A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Update

Adam DeLuca, Director Security Operations

NERC Board of Trustees

Technology and Security Committee Open Session

November 3, 2021

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Threat Landscape
- Operations Update

Cybersecurity Threat Landscape

- Vulnerabilities
  - Adversaries continue scanning for unpatched systems and legacy vulnerabilities
  - Vulnerability disclosures continue to increase
    - Blackberry QNX real-time operation system disclosure (APB-21-05)
    - F5, CISCO, Microsoft, VxWorks, and Industrial Control Systems (ICS) vendors
    - NIST NVD on pace to have 21K vulnerabilities in 2021
- E-ISAC Response
  - Increased production and information sharing
    - 2020: 292 portal posts vs. 2021: 415 (30% increase)
    - New products
      - ICS Security Bulletins
      - Weekly Vulnerability Summaries

Cybersecurity Threat Landscape

- Ransomware
  - Ransomware attacks increased 288% in the first half of 2021
    - 10% of all attacks targeted the electricity sector
  - Ransomware gangs continue to be associated with nation-state actors, particularly Russia
  - Conti and Lockbit groups have been very active

- E-ISAC Response
  - 2021: 214 Ransomware posts (61% increase)
  - Weekly Ransomware Update
  - E-ISAC Report: Ransomware Attack Techniques (Posting 135279)

Physical Security Threat Landscape

- Domestic Violent Extremists and Activism
  - Threats targeting electricity assets
  - Traditionally, fall brings more campaigns against transmission lines, pipelines and generation assets

- E-ISAC Response
  - Monitoring future trends
    - Geo-political implications to the sector
    - Civil Unrest
  - New products
    - Physical security online threat deck
    - Vulnerability of Integrated Security Analysis Workshops

Operations Update

- Watch Operations Team is 24x7x365
  - Handle over 360 cases per month since February 2021
- Primary Functions
  - Monitoring and Alerting
    - Dark Web (cyber crime and ransomware), Shodan alerts, Open Source
  - Informational Support and Real-Time Analysis
    - Over 600 direct to members and partners since 2021
    - 21% increase in postings in 2021 (YTD)
- E-ISAC Stakeholder Survey Feedback
  - More targeted production and efficiency
    - Consolidated reports, more mature thresholds for production
      - CRISP IOC real-time support, weekly wrap ups (already in production)
    - Continuous improvement

Operations Update

- CRISP OT Dragos Pilot underway
  - Training completed
  - Threat hunts producing results
- Small and Medium Utility MEC Working Group
  - Weekly situational report developed
  - Member driven portal community established
- Survey Feedback
  - Focus on targeted, actionable production
    - Portal production from threat hunts
      - Formalized, direct to members, portal postings for industry
      - Dedicated production check points for postings and other product
    - Streamlined processes and procedures

Questions and Answers

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Stakeholder Feedback Surveys

Bluma Sussman, Director, Membership

NERC Board of Trustees

Technology and Security Committee Open Session

November 3, 2021

Progress Update

- Conducted additional analysis of J.D. Power Report findings
- Reviewed data with E-ISAC leadership teams and identified opportunities
- Engaged with respondents who gave lower NPS scores
- Developing Action Plans

Survey Follow Up

- Leadership team outreach to lower NPS scores
  - Conducted outreach to 10% of respondents; interacted with half
  - Aligned outreach to areas of expertise across the team
  - Feedback aligned with overall survey themes

I want to be able to filter on the Portal by topic or region

Ability to chat or share with affinity groups

I'm looking for clearer guidance on what to share

Lots of noise on the Portal, can we streamline who can share information?

More special topic webinars and briefings on trends

Looking for products that are geared to staff at my level

Survey Feedback

- Overall Satisfaction (OSAT) and Net Promoter Score (NPS) are excellent
  - 95% rated their overall experience as *Good to Perfect*
  - 93% use E-ISAC products and posts to inform
  - 89% prefer receiving information via email notifications
  - 67% prefer some curation of information
  - 49% prefer virtual only events or a mix of in-person and virtual

Survey Feedback

- Improve information sharing
  - Minimize barriers to sharing information and make information easier to consume
- Explore ways to meet the needs of a diverse membership
  - Stakeholders would like both inclusive *and targeted content*
  - Audience segmentation
- Event participation
  - GridEx and GridSecCon
  - Industry Engagement Program (IEP)
- Amplify successful outreach programs including IEP and physical and cybersecurity working groups

Next Steps

- Develop and Implement Action Plans by Dec 31, 2021
- Continue to Follow up on Feedback
- Conduct Next Survey in 2022

Questions and Answers

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

GridEx VI

Laura Brown, Director Strategy, Policy, and Programs

NERC Board of Trustees

Technology and Security Committee Open Session

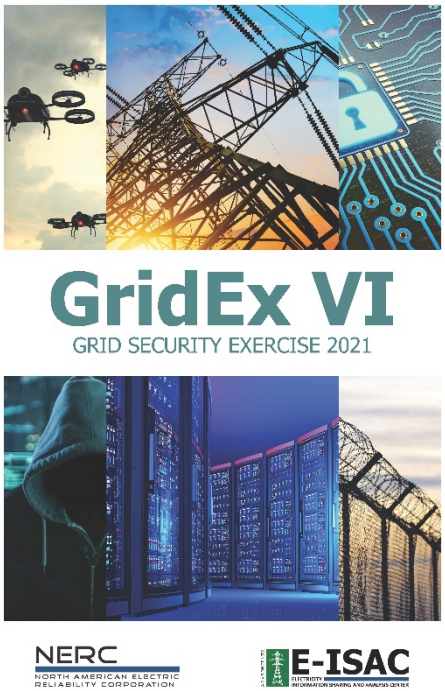
November 3, 2021

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

GridEx VI Goal and Objectives

Exercise the resilience of the North American electricity system in the face of a coordinated attack from a nation-state adversary



- Activate incident, operating, and crisis management response plans
- Enhance coordination with government to facilitate restoration
- Identify interdependence concerns with natural gas and telecommunications sectors
- Exercise response to a supply chain-based compromise to critical components
- Identify common mode and cyber operation concerns across interconnections

Executive Tabletop

- Scenario impacts North American west coast
- Includes greater participation from other critical infrastructure sectors
- Will be conducted virtually
- Brock Long, Hagerty Consulting, Former FEMA Administrator will facilitate the tabletop

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Align Project

Stan Hoptroff, Vice President, Business Technology
LaCreacia Smith, Senior PMO Manager, ERO PMO
Lonnie Ratliff, Senior Manager, Cyber and Physical Security Assurance
Technology and Security Committee Open Meeting
November 3, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Align – Benefits
- Canadian Update
- Align Project Timeline
- Release 3 and 4 Updates
- Current Challenges
- How to Stay Informed

Align – Benefits

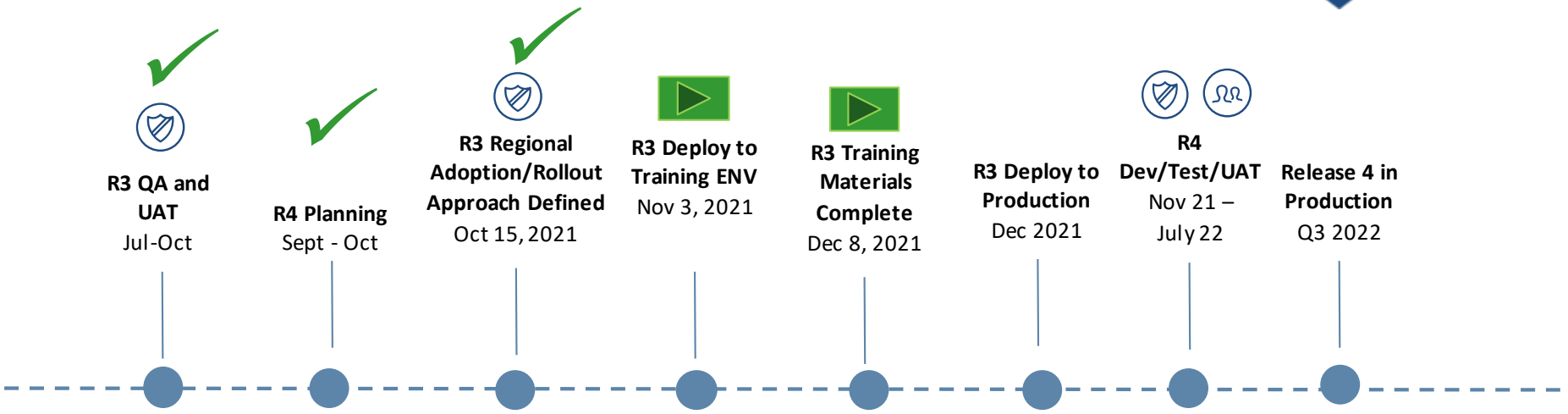
Moving to a common platform has provided:

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

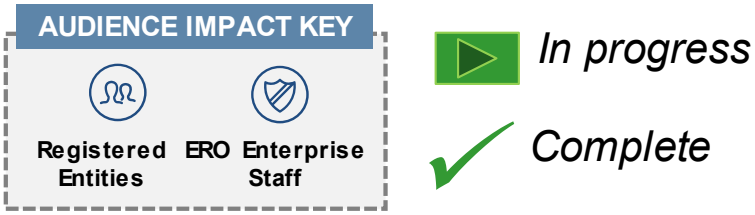
Canadian Update

- Implementation Plan
  - Manitoba & Saskatchewan (MRO) – Q1 2022
  - Alberta & British Columbia (WECC) – Q2 2022
  - Nova Scotia (NPCC) – Q4 2022

Align Timeline



- *A 3-day outage is required to deploy Release 3 to production environment (to be announced)*



Release 3 Functionality

Disclaimer

- Please be advised that the following screenshots are from our test environment and is ***TEST DATA*** (other than public registration information).
- Data shown is not complete information that would be expected in the production/live environment.

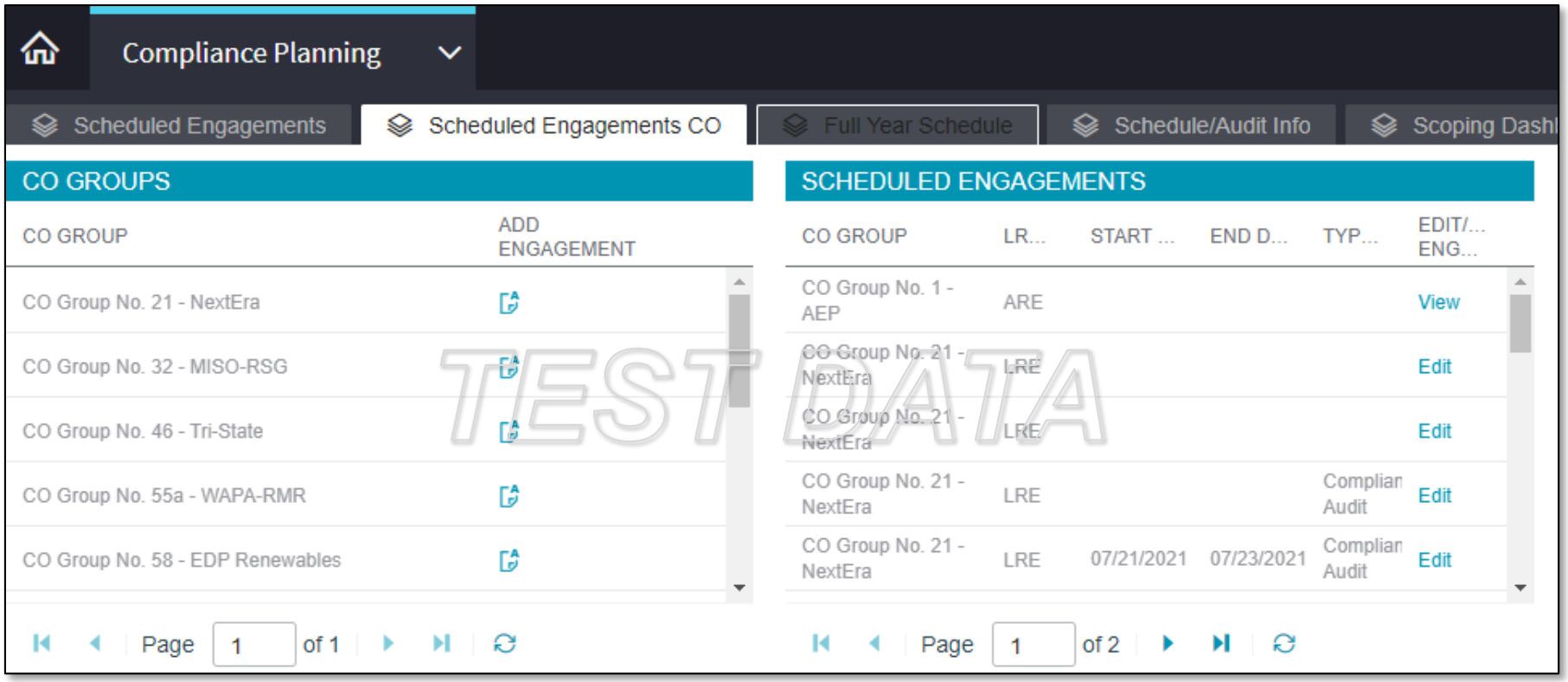
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Scheduled Engagement Dashboard

SCHEDULED ENGAGEMENTS

SCHEDULE ID	REGISTRATION	START DATE	END DATE	TYPE NAME	EDIT ENGAGEMENT
SH21-00370	NCR01015 - Montana-Dakota Utilities Company in MRO	10/06/2021	10/15/2021	Compliance Audit	Edit
SH21-00370	NCR01143 - Southwest Power Pool, Inc. in MRO	10/06/2021	10/15/2021	Compliance Audit	Edit
SH21-00363	NCR00381 - Hennepin County, MN in MRO				Edit
SH21-00352	NCR11880 - Upstream Wind Energy, LLC in MRO	09/17/2021	11/26/2021	Compliance Audit	Edit
SH21-00350	NCR00303 - Municipal Energy Agency Of Nebraska in MRO	09/13/2021	09/15/2021	Compliance Audit	Edit
SH21-00349	NCR00102 - Basin Electric Power Cooperative in MRO	09/13/2021	09/14/2021	Compliance Audit	Edit
SH21-00339	NCR00961 - Alliant Energy - East in MRO	09/30/2021	01/01/2022	Spot Check	Edit
SH21-00338	NCR00961 - Alliant Energy - East in MRO	09/01/2021		Compliance Audit	Edit
SH21-00337	NCR00961 - Alliant Energy - East in MRO	09/01/2021	09/03/2021	Spot Check	Edit
SH21-00336	NCR00962 - Alliant Energy - West in MRO	09/13/2021	09/15/2021	Compliance Audit	Edit
SH21-00335	NCR00102 - Basin Electric Power Cooperative in MRO				Edit
SH21-00327	NCR00961 - Alliant Energy - East in MRO	08/27/2021	08/31/2021	Compliance Audit	Edit
SH21-00323	NCR11778 - Thunder Ranch Wind Project, LLC in MRO			Spot Check	Edit

Coordinated Oversight Dashboard



Detailed Annual Schedule

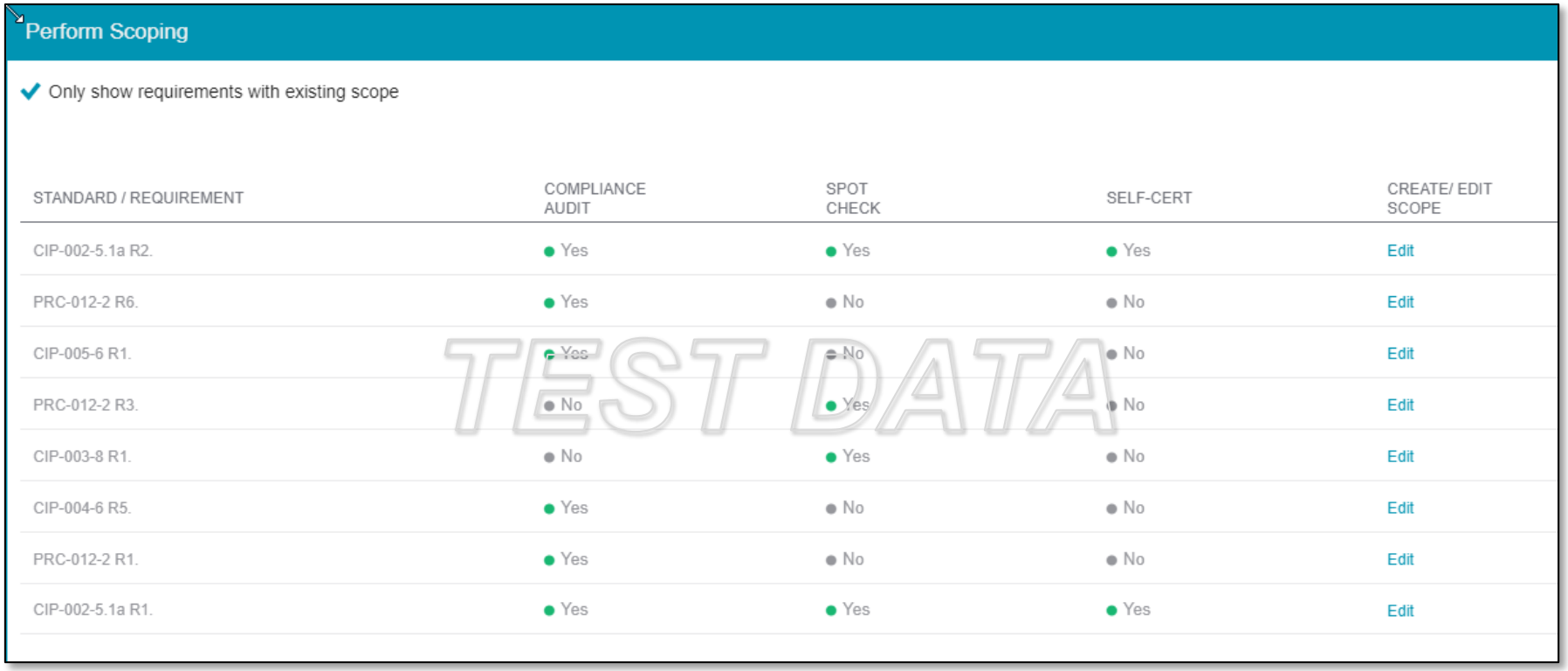
FULL YEAR SCHEDULE

YEAR	NCR/CO GROUP #	ENTITY NAME(S)	FUNCTIONS	R / ...	ENGAG... SCOPE	ST... DATE	END DATE	ANP DATE	ASSIGNED RESOU...	OBSERVERS
2021	NCR00303	Municipal Energy Agency Of Nebraska	RP	R	CIP	08/03/2(	08/14/20		Sophie Gommers	
2021	NCR00102	Basin Electric Power Cooperative	DP, GO, GOP, RP, TO, TP	R	O&P	11/29/2(	12/03/20		MRO Editor 1	
2021	NCR00961	Alliant Energy - East	BA, DP, GO, GOP, RP	R	Both	08/16/2(	08/21/20		Andy Rodriquez, Caroline Bommel, Dan	ERO 1, ERO 2, ERO 3,
2021	NCR00674	Minnesota Power (Allete, Inc.)	BA, DP, GO, GOP, RP, TO,	R	O&P	09/06/2(	09/20/20		Admin Admin, align tester 3, Andy	Aviance Clay
2021	NCR00818	Madison Gas And Electric Company	BA, DP, GO, GOP, RP	R	CIP	08/16/2(	08/20/20		Brenton Matthews, MRO Editor 1	
2021	NCR11823	Red Pine Wind Project, LLC	GO, GOP	R	CIP	08/18/2(	08/25/20		Caroline Bommel, Dan Chanda	
2021	NCR01081	City Utilities Of Springfield, MO	DP, GO, GOP, RP, TO, TOP,	R	CIP	08/06/2(	09/06/20		Andy Rodriquez, Jochem Tolk	
2021	NCR00860	Omaha Public Power District	DP, GO, GOP, RP, TO, TOP	R	CIP	08/24/2(	08/28/20		Caroline Bommel, MRO Editor 1	

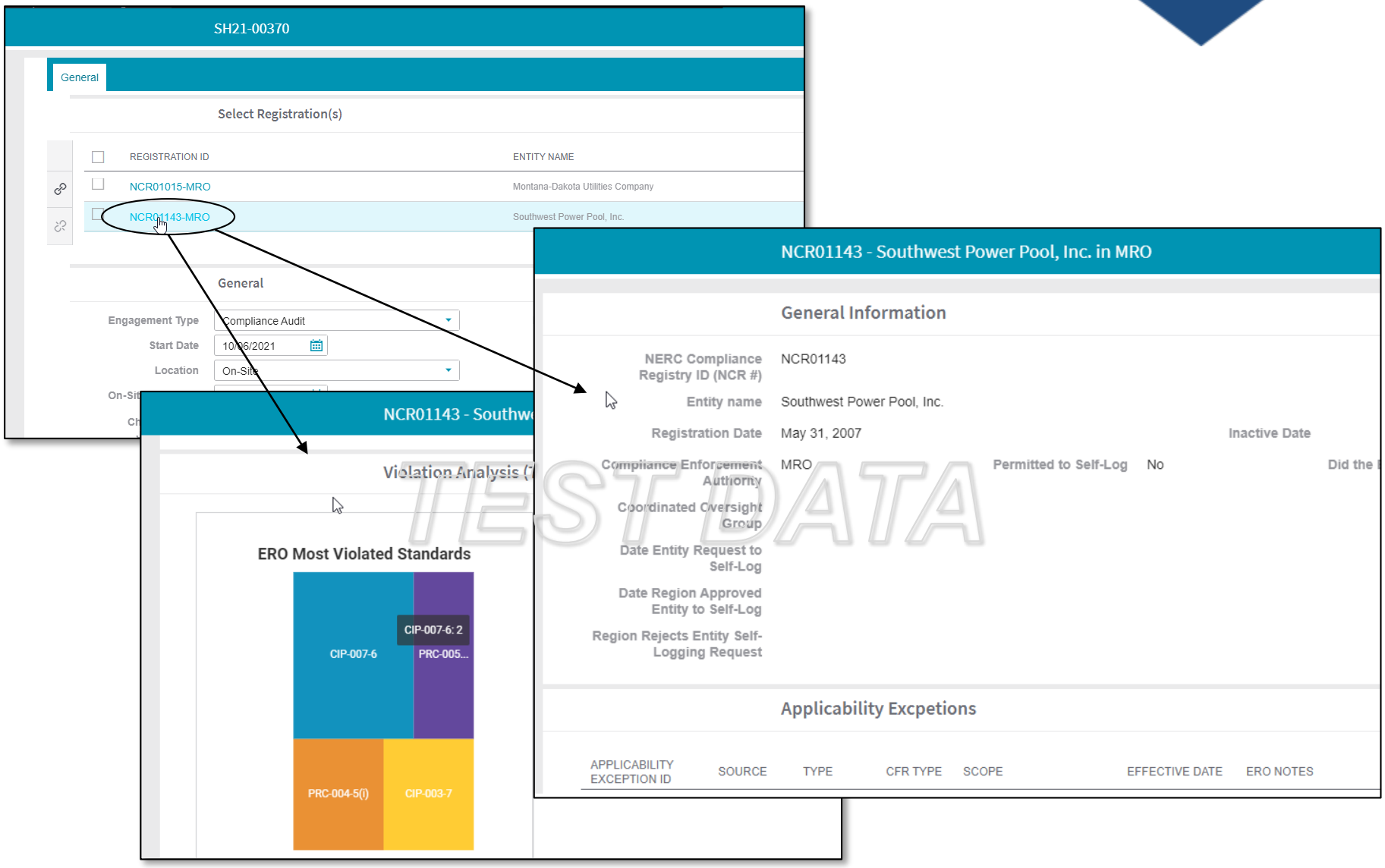
Detailed Scheduling Dashboard

REGISTRATION	LRE/ARE	DATE LAST COMPLIANCE A...	SCOPE ... AUDIT	DATE LAST COMPLIANCE INV.	SCOPE LAST COMPLIANCE ...	DATE LAST SPOT CHECK	SCOPE LAST SPOT CHECK
NCR00102 - Basin Electric Power...	LRE	09/14/2021	CIP	08/15/2021	CIP	08/14/2021	Both
NCR00303 - Municipal Energy Agency Of...	LRE	11/08/2021	O&P			08/14/2021	CIP
NCR00381 - Hennepin County, MN in MRO		09/23/2021	CIP				
NCR00633 - Tenaska Gateway Partners Ltd...	ARE						
NCR00658 - Westar Energy, Inc. in MRO		08/18/2021	Both				

Scoping for Engagements



Data Links to Other Views



Align Release 4 Functionality

- Audit Enhancements
- Scheduling Enhancements
- Complaints
- Inherent Risk Assessment
- Compliance Oversight Plan

Challenges

- **Project Fatigue:** Maintaining team and stakeholder engagement
- **People:** Parallel efforts (R3 training & rollout, R4 development)
- **Technical:** Balancing production with on-going development efforts; system status notifications; permission issues
- **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
- 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 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 Technical Feasibility Exceptions
- Create, manage and respond to Periodic Data Submittals
- Create and manage Self Certifications
- Receive and respond to 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
- Expand RFIs for Audits

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 and Compliance Oversight Plan)
- Expand RFIs for Compliance Planning

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Business Technology

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Open Meeting
November 3, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Program Area Technologies
- Shared Services Technologies
- Business Technologies

Program Area Technology

- Current Investments
  - Standards Reporting on NERC.com
  - E-ISAC Portal migration to Salesforce: December 2021
- Future Investments
  - Registration System (CORES) Enhancements
  - GADS Solar and GADS Wind
  - Replacement for Reliability Coordinator Information System
  - Reliability Assessment Data System (RADS)
  - NERC.com modernization

NERC Applications/Shared Services

- Current Investments
  - DC Office Buildout in support of NERC 2.0
- Future Investments
  - Integrated Human Resources and Finance & Accounting systems
  - Internal Audit and Risk Management system
  - Extended AV Collaboration Features, MS Teams

Business Technology

- Current Investments
  - Mobile Device Management (MDM)
  - Identity Access Management
  - Privileged Access Management
  - Data Loss Prevention
- Future Investments
  - Enhanced Cyber Security Capabilities
  - Disaster Recovery Implementation
  - Selected Core Infrastructure to off-premise (enhanced support and security)

Questions and Answers