A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Update

Manny Cancel, CEO E-ISAC

Technology and Security Committee Meeting

May 12, 2021

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Director of National Intelligence (DNI) Annual Threat Assessment
- Microsoft Vulnerabilities Report
- Department of Energy (DOE) 100 Day Plan
- Threat Landscape
- Strategic Partnerships and Industry Coordination
- Portal Upgrade
- Events
- Feedback Survey

DNI Annual Threat Assessment

- China, Russia, Iran and North Korea possess capability to disrupt critical infrastructure
- Terrorist organizations continue to plot attacks
- COVID-19 will continue to strain governments and societies, fuel crises, political unrest, and geopolitical competition
- Ecological degradation and climate change will continue to fuel disease outbreaks, threaten food and water supply, and exacerbate political instability
- Organized crime will continue to take its toll
- Emerging and disruptive technologies will continue to pose unique challenges

Microsoft Vulnerabilities Report

- Unpatched vulnerabilities are the cause of 1 in 3 breaches
- 48% increase in vulnerabilities in 2020
- Vulnerabilities facilitated elevation of privilege and ransomware
- Most vulnerabilities would have been mitigated by removal of administrative privileges
- Password and endpoint management
- Secure remote access

DOE 100 Day Plan

- Establish near real time situational awareness, indications, warnings, and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks across electricity subsector
- High-impact activities executable within 100 days
  - Focus on networks that touch the largest number of Americans' lives or that significantly impact homeland and national security
  - Enhance the integrity and security of priority sites' control systems by installing technologies and systems to provide visibility and detection of threats

Threat Landscape
Supply Chain Compromise

- US Government officially attributes to Russian Federation
- New malware variants detected and tools released
- No impact to reliability of bulk power system
- E-ISAC/ESCC Tiger Teams continue to monitor situation
- Guidance
  - Keep operating system and enterprise software patches and maintain awareness of latest threats
  - Disable sharing services or if services are required, use complex passwords or Active Directory authentication
  - Restrict permission to install and run unwanted software applications and administrators only when required
  - Configure firewalls to deny unsolicited connection requests

Threat Landscape
Microsoft Exchange Vulnerabilities

- Initial disclosure focused on HAFNIUM exploitation of four Zero-Day vulnerabilities for on-premise exchange environments
- USG required patches to be applied ASAP (CISA ED 21-02)
  - E-ISAC issued APB, and NERC issued a Level 1 Alert
- Microsoft disclosed four additional vulnerabilities for Exchange
  - Two of the vulnerabilities focused on pre-authentication, no login required
  - No known active exploitation at time of disclosure

Threat Landscape Other Vulnerabilites

- F5 BIG-IP
- Pulse Connect Secure and Codecov breaches
- Ransomware variants: REvil/Sodinokibi, CLOP, DoppelPaymer, Nefilim shares

Threat Landscape Physical Security

- Continuing Threats/Risks
  - 43% increase in number of members voluntarily sharing information
    - Domestic Violent Extremist Groups
    - Civil Unrest and Activism
    - Emerging Technology (drones)
    - Theft
- Update on New Products/Existing Efforts
  - New Drone Flightpath Analysis Pilot
  - Physical Security Year in Review: 2020
  - New analytical products

Strategic Partnerships and Industry Coordination

- Electricity Subsector Coordinating Council (ESCC)
- National Infrastructure Advisory Council and Cyber Solarium Coordination / DOE 100 Day Initiative
- IESO
- U.S. Government Partners
- Cross-Sector ISACs
- Analysis and Resilience Center (ARC)
- IronNet

Portal Upgrade

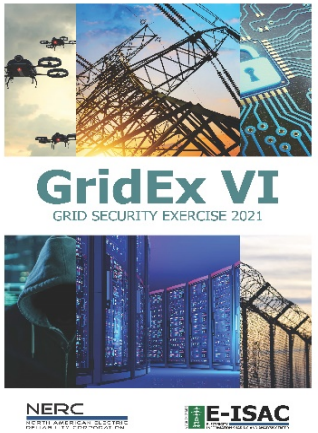
- Portal re-platform — targeted for July 2021
  - Increased security
  - Self-service and improved usability

Events

- GridSecCon 2021 will take place virtually
  - October 18 — Training Opportunities
  - October 19-20 — Keynotes, Breakout Sessions, Panels

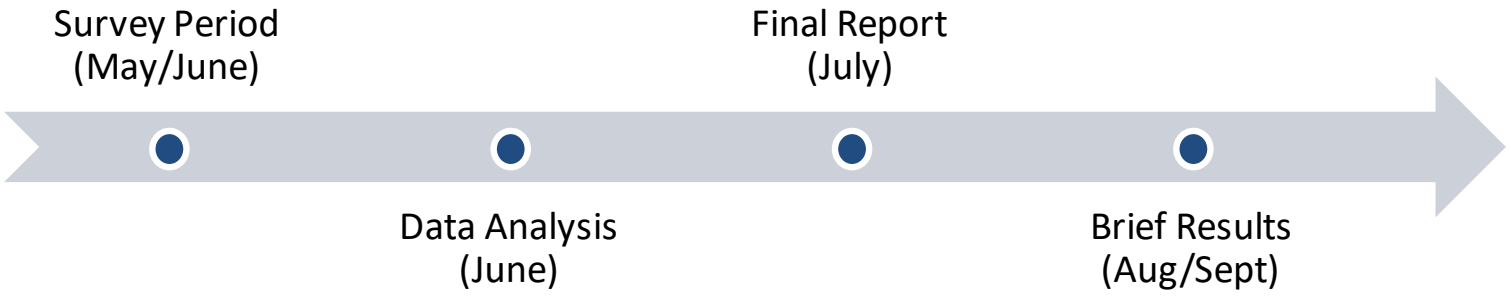
GRIDSECCON 2021
NERC • E-ISAC • TEXAS RE

- Grid Ex VI
  - Distributed Play – November 16-17
  - Executive Tabletop – November 18
    - Will be conducted in hybrid mode



Stakeholder Feedback Surveys

- JD Power Stakeholder Feedback Surveys
  - Members (AOOs, MSP, Balancing Authority, RTO/ISO)
  - Partners (Gov't, Cross-Sector, Trade Associations, Nat'l Labs)
  - Gather feedback on stakeholder experience, products, and services
  - Identify best practices and areas for improvement



- Additional sources of feedback
  - Surveys (CRISP, Physical Security Advisory Group)
  - Programs (Industry Engagement Program)

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Align Project Update

Stan Hoptroff, Vice President, Business Technology
Andy Rodriquez, Director, Business Technology
Technology and Security Committee Meeting
May 12, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

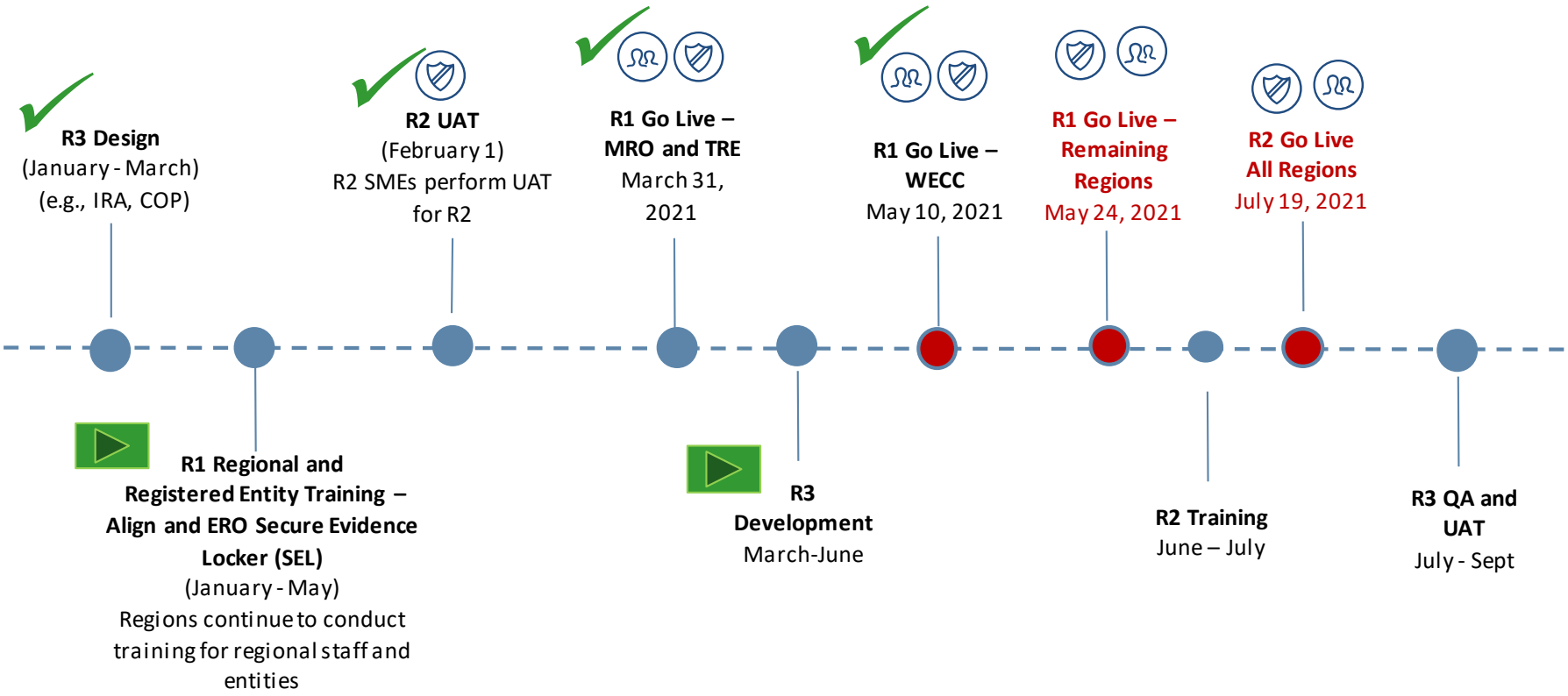
- Align Benefits
- Align Timeline
- Release 2 Functionality
- Release 3 Functionality
- Challenges
- How to Stay Informed

Align - Benefits

Moving to a common platform will provide:

- **More secure** method of managing and storing Compliance Monitoring and Enforcement Program (CMEP) data
- Alignment of **common** and 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

Align Timeline (As of May 1, 2021)



AUDIENCE IMPACT KEY

Registered Entities | ERO Enterprise Staff

In progress

Complete

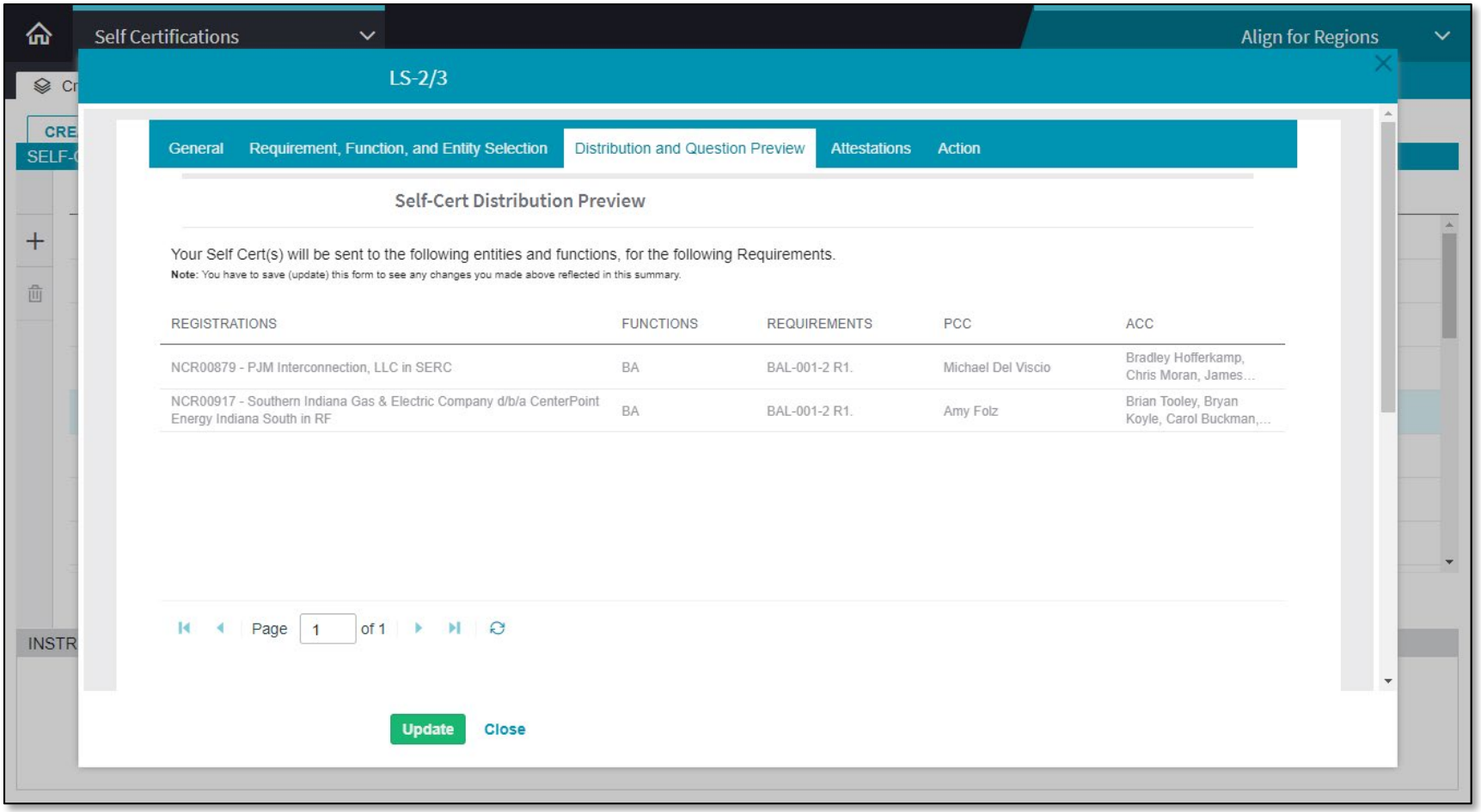
Release 2
Periodic Data Submittals (PDSs), Technical Feasibility Exceptions (TFEs), Self- Certifications

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

R2: Self-Certifications, PDSs, and TFE Process Improvements

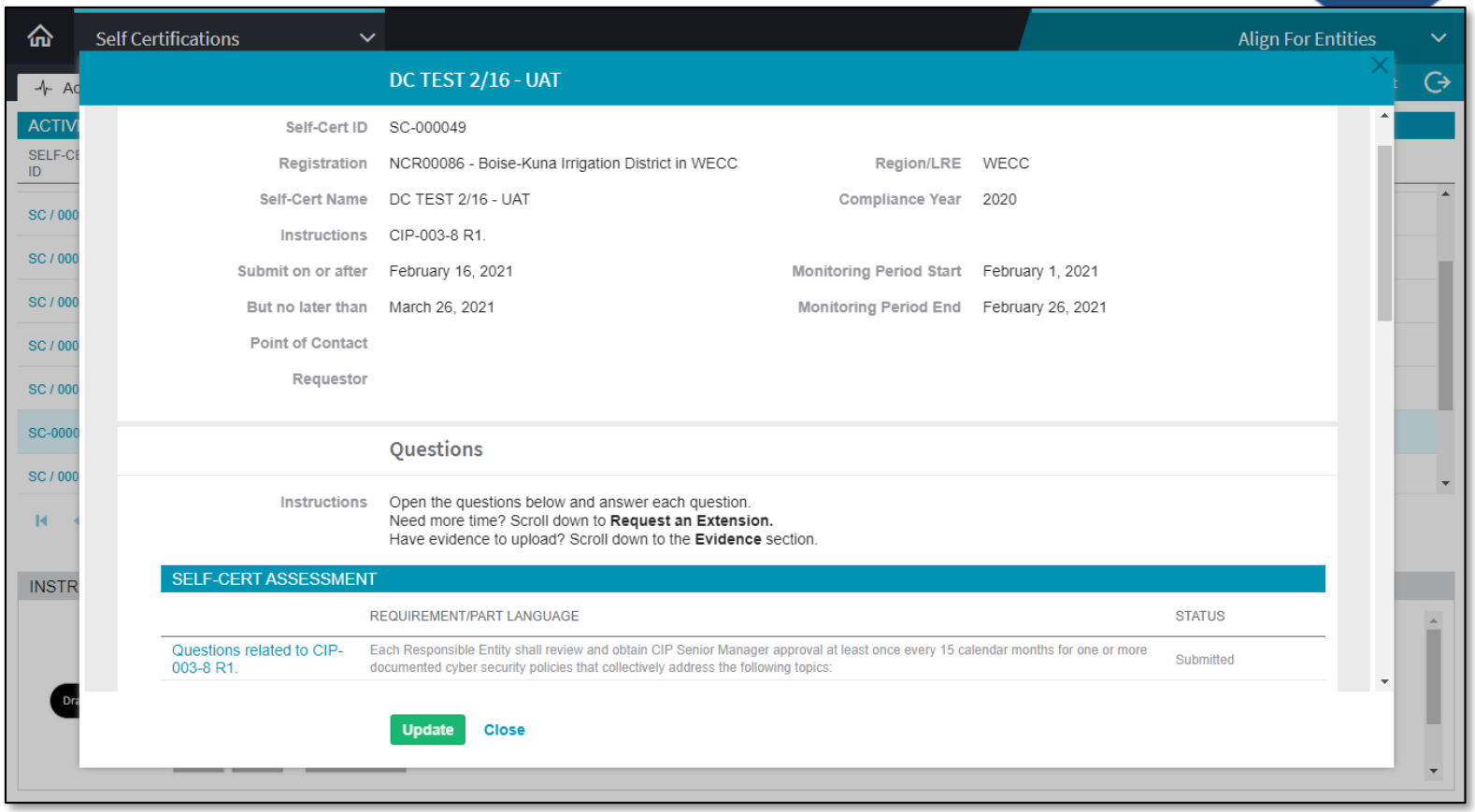
Topic	Current State	Future State
Self-Certifications	• Regions make use of both "traditional" and "guided" self-certifications; application of each and tools used varies by region • Rules of Procedure (ROP) language is based on "traditional" self-certifications • Self-certification forms vary in content and functionality	• Establish a single self-certification process, removing the distinction between "guided" and "traditional" self-certifications; Regions will have the flexibility to ask clarifying questions and request evidence at time of submission and anytime during the process • Explore opportunity to clean up ROP language to better reflect current processes • Self-certifications will be sent to registered entities as a common form containing applicable standards and requirements as defined by the CEA
Periodic Data Submittals (PDSs)	• PDSs for standards on the national schedule are submitted through a variety of tools • Variety of templates used for PDSs • Do not have a method for tracking a "no" or "not applicable" response to PDS as data, which causes extra work for entities and Regions (creating, submitting, and reviewing blank spreadsheets/templates) • No functionality to account for Multi-Region Registered Entity Coordinated Oversight	• Day 1 implementation will focus on standards where data is currently being submitted in CITS/CDMS; additional standards may be rolled into BWise in the future • PDS response templates will be standardized where feasible; to be explored further in design • Create ability for entities to report "no" or "not applicable" so that it is easily visible/reportable, and can be tracked for future PDS requests to avoid duplicate requests to entities • CEAs will be able to send a PDS to all entities for which they are the Lead Region
Technical Feasibility Exceptions (TFEs)	• Significant time and effort required to create reports for NERC and FERC • Volume of TFEs continues to reduce over time due to revisions to standards	• A single standardized form to facilitate easier NERC and FERC reporting • Continue discussions with Steering Committee on future of TFE program and approach to implementation

Self-Certifications



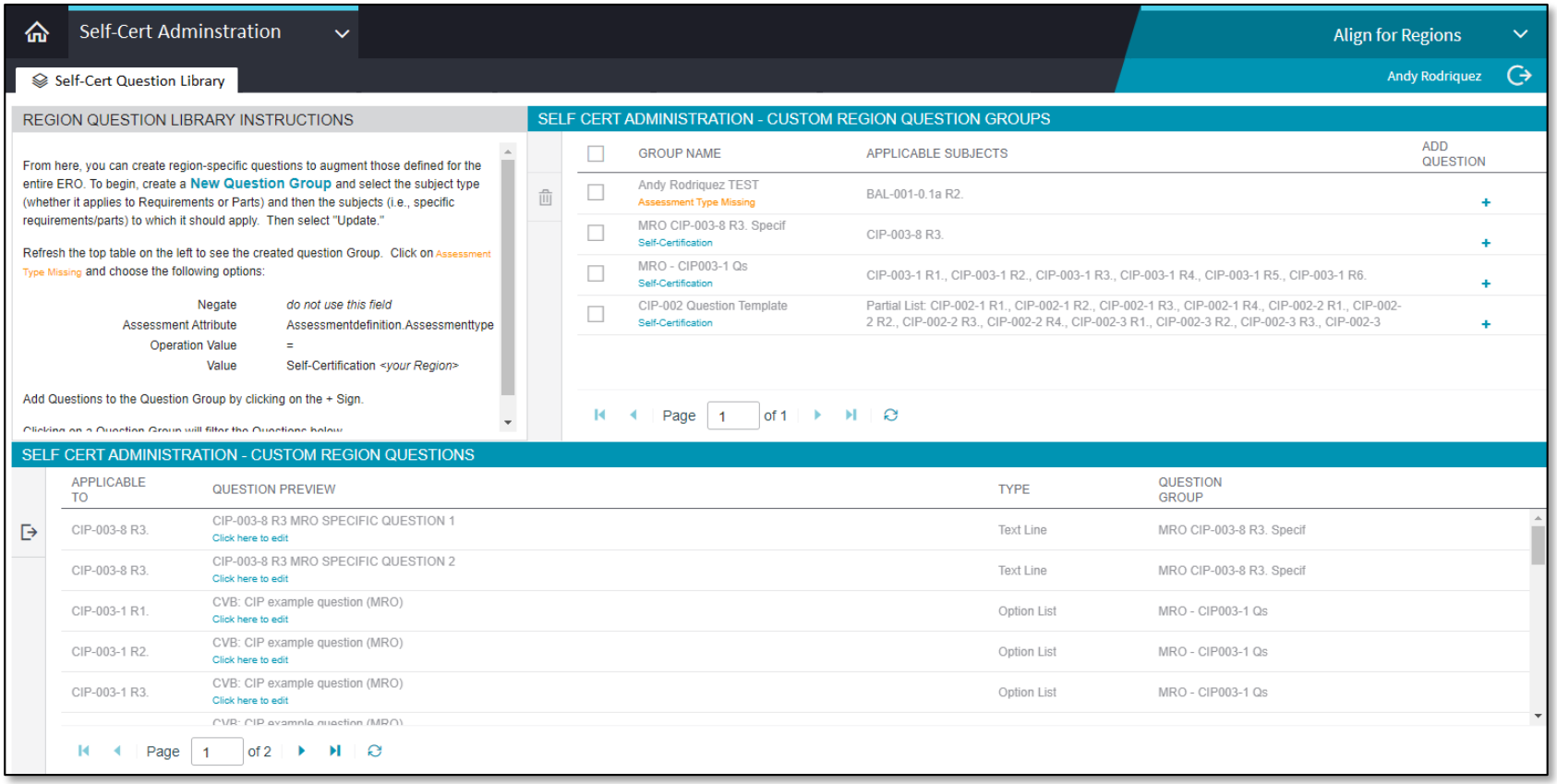
- Regional Entities create bulk-distributions of Self-Certifications based on function, entity, requirement, or any combination of the three

Self-Certifications



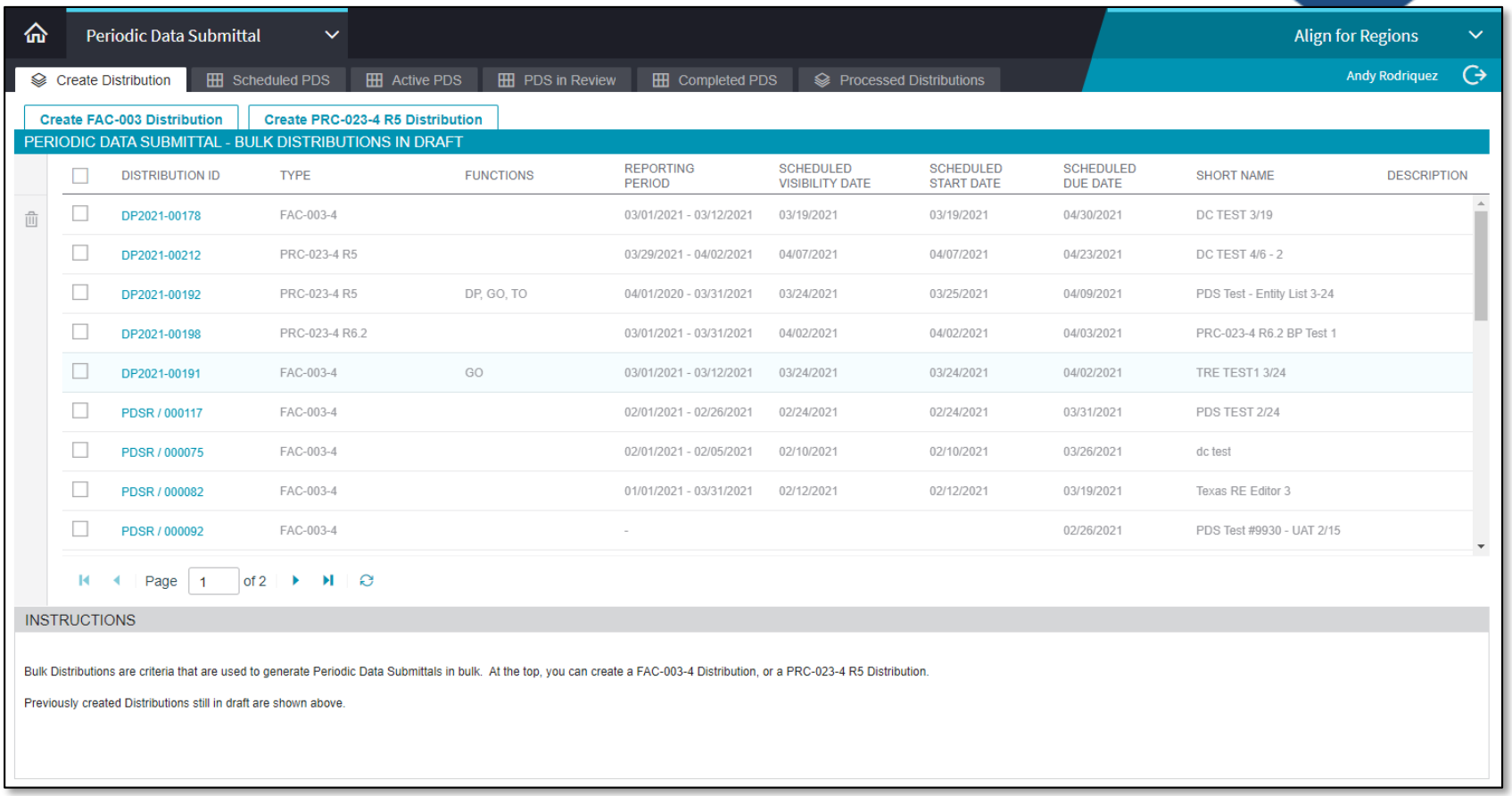
- Entities respond to questions, submit evidence to SEL, submit any Findings
- Supports Entity Attestations to streamline future processing
- Regional Entities review and create Findings, if needed

Self-Certification Customization



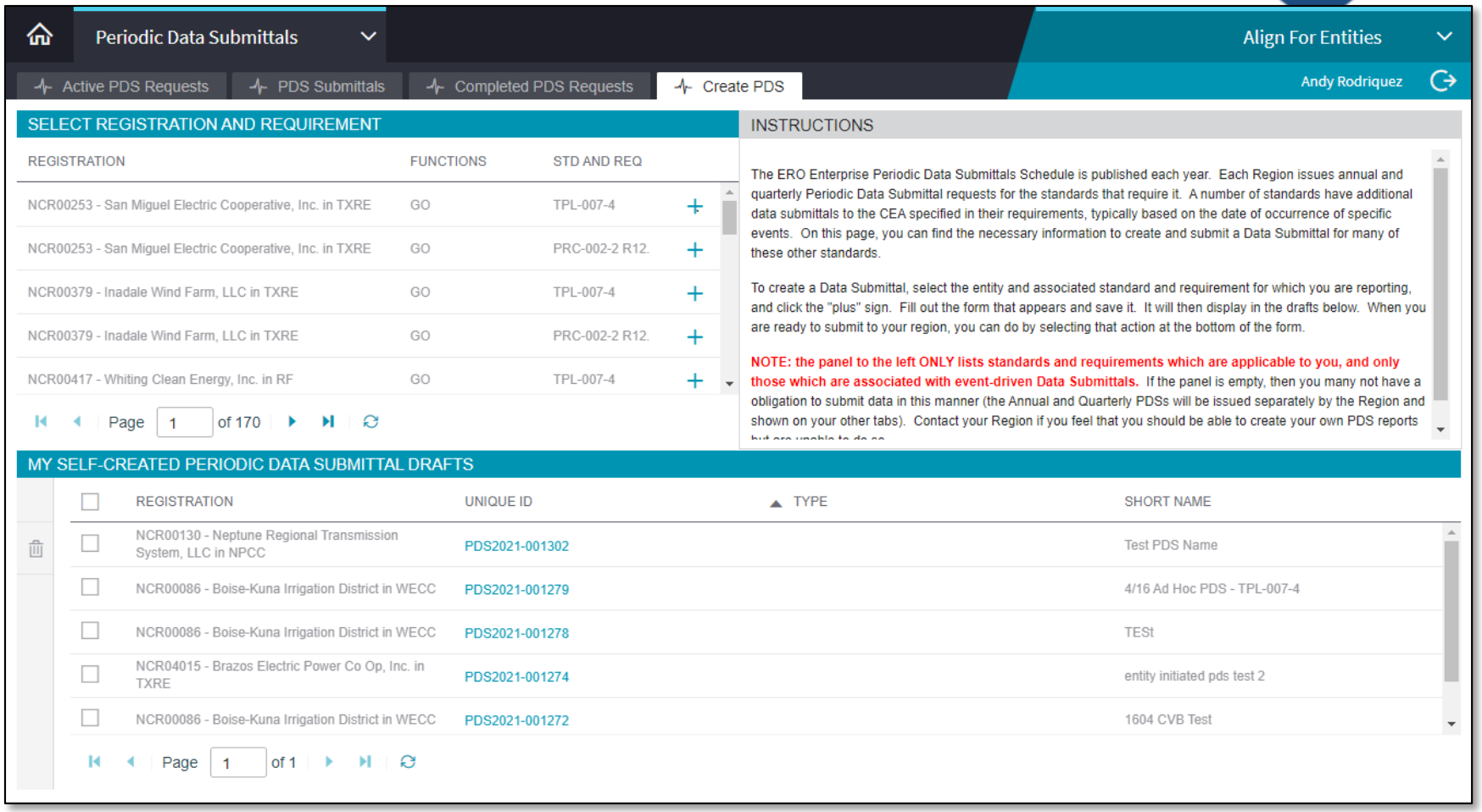
- Regional Entities can create custom questions for specific requirements in their region
- NERC can do the same across all Regional Entities

Periodic Data Submittals



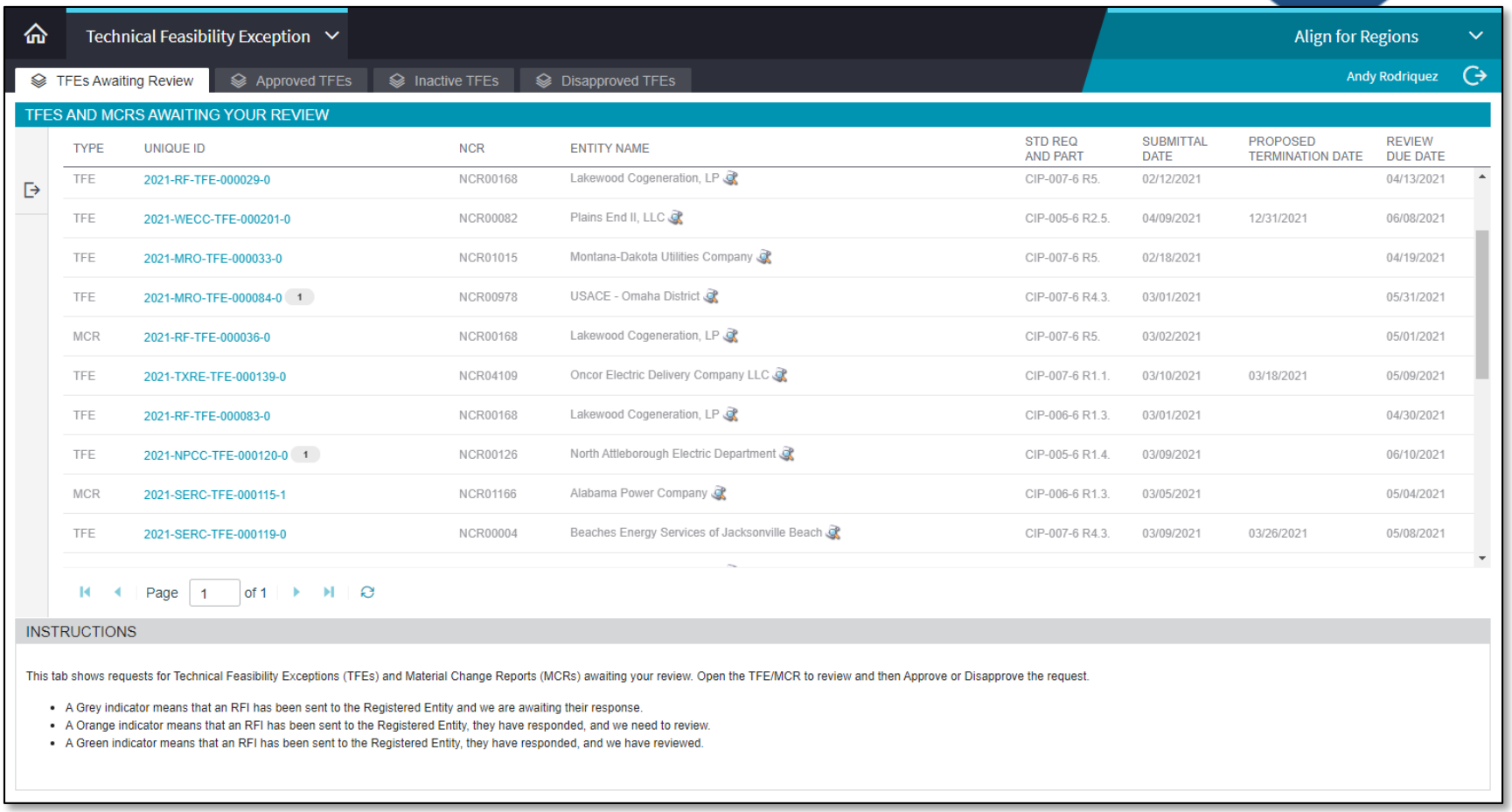
- Regional Entities create and schedule bulk PDS distributions
- Entities respond and submit data to SEL
- Support Entity Attestations to streamline future processing

Event-Driven Data Submittals



- Registered entities can also create event-driven data submittals

Technical Feasibility Exceptions



- Entities create TFEs and Material Change Reports in Align and submit evidence to SEL
- Regional Entities review, request information, and approve/reject

Release 3 Functionality

- Inherent Risk Assessments
- Compliance Oversight Plans
- Compliance Audits, Spot Check, and Investigations
- Complaints

Challenges

- **Resources:** Multiple parallel efforts (R1 training/rollout, R2 user acceptance testing, R3 design, ongoing stakeholder engagement)
- **Budget pressure:** Balance in-scope efforts with continuous improvement requests (i.e., 50 enhancements from stakeholders)
- **Security vs Usability:** Can involve multiple steps to keep data secure

How To Stay Informed

Key communication vehicles:

- Align newsletter for Regional Entities and registered entities
- Regional Change Agent Network
- Dedicated project page on NERC.com: Click Here
- Upcoming Compliance Monitoring and Enforcement Program (CMEP) regional workshops
- Trades meetings
- NERC News
- Social media

Questions and Answers

Background and Reference Material

Align Release 1: What to expect as a registered entity?

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 1: What to expect as a Regional Entity?

Stakeholder Group

Regional Entities

Release 1 Functionality

- Receive Self-Reports and Self-Logs from entities
- Manually create findings that result from any monitoring method (Audits, Spot Checks, Investigations, PDSs, Self-Certifications, Complaints)
- Perform Preliminary Screens, Potential Noncompliance (PNC) Reviews, and disposition determinations for each PNC/EA
- Send and received responses to RFIs
- Trigger notifications such as Notice of Alleged Violation(s) and Proposed Penalty or Sanction, Notices of Confirmed Violation(s), Compliance Exception Letter(s), Find, Fix, Track & Report Letter(s), and Settlement Agreements
- Receive, review, and approve mitigating activities (informal) and Mitigation Plans (formal)
- Receive notifications and view dashboards on new/open action items
- Generate report of NERC Standards and Requirements applicable to a registered entity

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Jeff Hicks, Director, Business Technology
Technology and Security Committee Meeting
May 12, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

- ERO Business Technology Projects Update
  - Continued focus on cyber protection and aging infrastructure
- Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
  - Salesforce customer relationship management (CRM)
- Hybrid Meeting Technologies
- Security Advisory Group (SAG)
- Priorities Looking Ahead

Infrastructure/Cyber Security

- Anti-virus protection upgrade
- Server operating system upgrade
- Audio Visual lease refresh
- Mobile Device Management new capability
- Email encryption upgrade

E-ISAC

- **E-ISAC Portal** – Platform replacement to Salesforce underway; expected go live in Q3 2021
- **E-ISAC Data Platform (EDP)** – Implemented functionally in June 2020; converted to a robust, reliable, secure production platform in NERC's leased data center; continue to expand analytical capabilities
- Enable and support the CRISP Operational Technology (CRISP OT) pilot

Hybrid Meeting Capabilities – Goals

- Enable an experience for virtual attendees that allows them to follow and participate effectively
- Investigate the creation of an ERO-wide Hybrid Meeting/ Communication Solution
- Elevate the overall meeting experience by using new technologies and to build an effective Hybrid Meeting approach
- Provide a simple, intuitive and consistent experience for all participants

SAG

- Advisory body established by NERC Management
- Represents all industry sectors; engagement at the Chief Information Security Officer level
- Will interface with NERC Information Technology Leadership
- Supports NERC Management with expertise and advice on data confidentiality, integrity and security
- Sensitive industry information stored or processed by NERC
- ERO Secure Evidence Locker update provided on April 23, 2021

Priorities Looking Ahead

- Analytical capabilities for the E-ISAC
- Accelerated adoption of Salesforce capabilities for the E-ISAC
- Implementation of Microsoft Teams
- Regional focus on cyber security
- Various software/hardware upgrades to NERC infrastructure

Questions and Answers