A DIVISION OF NERC

E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Update

Threat Landscape and Programmatic Update

Matthew Duncan, Director, Intelligence, E-ISAC
NERC Technology and Security Committee Open Session
August 11, 2021

Agenda

- Threat Landscape
- CRISP Update
- DOE 100 Day Plan
- 24x7 Watch Update

Threat Landscape – Supply Chain Compromise

- Russian and other adversaries remain active
  - SolarWinds
  - Microsoft Exchange Server
  - Pulse Connect Secure
  - Kaseya
- FERC-E-ISAC White Paper on SolarWinds Supply Chain Compromise
  - Consider system risk-based approach for protecting most critical assets
  - Baseline critical access and administrative privileges
  - Exercise response plans with third-party vendors, partners and government
  - Conduct security assessments or penetration tests to ensure baseline
  - Increase timeliness of voluntary reporting and mandatory CIP-008 reports

Threat Landscape – Ransomware and DDOS

- Ransomware
  - Ransomware criminals targeting critical infrastructure
  - Colonial Pipeline (DarkSide), JBS (REvil), and Kaseya compromises (REvil)
  - Compromises exploit trusted-third party vendors
  - Law enforcement and government partners should be notified and engaged ASAP
- Denial-of-Service (DoS) Attempts
  - Ongoing DoS activity in critical infrastructure sectors
  - No outages or reported threats to reliability
  - DoS mitigation services should be enabled with Internet Service Providers

Threat Landscape – Physical Security

- Drone analysis “Project Flyover”
  - Overlay drone activity on electricity asset information and analyze for significant trends
- Domestic violent extremist groups targeting critical infrastructure
- Ongoing indiscriminate damage to distribution assets
- Increase in copper and precious metals theft

CRISP Update

- CRISP Survey Results
  - Survey respondents were satisfied with E-ISAC's management of CRISP (**94%**)
  - **94%** of respondents have benefited from CRISP, with **76%** of the respondents stating that their organization has taken action because of CRISP
- CRISP OT Dragos Pilot underway
  - Installation and access completed
  - Training and analysis/paired hunting underway
- CRISP Essence Integration Pilot
  - Seven CRISP participants to receive Essence and three Essence participations to receive CRISP
  - Technology can be used by cybersecurity and operating engineers to protect IT/OT systems against unknown, emerging threats

DOE 100 Day Plan – Update

- Establish greater ICS visibility in electricity subsector
- E-ISAC will have access to data distribute information to all members
- E-ISAC analysts currently undergoing intensive training on Dragos Neighborhood Keeper and NRECA Essence platforms
- NERC Practice Guide issued

DRAGOS
NEIGHBORHOOD KEEPER
Collective Defense for Industrial Cybersecurity

ESSENCE 2.0
Integrated Cyber/OT Protection
Defending America's Energy Supply
NRECA
America's Electric Cooperatives

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP

GIAC RESPONSE AND INDUSTRIAL DEFENSE
GRID

24x7 Watch Operations – One Year Later

- E-ISAC 24x7 Watch Operations activated in March 2020 and officially established in July 2020
- Staffed by 11 FTEs and supported by other E-ISAC groups
- 150% increase in production
- Proactive outreach to members and partners
  - Industrial Control Systems notification
  - Ransomware Group alerts
  - Government and Membership engagement and information sharing
  - Cross-sector ISAC coordination
  - Cyber Crime Forum monitoring

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Marvin Santerfeit, Director IT Solutions and Support

Technology and Security Committee Meeting
August 11, 2021

RELIABILITY | RESILIENCE | SECURITY

Agenda

- NERC IT Infrastructure Update
- Disaster Recovery Update
- NERC IT Infrastructure Future Priorities

Infrastructure Update

- Multi-Factor Authentication (MFA) for infrastructure support accounts
- MFA for Human Resources Applications to enhance security
- MFA for Concur (Expense reporting/invoice approval) application to enhance security
- Refreshed 66 leased laptops (50 more planned 2021) to avoid end of life failures
- Email encryption upgrade and enhancements for outbound external emails
- Enhanced Client Support Ticketing system for stakeholders – enabled text alerting capability for critical tickets.

Disaster Recovery Update

- Disaster Recovery IT Run Book focused on restoration of critical data and applications in the event of a catastrophic event
- Renewed focus on backups, and more importantly recovery capabilities
- Upgraded backup tape library to reduce restoration times
- Monthly tracking of backup and recovery metrics; currently tracking at 97% completion with 3% requiring manual intervention

Infrastructure Looking Ahead

- Continue to strengthen our software patching capabilities (e.g., fully automate server patching)
- Implement additional email authentication protections
- Retire Skype messaging environment (remove 8 severs)
- NERC Employee Self-Service IT equipment portal for commodities
- Complete dashboard for Top-10 IT operational metrics

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Align Project Update

Stan Hoptroff, Vice President, Business Technology
LaCreacia Smith, Senior PMO Manager, ERO PMO
Technology and Security Committee Meeting
August 11, 2021

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Align – Benefits
- Canadian Update
- Registered Entity Perspective – Release 1
- Align Project Timeline
- Release 3 and Release 4 Functionality
- Current Challenges
- How to Stay Informed

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** & 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

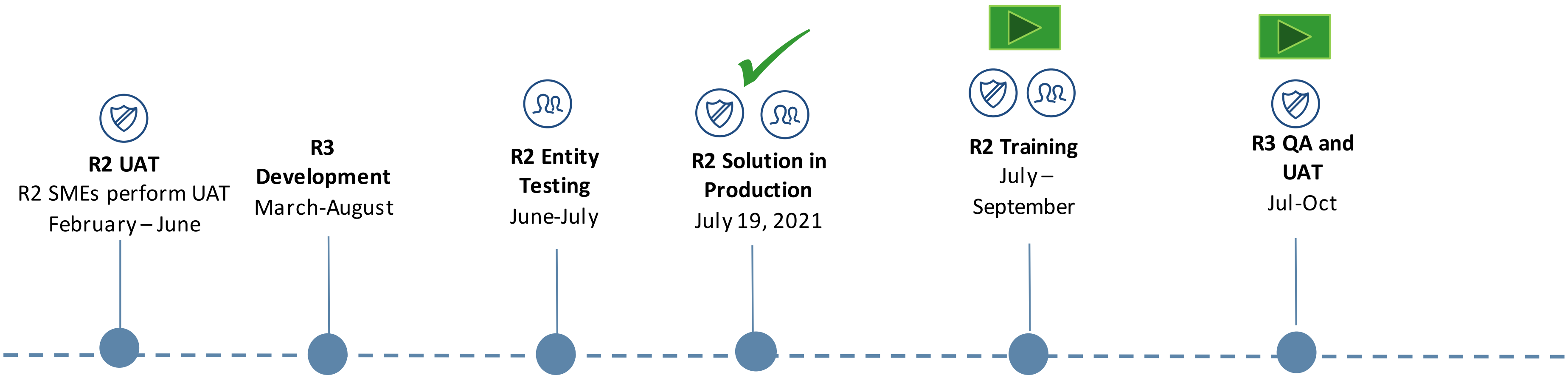
Canadian Update

- Release 1 – Ontario went live on 5/24/21
- Provinces that will adopt Align include:
  - Alberta
  - British Columbia
  - Manitoba
  - Nova Scotia
  - Saskatchewan

Registered Entity Perspective – R1

- Positives shared from the Release 1 Rollout
  - Announcements and training opportunities
  - Training was important and well done
  - First impressions with Self-log submittals were positive
  - Overall, the system is easy to use and navigate
- Areas for Improvement
  - In some cases, windows for training were very tight
  - A template for required fields would be helpful
  - Closed help desk tickets without resolution

Align Timeline



R2 UAT
R2 SMEs perform UAT
February – June

R3 Development
March-August

R2 Entity Testing
June-July

✓ **R2 Solution in Production**
July 19, 2021

▶ **R2 Training**
July – September

▶ **R3 QA and UAT**
Jul-Oct

- *Release 2 go live by Region/feature*
- *Release 3 adoption plan will be determined in Q4*
- *Release 4 go live to be announced after R3 go live*

AUDIENCE IMPACT KEY

Registered Entities

ERO Enterprise Staff

▶ *In progress*

✓ *Complete*

Release 2 Regional Go-Live Dates

Region	TFE	PDS	Self Certs
MRO	✓	10/1	10/1
NPCC	✓	10/1	10/1
RF	✓	10/1	10/1
SERC	✓	10/1	10/1
TRE	✓	✓	✓
WECC	✓	✓	9/1

Align Release 3 & 4 Functionality

- **Release 3:** Audit, Spot Check, Investigations, and Scheduling
- **Release 4:** Audit and Scheduling Enhancements, Complaints, Inherent Risk Assessment (IRA), and Compliance Oversight Plan (COP)

Challenges

- **Resources:** Parallel efforts (R2 training/rollout, R3 development)
- **Adoption:** Stakeholder, Regions and NERC's ability to absorb changes
- **Security vs Usability:** Multiple steps to keep data secure
- **Technical:** Migrating open records from and decommissioning legacy systems
- **Project Fatigue:** Maintaining team and stakeholder engagement
- **Cost Management:** Balancing available funds and enhancement requests

How To 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
- NERC News
- Social media

Questions and Answers

Background and Reference Material

Align Release 1: What We Delivered

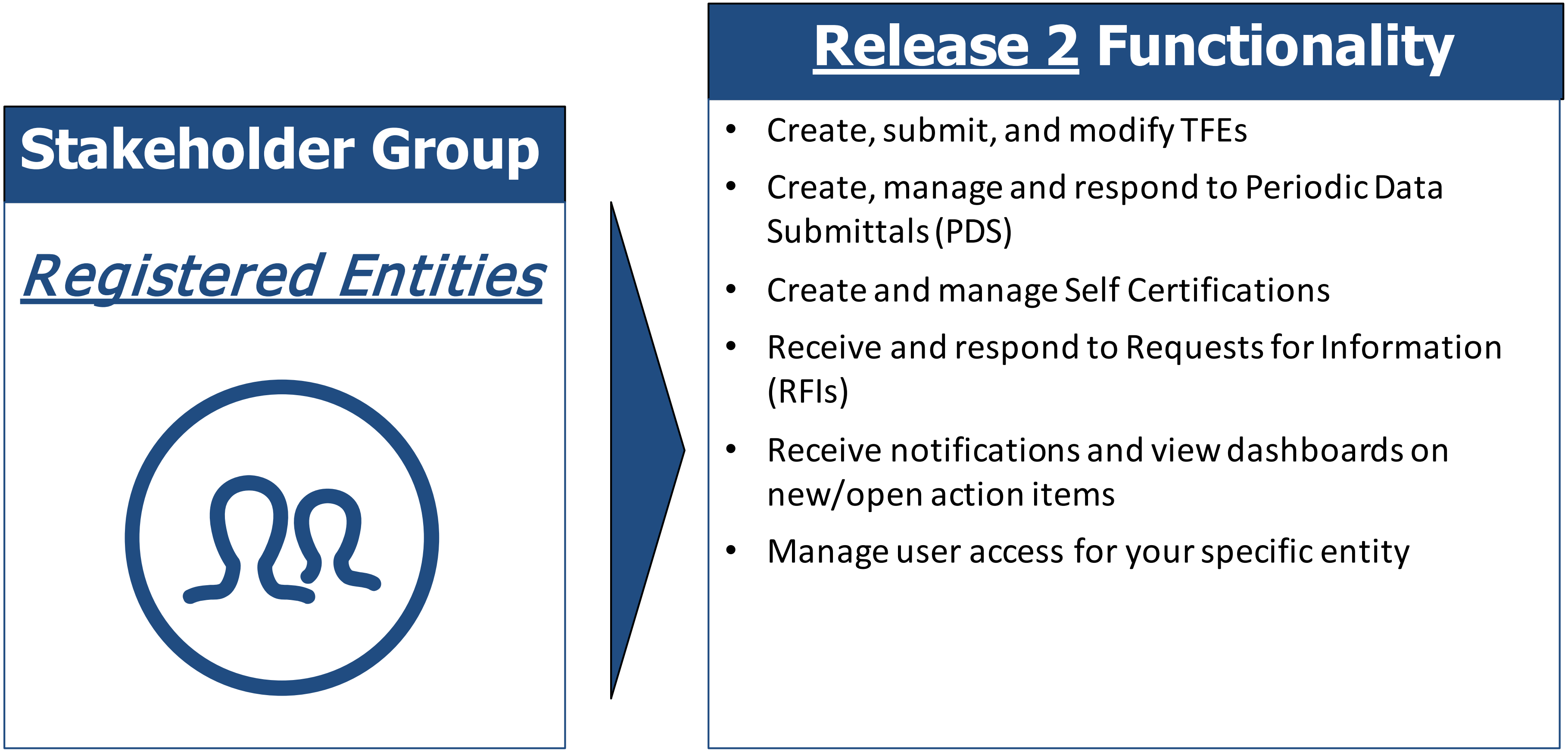
Stakeholder Group

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 NERC Standards and Requirements applicable to your entity
- Manage user access for your specific entity

Align Release 2: What We Delivered



Stakeholder Group

Registered Entities

Release 2 Functionality

- Create, submit, and modify TFEs
- Create, manage and respond to Periodic Data Submittals (PDS)
- Create and manage Self Certifications
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Manage user access for your specific entity

Align Release 3: What to Expect As a Registered 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
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Manage user access for your specific entity

Align Release 4: What to Expect As a Registered Entity

Stakeholder Group

Registered Entities

Release 4 Functionality

- Enhanced Audit and Scheduling functionalities
- Compliance Planning (Inherent Risk Assessment (IRA), Internal Controls Evaluation, and Compliance Oversight Plan (COP))
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Manage user access for your specific entity