incidents with the E-ISAC and law enforcement

- FERC has directed NERC to conduct an assessment of physical security landscape and provide recommendations for any needed adjustments to CIP-014

- Assess protections in place against a coordinated attack (physical or cyber) and determine what next tranche of protection investments gain in risk reduction versus cost

- Attacks on Service Providers
  - Engineering firm compromise exposes industry data
  - Communications vendor compromise impacts business operations
  - Timeliness of vendor disclosures

- Ransomware
  - Exploiting legacy vulnerabilities
  - Targeting small and medium utilities

- Exposed ICS Devices on the internet
  - Devices found using Shodan
  - Guidance to identify devices issued

E-ISAC
A DIVISION OF NERC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

- Anticipated winter pro-Russia activity
  - Continued Russian physical/cyber attacks against Ukrainian energy
  - Russian military destructive and ransomware cyber activity in Poland
  - Amplified Russian disinformation around increased energy costs
  - Killnet DDoS activity
- Continued scanning and targeting by China
  - Top Common Vulnerabilities exploited by China advisory
  - Compromise of digital certificate authorities in Asia

RELIABILITY | RESILIENCE | SECURITY

- 2022 program year in review

- 14% increase in new participants year over year

- Completed CRISP — Essence Integration Pilot in December 2022

- Five Year Strategy — 2023 Milestones

- Technology update

- DOE investing in new sensor suite

- Natural gas expansion in partnership with DOE and American Gas Association

- **Purpose:** The Vendor Affiliate Program brings together security/OEM vendors and member utilities to collaborate upon vulnerabilities, risks, and mitigation best practices
- 2022 Vendor Affiliate Program Partners
  - Silver: Schweitzer Engineering Laboratories and Axio
  - Bronze: Siemens Energy, Nozomi Networks, 1898 & Co.
- U.S. Chamber of Commerce Supply Chain Working Group
- 2023 Engagement Opportunities
  - Portal Access (Read and Post)
  - Vendor Working Groups / Quarterly Meetings
  - Participation in: Monthly Briefings, IEPs, GridSecCon, GridEx

- Revenue-Based Program Model

- Revenue will be Reinvested to:
  - Self-Fund Vendor Affiliate Program
  - Offset cost of other E-ISAC programs, services, and technology

- Program Growth Plan
  - 2022 — 5 vendors
  - 2023 — 15 vendors
  - 2024 — 30 vendors

- $87,000 Total Committed Revenue

NERC, the E-ISAC, and NPCC are co-hosting the 12th annual GridSecCon in Québec City, Canada, on October 17–20

- Conference and hotel registration will open in May
- Exhibitor/Sponsorship information and Call for Abstracts coming soon
- For more information or assistance, please contact events@eisac.com

- GridEx VII will take place on November 14–16, 2023

  - Distributed Play (E-ISAC members and partners), November 14–15, 2023

    - Audience: E-ISAC members and partners, to include electricity industry, government agencies, other relevant organizations

    - Registration for GridEx VII is now open to E-ISAC members and partners with Portal access at www.register4gridex.eisac.com

  - Executive Tabletop (invitation only), November 16, 2023

    - Audience: industry and government executives from the ESCC, EGCC, and impacted entities

- Email questions to GridEx@eisac.com

Questions and Answers

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

ERO Enterprise Business Technology

Action
Update

Background

Management will provide an update on NERC's Business Continuity Program (BCP), Align, and the Security Advisory Group.

- <u>Business Continuity Program</u>: Management will review the purpose and operation of the BCP, including a description of the BCP team, inputs and influences, Regional Entity engagement, and test scenarios to exercise operation of the BCP.

- <u>Align</u>: Management will review the timeline for the final steps for completion of the Align tool, retirement of legacy applications, and the transition of Align governance to the Operations Leadership Team.

- <u>Security Advisory Group</u>: Management will provide an update on the meetings of the Security Advisory Group.

ERO Enterprise Business Technology Update

Stan Hoptroff, Vice President, Business Technology
Dee Humphries, Director, Project Management Office
Technology and Security Committee Open Meeting
February 15, 2023

RELIABILITY | RESILIENCE | SECURITY

- NERC Business Continuity Program (BCP) - Sustainability, Corporate Risk Reduction

- Align Update

- Security Advisory Group (SAG)

- Critical Skills Update

RELIABILITY | RESILIENCE | SECURITY

- BCP Plan Purpose

- BCP Team

- Inputs and Influences
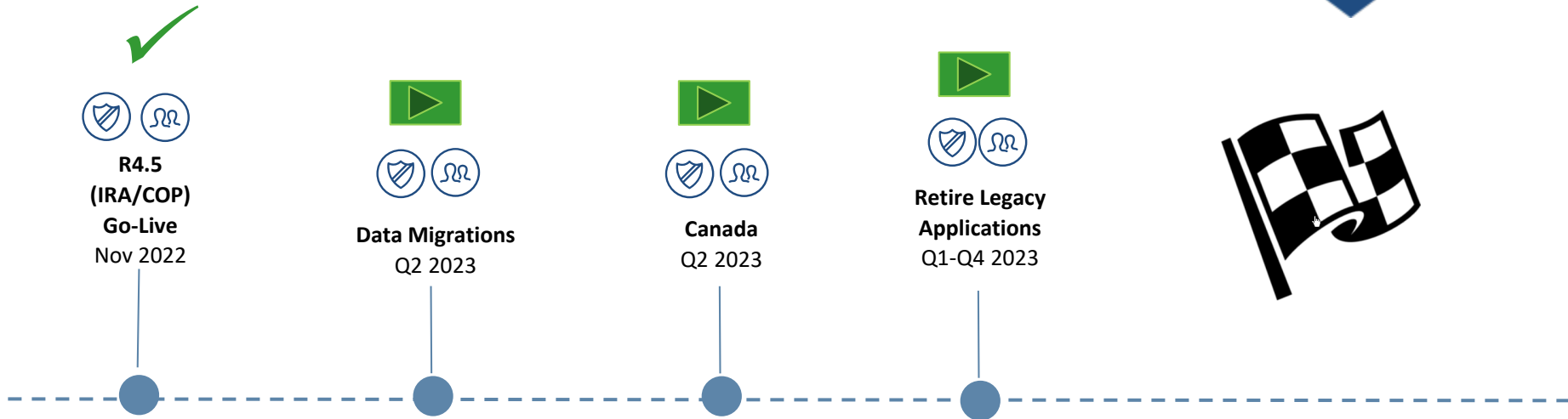
- Regional Engagement

- Scenarios

RELIABILITY | RESILIENCE | SECURITY

- Ensure organizational resilience

- Safeguard business critical operations

- Protect employees and stakeholders

RELIABILITY | RESILIENCE | SECURITY

- Dee Humphries, BCP Champion

- Stephanie Lawrence, BCP Administration

- Internal Support Team: Represented by critical business functions

- Crisis Management Team: NERC Officers and key employees

- Documentation
  - Policy
  - Department level response plans
  - Business Impact Analysis of processes and systems
  - Crisis Management contact list and resources
  - Incident Response Plan and Ransomware Framework
- Emergency Communications Approach
  - NERC Communications Team
  - Satellite phone communications technology
  - Emergency alert system – Send Word Now
- Outside Counsel and Other Experts

RELIABILITY | RESILIENCE | SECURITY

- Regional Entity CEOs invited to participate in scenarios

- Share lessons learned

- Determine ERO Enterprise BCP framework

- Definition: Tabletop exercise

- Frequency: Twice per year

- Post-tabletop reviews

- Recent scenarios

- Upcoming scenarios

R4.5 (IRA/COP) Go-Live
Nov 2022

Data Migrations
Q2 2023

Canada
Q2 2023

Retire Legacy Applications
Q1-Q4 2023

AUDIENCE IMPACT KEY

Registered Entities

ERO Enterprise Staff

In progress

Complete

"For the first time, we now have one purpose-built system that supports all of our CMEP work from end to end."

- Steve Noess, Vice President, Reliability & Security Oversight, WECC

9

- Feedback Received
  - Align easy to use and navigate
  - Additional training needed
  - Additional enhancements requested
  - ERO SEL secure but inconvenient
- December 5, 2022 Training Webinar
  - More than 400 participants
  - Questions focused on SEL and data submittal; very few on Align
- Current Activities
  - Vetting enhancements
  - Planning additional training

- **Operations Leadership Team (OLT):** Align Steering Committee will transition duties to OLT in Q2 2023, after Canada and data migrations are complete

- **Product Management Team:** Meeting quarterly; OLT approved three-year roadmap in January

- **Align User Group:** Currently engaged and meeting quarterly; determining priorities

Operations Leadership Team

Align Product Management Team

Functional Owners

IT Team

Align User Group

Business Users
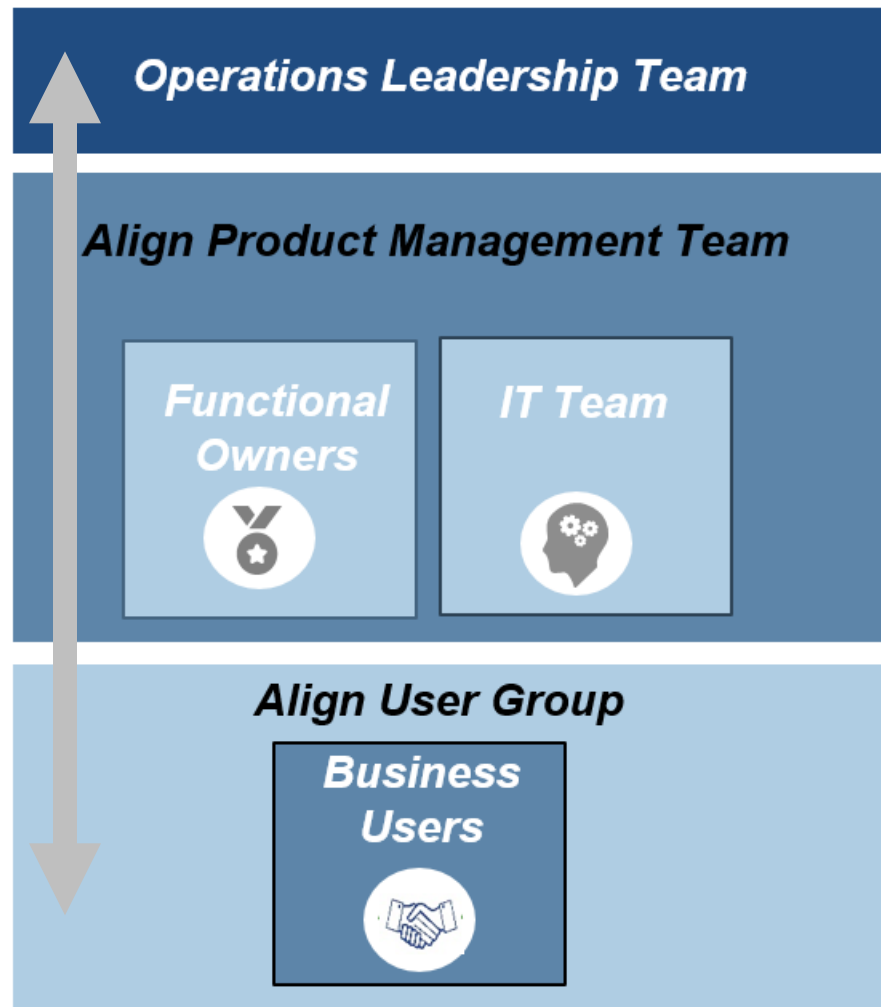
- In-person meeting
- ERO SEL Roadmap
- Additional National Institute of Standards and Technology frameworks

- **Cyber Security**
  - Quality Assurance
  - Cloud Computing
  - Analytics
- **Application Development**
  - Technology Success Support
  - Project and Vendor Management

Questions and Answers

RELIABILITY | RESILIENCE | SECURITY

Background and Reference Material

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

Annual Review of Committee Mandate

Action
Review

Background
As part of the annual review of all Board of Trustees Committee mandates, the NERC Legal Department has reviewed the current Technology and Security Committee mandate and is not recommending any revisions at this time.