A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Operations

Manny Cancel, NERC Sr. Vice President and E-ISAC CEO

Technology and Security Committee Open Meeting

February 15, 2023

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

Agenda

- 2022 Review
- Threat Briefing
- Cybersecurity Risk Information Sharing Program (CRISP)
- Vendor Affiliate Program

2022 Security Overview

- 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

2022 Security Overview

- 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

2022 Security Overview

- 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)

E-ISAC Program Highlights

- 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

Physical Security Incidents

- 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

Physical Security Incidents

- 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

Next Steps

- 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

Cyber Threats

- 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

Geopolitical Threats

- 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

CRISP

- 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

Vendor Affiliate Program

- **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

Vendor Affiliate Program

- 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

GridSecCon 2023

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

NPCC, Inc.

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

- 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

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

Agenda

- NERC Business Continuity Program (BCP) - Sustainability, Corporate Risk Reduction
- Align Update
- Security Advisory Group (SAG)
- Critical Skills Update

BCP Overview

- BCP Plan Purpose
- BCP Team
- Inputs and Influences
- Regional Engagement
- Scenarios

BCP Purpose

- Ensure organizational resilience
- Safeguard business critical operations
- Protect employees and stakeholders

BCP Team

- Dee Humphries, BCP Champion
- Stephanie Lawrence, BCP Administration
- Internal Support Team: Represented by critical business functions
- Crisis Management Team: NERC Officers and key employees

BCP: Inputs and Influences

- 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

BCP: Regional Involvement

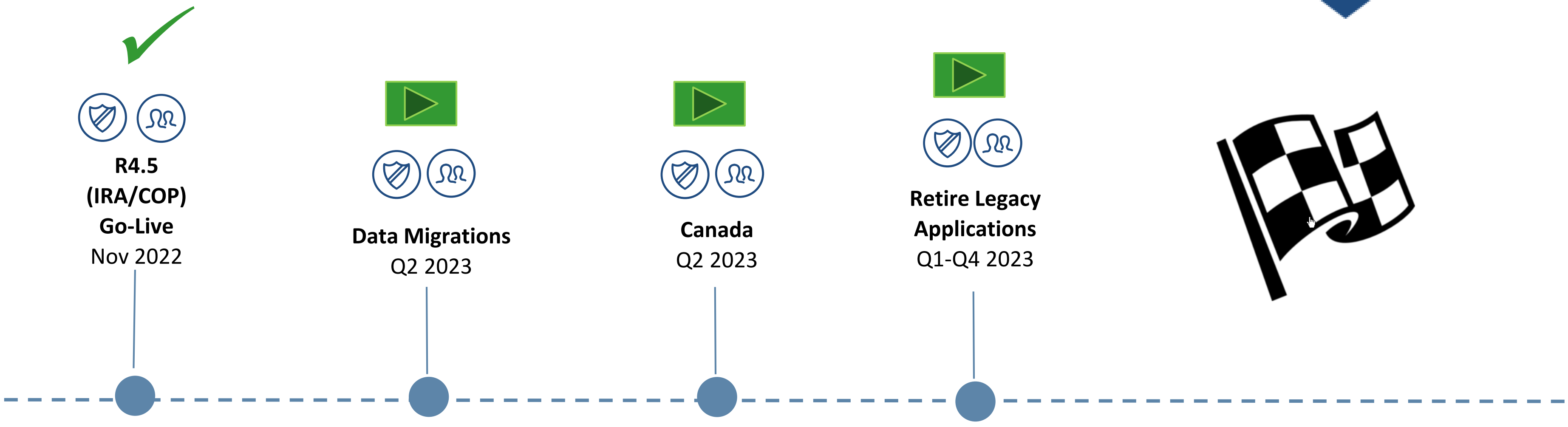
- Regional Entity CEOs invited to participate in scenarios
- Share lessons learned
- Determine ERO Enterprise BCP framework

BCP: Scenarios

- Definition: Tabletop exercise
- Frequency: Twice per year
- Post-tabletop reviews
- Recent scenarios
- Upcoming scenarios

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Align Timeline



✓ 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*

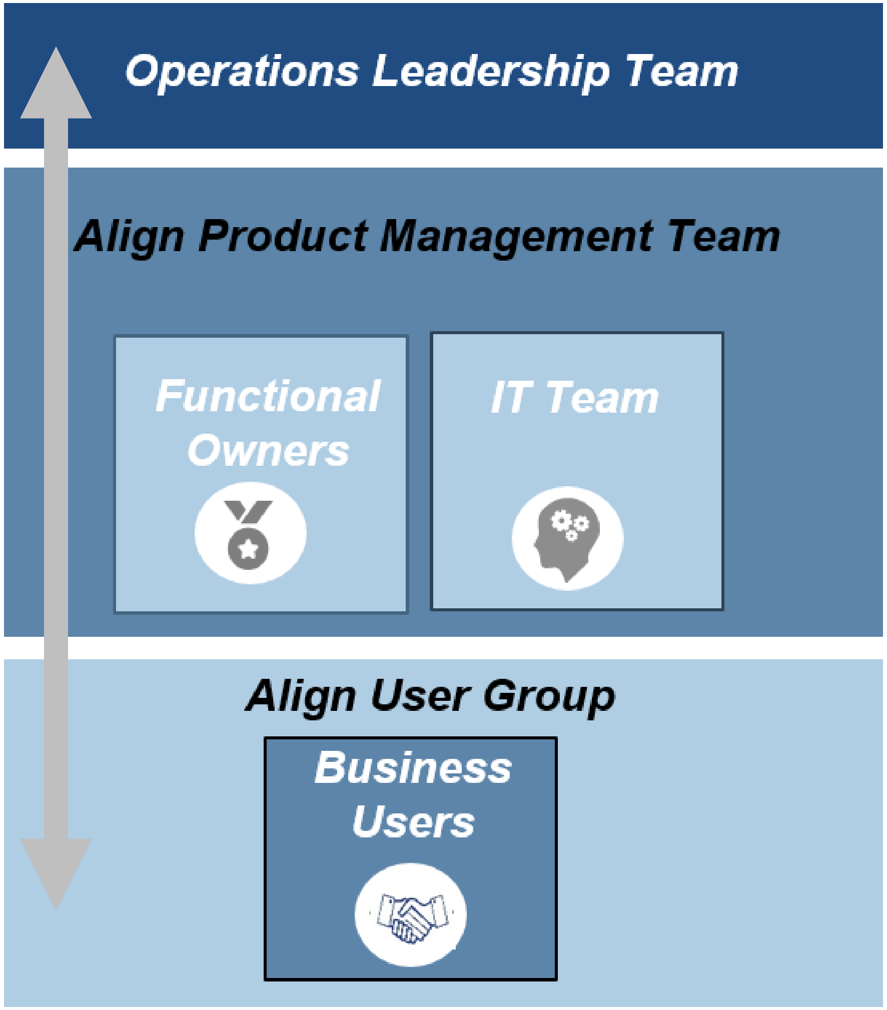
> *"For the first time, we now have one purpose-built system that supports all of our CMEP work from end to end."*
>
> - Steve Noess, Vice President, Reliability & Security Oversight, WECC

Align Update

- 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

Align Governance Transition

- **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



Security Advisory Group

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

Critical Skills

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

Questions and Answers

Background and Reference Material

Align – Benefits

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