E-ISAC Operations

Manny Cancel, Senior Vice President and CEO of the E-ISAC, NERC
Laura Brown, Director, E-ISAC Strategy, Policy, and Programs, NERC
Technology and Security Committee Open Meeting
August 17, 2022
• Collective Defense
• Membership
• Threat Landscape
• Vendor Affiliate Program
• Natural Gas Engagement
• Cross-border cooperation with Canadian industry/government (IESO, Cyber Centre, and Electricity Canada)
• Stand up of the new Energy Threat Analysis Center with U.S. Department of Energy (DOE)
• Increase Cybersecurity Risk Information Sharing Program engagement with partners (Cyber Centre, other ISACs, IESO, DOE, DHS)
• Engage through the Electricity Subsector Coordinating Council
• Canadian Organizations
  ▪ 58 member and 10 partners
  ▪ 31 out of 42 Electricity Canada members

• Member Additions
  ▪ Over 100 new organizations and 1,110 new users joined the E-ISAC community in Q1-2 2022

• Industry Engagement Program
  ▪ Tailored to specific stakeholder groups including Canadian membership
• Russian cyber threat actors are exploring options for potential counterattacks against critical infrastructure

• Preparedness Guidance:
  ▪ Cyber Centre – Guidance for Heightened Threat Environments
  ▪ Joint U.S. and Canadian Alert on weak security controls and practices routinely exploited for initial access
  ▪ E-ISAC ICS ‘SHIELDSD- UP’ for electricity released
  ▪ E-ISAC Geopolitical Preparedness Guide
• Microsoft - "Defending Ukraine: Early Lessons from the Cyber War"

  ▪ Increased Russian network penetration and espionage against Allies
  ▪ Russian agencies conducting global cyber influence operations
  ▪ Need for collective defense
  ▪ Disburse and distribute digital operations/assets
  ▪ Cyber Threat Intelligence and end-point protection
Recent Russian network penetration and cyber espionage operations outside Ukraine

Russian network intrusion targets

- Government agencies: 49%
- IT sector enterprises: 20%
- Critical infrastructure organizations: 19%
- NGOs: 12%

- Russian network intrusions: 128
- Countries: 42
- Success rate: 29%

In most instances the victims were operating on premises, not in the cloud.

Source: Microsoft, “Defending Ukraine: Early Lessons from the Cyber War”
• **Current activities**
  - Dragos threat hunting and intelligence support
  - Industrial Control Systems (ICS) Security Bulletins
  - Use of Neighborhood Keeper
  - Coordination with DOE ETAC on specific OT threats

• **Planned activities**
  - Acquiring additional resources with ICS operations and security experience
  - NRECA Essence and CRISP Integration
  - Long-term: integrating CRISP and OT feeds
Future Opportunities

- Enhancing sharing operational and security information with government
- Enhancing security coordination between electricity and gas
- Developing legislation that provides incentives to collaborate to improve cyber security for critical infrastructure
- Establishing E-ISAC Vendor Affiliate Program
- Enhancing OT threat response capabilities
Questions and Answers
Vendor Affiliate Program
Utilities Face New Challenges
Managing Third Party Risk

- Increasing complexities and risk in reliance on supply chain software components
- Vendors who supply and manage products and software to industry are getting more engaged to address real world vulnerabilities impacting electricity
- Modeled on best practices and vendor programs across other critical infrastructure sectors
Introducing the E-ISAC Vendor Affiliate Program

- Fee-for-service program introduces a new membership model
- Three levels of membership
  - Bronze Level ($10,000 / year)
  - Silver Level ($25,000 / year)
  - Gold Level ($40,000 / year)
- Focus on facilitating thought leadership and timely information sharing; no business development allowed
- 2022 “soft launch” with incremental implementation over three years
Vendor Affiliate Program
Membership Benefits

**Bronze**
- 5 Portal user accounts
- Promote one event on Portal calendar
- GSC networking session
- Partnership and brand awareness

**Silver**
- 15 Portal user accounts
- Present on one webinar
- Promote two events on Portal calendar
- GSC networking session
- Participate in IEP session
- Partnership and brand awareness

**Gold**
- Unlimited Portal user accounts
- Present on two webinars
- Promote four events on Portal calendar
- GSC networking session
- GSC panel or training
- Invitation to IEP session
- Partnership and brand awareness
Onboarding Plan and Cost Analysis Through 2024

- 2022 – 5 vendors
- 2023 – 20 vendors
- 2024 – 30 vendors
  - 1 additional FTE to support vendor program growth
Next Steps

- **Finalize Program**
  - Identify soft launch participants
  - Finalize marketing content
  - Notify FERC about new cost-model and anticipated revenue

- **Soft Launch (July–August)**
  - Onboard initial set of five (5) vendors for 2022–2023, pro-rated $$
  - Outreach to existing vendors and other interested parties

- **Full Launch (September–December)**
  - Extend outreach for 2023 participants

- **Contact** [Bluma.Sussman@eisac.com](mailto:Bluma.Sussman@eisac.com)
Questions and Answers
Natural Gas Engagement
• Real world cyber attacks and weather-related events are becoming more frequent

• These challenges highlight the need for greater alignment and coordination

• Natural gas and gas pipeline companies will increase resilience through CRISP and E-ISAC membership; access to cyber and physical threat information and analysis

Natural Gas Consumption by Sector (2021)

Source: www.eia.gov
Strategy: Expand Stakeholder Community to Reduce Risk

• Expand CRISP/E-ISAC Membership
  - 100+ combo companies are E-ISAC members
    o Expand E-ISAC membership by 10% by EOY
  - Build off Natural Gas/Electric combo utilities who are already CRISP members

• Membership Benefits
  - Access to secure CRISP data, workshops, private, member-only chat channels
  - Access to secure E-ISAC Portal information and analysis on physical and cyber threats
  - Participation in monthly briefings, IEPs, GSC, and webinars
  - Access to government partners and industry vendors
Industry Alignment and Input

- Early engagement with industry stakeholders and trade associations
- Input from gas/gas combo utilities
- Coordination with partners
- Collaboration across NERC and E-ISAC
Ongoing

Information sharing
Analyst-to-analyst exchange
Joint products
Membership growth

Q3
Socialize plan
Develop communications
Ready Portal and onboarding materials

Q4
Internal communications rollout
CRISP outreach
Establish regular coordination with trades
Questions and Answers
ERD Enterprise Business Technology Scope and Focus 2023-2025

Stan Hoptroff, Vice President, Business Technology Technology and Security Committee Open Meeting August 17, 2022
• Critical IT Investments
• Critical Skills to Be Acquired and Retained
• NERC and ERO Application Roadmap
• Align Release 4.0 and Release 4.5
• Align Governance
• NERC Business Technology Success Team – Spotlight
• Security Advisory Group (SAG)
Critical IT Investments

• Ensure the protection of our platforms and applications
• Provide foundational infrastructure to support the ERO Enterprise
• Build and provide applications that enable our core mission
Critical Skills

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

• Cyber Security
• Platforms
• Application Development and Enhancements
• Acceleration of Cloud Computing
• Foundational Infrastructure and Specialized Infrastructure
• NERC Alerts Upgrade
• Generating Availability Data System (GADS) Wind Submission Site Retirement
• GADS Solar
• Reliability Coordinator Information System Replacement
• Enterprise Data Analytics Center
• Identity and Access Governance
• Security Operations Enhancements
• Bulk Electric System Performance Risk Analysis
• Reliability Assessment Data System
• Resource Adequacy Upgrade
• Corporate Risk Management
• NERC Public Site
• Perimeter Protection Enhancements
• NERC Application Platform upgrade (xRM)
• Master Data Management
• Inadvertent Upgrade
• Central Repository of Curtailments Upgrade
• Automated Testing Framework
• Secure Evidence Locker (SEL) Refresh
• Cloud Security Enhancements
Align Timeline

**AUDIENCE IMPACT KEY**
- Registered Entities
- ERO Enterprise Staff

**In progress**
- R4.5 (IRA/COP) UAT Go-Live September 2022

**Complete**
- R4.0 (Scheduling and Audit) Go-Live June 22, 2022
- R4.5 (IRA/COP) UAT Jul-Aug 2022
- R4.5 Training & Adoption Aug-Oct 2022
- Data Migrations Dec 2022

**Begin Retiring Legacy Applications Dec 2022**

--R4.5 Go Live moved from October to September (soft launch); date is dependent on performance testing results
**Operations Leadership Team:**
NERC and ERO Enterprise leadership;
Provides vision and executive oversight

**Product Management Team:**
Comprised of NERC and Regional compliance and
enforcement leadership, and NERC IT;
Determines business needs for Align and ERO SEL;
defines and supports project scope and delivery

**Align User Group**
Represents Region and registered entity end users of
Align and ERO SEL; provides input into functionality
and business needs; supports project delivery through
requirements definition and user acceptance testing
The Business Technology Success All-Star Team

ERO Enterprise

2022
ATL

Jeremy Bryant
2022
ATL

Travis Heyward

2022
DC

Maria De Souza

2022
DC

Ravee Broker
• PCs and peripherals (monitors, docks, etc.)
• Mobile devices (iPhones, iPads)
• Employee and Contractor On-boarding and Off-boarding
• Meeting Support
• Special Projects
• NERC Desktop Support
• ERO Enterprise Account Support
• ERO Enterprise Application Support
Support Tickets - Overall Trends

**Increasing Ticket Volumes per Week**

The Pandemic increased demand for NERC support; Align increased demand for ERO Enterprise Support.
General Categories of Tickets by Quarter

As technologies change and grow, so does the amount of support needed.
Support Tickets - Overall Trends

**Priorities of Tickets by Quarter**

*Tickets are not becoming more critical… there are just more of them.*
Business Technology Success “Sharpening the Saw”

Improved Data Collection, Triage, and Prioritization

User Friendly Look and Feel
Business Technology Success
Supporting the ERO Enterprise
• SAG is comprised of security leadership from the industry for advisement of key NERC Security Initiatives
• Engaged in annual review of SEL
• Will engage on advisement of security plans
Questions and Answers
Background and Reference Material
**Enterprise Solutions**

- Compliance, Enforcement and Mitigation: Align
- Secure Evidence Locker: SEL
- Generation Analysis: E-GAR
- Reliability Coordinator Information: RCIS
- Wind Generation Availability: GADS Wind
- Geo-magnetic Disturbances: GMD
- Centralized Organizational Registration: CORES
- Resource Adequacy: RA
- Standards Balloting System: SBS
- Bulk Electric Network Exception Tracking: BESNet
- Coordinated Functional Registration: CFR
Enterprise Solutions

- Misoperations Data System
- Event Analysis Management
- User Management and Records
- External Collaboration
- Phasor Measurement Unit
- ERO Registered Entity Portal
- Joint Registration Organization
- Curtailment Events
- Grid Security Technology
- NERC Membership
- ERO Training Portal

MIDAS
TEAMS
UMR
Extranet
PMU
ER0 Portal
JRO
CRC
GST
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
Align Release 4 and 4.5: What to Expect

Stakeholder Group

Registered Entities

Release 4 Functionality

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