

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





- 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



- 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



- 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



- 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



- 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



- 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



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



- 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



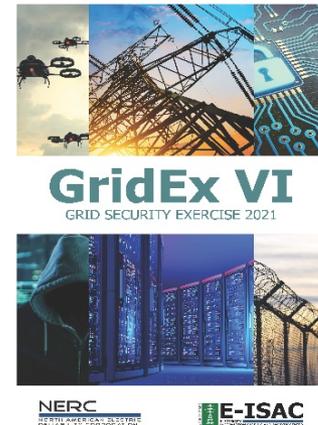
- Electricity Subsector Coordinating Council (ESCC)
- National Infrastructure Advisory Council and Cyber Solarium Coordination / DOE 100 Day Initiative
- IESO
- U.S. Government Partners
- Cross-Sector ISACs
- Analysis and Resilience Center (ARC)
- IronNet



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

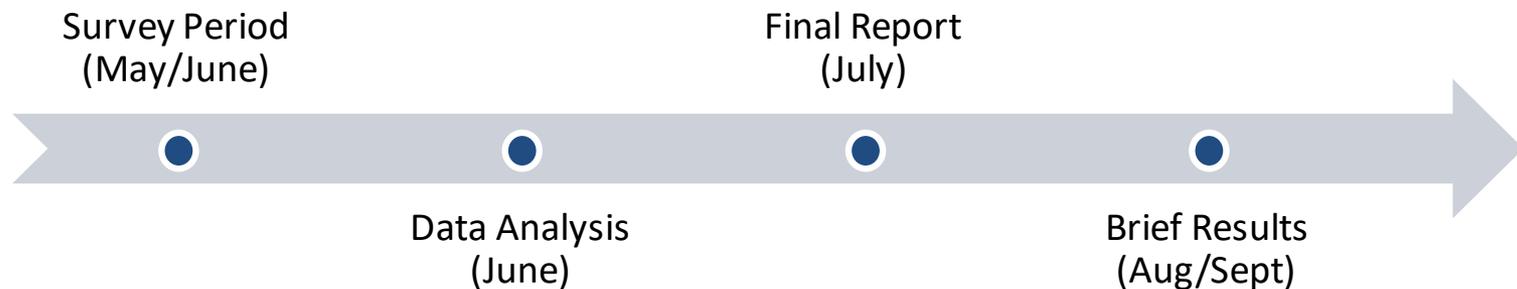
- GridSecCon 2021 will take place virtually
 - October 18 — Training Opportunities
 - October 19-20 — Keynotes, Breakout Sessions, Panels
- Grid Ex VI
 - Distributed Play – November 16-17
 - Executive Tabletop – November 18
 - Will be conducted in hybrid mode

GRIDSEC CON 2021
NERC • E-ISAC • TEXAS RE





- 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)

A stylized map of North America, including the United States, southern Canada, and northern Mexico. A solid blue horizontal band is superimposed across the middle of the map, passing through the United States. The text 'Questions and Answers' is centered within this blue band.

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Align Project Update

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

RELIABILITY | RESILIENCE | SECURITY

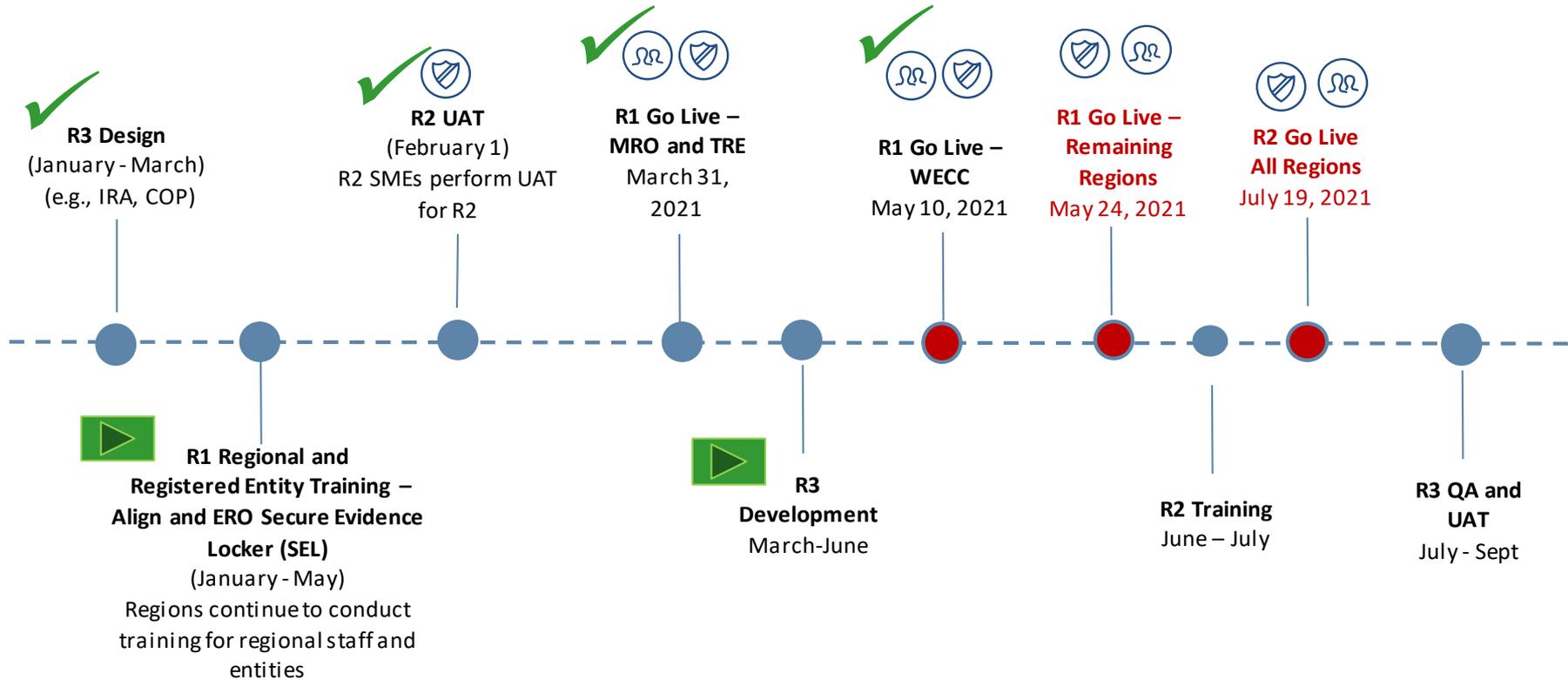


- Align Benefits
- Align Timeline
- Release 2 Functionality
- Release 3 Functionality
- Challenges
- How to Stay Informed

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
 Enterprise Staff
 ERO

In progress
 Complete

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

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

Topic	Current State	Future State
Self-Certifications	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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

Align for Regions

LS-2/3

General Requirement, Function, and Entity Selection Distribution and Question Preview Attestations Action

Self-Cert Distribution Preview

Your Self Cert(s) will be sent to the following entities and functions, for the following Requirements.
Note: You have to save (update) this form to see any changes you made above reflected in this summary.

REGISTRATIONS	FUNCTIONS	REQUIREMENTS	PCC	ACC
NCR00879 - PJM Interconnection, LLC in SERC	BA	BAL-001-2 R1.	Michael Del Viscio	Bradley Hofferkamp, Chris Moran, James...
NCR00917 - Southern Indiana Gas & Electric Company d/b/a CenterPoint Energy Indiana South in RF	BA	BAL-001-2 R1.	Amy Folz	Brian Tooley, Bryan Koyle, Carol Buckman,...

Page 1 of 1

Update Close

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

The screenshot displays a web interface for self-certifications. At the top, there's a navigation bar with 'Self Certifications' and 'Align For Entities'. The main content area is titled 'DC TEST 2/16 - UAT'. Below this, there are several fields for registration and compliance details. A 'Questions' section follows, with instructions on how to proceed. At the bottom, there is a 'SELF-CERT ASSESSMENT' table with one entry.

Self-Cert ID	SC-000049	Region/LRE	WECC
Registration	NCR00086 - Boise-Kuna Irrigation District in WECC	Compliance Year	2020
Self-Cert Name	DC TEST 2/16 - UAT	Instructions	CIP-003-8 R1.
Submit on or after	February 16, 2021	Monitoring Period Start	February 1, 2021
But no later than	March 26, 2021	Monitoring Period End	February 26, 2021
Point of Contact			
Requestor			

Questions

Instructions Open the questions below and answer each question.
Need more time? Scroll down to **Request an Extension**.
Have evidence to upload? Scroll down to the **Evidence** section.

SELF-CERT ASSESSMENT		
REQUIREMENT/PART LANGUAGE		STATUS
Questions related to CIP-003-8 R1.	Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:	Submitted

Update Close

- 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

The screenshot displays the 'Self-Cert Administration' interface. At the top, there is a navigation bar with 'Self-Cert Administration' and 'Align for Regions' (set to 'Andy Rodriguez'). Below this is the 'Self-Cert Question Library' section.

The main content area is divided into two panels:

- REGION QUESTION LIBRARY INSTRUCTIONS:** Contains instructions on how to create region-specific questions, including a 'Negate' section with options like 'Assessment Attribute', 'Operation Value', and 'Value'.
- SELF CERT ADMINISTRATION - CUSTOM REGION QUESTION GROUPS:** A table listing question groups with columns for 'GROUP NAME', 'APPLICABLE SUBJECTS', and 'ADD QUESTION'.

GROUP NAME	APPLICABLE SUBJECTS	ADD QUESTION
Andy Rodriguez TEST <i>Assessment Type Missing</i>	BAL-001-0.1a R2.	+
MRO CIP-003-8 R3. Specif <i>Self-Certification</i>	CIP-003-8 R3.	+
MRO - CIP003-1 Qs <i>Self-Certification</i>	CIP-003-1 R1., CIP-003-1 R2., CIP-003-1 R3., CIP-003-1 R4., CIP-003-1 R5., CIP-003-1 R6.	+
CIP-002 Question Template <i>Self-Certification</i>	Partial List: CIP-002-1 R1., CIP-002-1 R2., CIP-002-1 R3., CIP-002-1 R4., CIP-002-2 R1., CIP-002-2 R2., CIP-002-2 R3., CIP-002-2 R4., CIP-002-3 R1., CIP-002-3 R2., CIP-002-3 R3., CIP-002-3	+

Below the groups panel is the 'SELF CERT ADMINISTRATION - CUSTOM REGION QUESTIONS' section, which is a table listing individual questions:

APPLICABLE TO	QUESTION PREVIEW	TYPE	QUESTION GROUP
CIP-003-8 R3.	CIP-003-8 R3 MRO SPECIFIC QUESTION 1 Click here to edit	Text Line	MRO CIP-003-8 R3. Specif
CIP-003-8 R3.	CIP-003-8 R3 MRO SPECIFIC QUESTION 2 Click here to edit	Text Line	MRO CIP-003-8 R3. Specif
CIP-003-1 R1.	CVB: CIP example question (MRO) Click here to edit	Option List	MRO - CIP003-1 Qs
CIP-003-1 R2.	CVB: CIP example question (MRO) Click here to edit	Option List	MRO - CIP003-1 Qs
CIP-003-1 R3.	CVB: CIP example question (MRO) Click here to edit	Option List	MRO - CIP003-1 Qs

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

Periodic Data Submittal

Align for Regions

Create Distribution | Scheduled PDS | Active PDS | PDS in Review | Completed PDS | Processed Distributions

Andy Rodriguez

Create FAC-003 Distribution | Create PRC-023-4 R5 Distribution

PERIODIC DATA SUBMITTAL - BULK DISTRIBUTIONS IN DRAFT

DISTRIBUTION ID	TYPE	FUNCTIONS	REPORTING PERIOD	SCHEDULED VISIBILITY DATE	SCHEDULED START DATE	SCHEDULED DUE DATE	SHORT NAME	DESCRIPTION
DP2021-00178	FAC-003-4		03/01/2021 - 03/12/2021	03/19/2021	03/19/2021	04/30/2021	DC TEST 3/19	
DP2021-00212	PRC-023-4 R5		03/29/2021 - 04/02/2021	04/07/2021	04/07/2021	04/23/2021	DC TEST 4/6 - 2	
DP2021-00192	PRC-023-4 R5	DP, GO, TO	04/01/2020 - 03/31/2021	03/24/2021	03/25/2021	04/09/2021	PDS Test - Entity List 3-24	
DP2021-00198	PRC-023-4 R6.2		03/01/2021 - 03/31/2021	04/02/2021	04/02/2021	04/03/2021	PRC-023-4 R6.2 BP Test 1	
DP2021-00191	FAC-003-4	GO	03/01/2021 - 03/12/2021	03/24/2021	03/24/2021	04/02/2021	TRE TEST1 3/24	
PDSR / 000117	FAC-003-4		02/01/2021 - 02/26/2021	02/24/2021	02/24/2021	03/31/2021	PDS TEST 2/24	
PDSR / 000075	FAC-003-4		02/01/2021 - 02/05/2021	02/10/2021	02/10/2021	03/26/2021	dc test	
PDSR / 000082	FAC-003-4		01/01/2021 - 03/31/2021	02/12/2021	02/12/2021	03/19/2021	Texas RE Editor 3	
PDSR / 000092	FAC-003-4		-			02/26/2021	PDS Test #9930 - UAT 2/15	

Page 1 of 2

INSTRUCTIONS

Bulk Distributions are criteria that are used to generate Periodic Data Submittals in bulk. At the top, you can create a FAC-003-4 Distribution, or a PRC-023-4 R5 Distribution.

Previously created Distributions still in draft are shown above.

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

Home
Periodic Data Submittals
Align For Entities

Active PDS Requests
PDS Submittals
Completed PDS Requests
Create PDS
Andy Rodriguez

SELECT REGISTRATION AND REQUIREMENT

REGISTRATION	FUNCTIONS	STD AND REQ	
NCR00253 - San Miguel Electric Cooperative, Inc. in TXRE	GO	TPL-007-4	+
NCR00253 - San Miguel Electric Cooperative, Inc. in TXRE	GO	PRC-002-2 R12.	+
NCR00379 - Inadale Wind Farm, LLC in TXRE	GO	TPL-007-4	+
NCR00379 - Inadale Wind Farm, LLC in TXRE	GO	PRC-002-2 R12.	+
NCR00417 - Whiting Clean Energy, Inc. in RF	GO	TPL-007-4	+

Page 1 of 170

INSTRUCTIONS

The ERO Enterprise Periodic Data Submittals Schedule is published each year. Each Region issues annual and quarterly Periodic Data Submittal requests for the standards that require it. A number of standards have additional data submittals to the CEA specified in their requirements, typically based on the date of occurrence of specific events. On this page, you can find the necessary information to create and submit a Data Submittal for many of these other standards.

To create a Data Submittal, select the entity and associated standard and requirement for which you are reporting, and click the "plus" sign. Fill out the form that appears and save it. It will then display in the drafts below. When you are ready to submit to your region, you can do by selecting that action at the bottom of the form.

NOTE: the panel to the left ONLY lists standards and requirements which are applicable to you, and only those which are associated with event-driven Data Submittals. If the panel is empty, then you may not have an obligation to submit data in this manner (the Annual and Quarterly PDSs will be issued separately by the Region and shown on your other tabs). Contact your Region if you feel that you should be able to create your own PDS reports but are unable to do so.

MY SELF-CREATED PERIODIC DATA SUBMITTAL DRAFTS

<input type="checkbox"/>	REGISTRATION	UNIQUE ID	TYPE	SHORT NAME
<input type="checkbox"/>	NCR00130 - Neptune Regional Transmission System, LLC in NPCC	PDS2021-001302		Test PDS Name
<input type="checkbox"/>	NCR00086 - Boise-Kuna Irrigation District in WECC	PDS2021-001279		4/16 Ad Hoc PDS - TPL-007-4
<input type="checkbox"/>	NCR00086 - Boise-Kuna Irrigation District in WECC	PDS2021-001278		TEST
<input type="checkbox"/>	NCR04015 - Brazos Electric Power Co Op, Inc. in TXRE	PDS2021-001274		entity initiated pds test 2
<input type="checkbox"/>	NCR00086 - Boise-Kuna Irrigation District in WECC	PDS2021-001272		1604 CVB Test

Page 1 of 1

- Registered entities can also create event-driven data submittals

Technical Feasibility Exception
Align for Regions

TFEs Awaiting Review
Approved TFEs
Inactive TFEs
Disapproved TFEs
Andy Rodriguez

TFES AND MCRS AWAITING YOUR REVIEW								
	TYPE	UNIQUE ID	NCR	ENTITY NAME	STD REQ AND PART	SUBMITTAL DATE	PROPOSED TERMINATION DATE	REVIEW DUE DATE
	TFE	2021-RF-TFE-000029-0	NCR00168	Lakewood Cogeneration, LP	CIP-007-6 R5.	02/12/2021		04/13/2021
	TFE	2021-WECC-TFE-000201-0	NCR00082	Plains End II, LLC	CIP-005-6 R2.5.	04/09/2021	12/31/2021	06/08/2021
	TFE	2021-MRO-TFE-000033-0	NCR01015	Montana-Dakota Utilities Company	CIP-007-6 R5.	02/18/2021		04/19/2021
	TFE	2021-MRO-TFE-000084-0 1	NCR00978	USACE - Omaha District	CIP-007-6 R4.3.	03/01/2021		05/31/2021
	MCR	2021-RF-TFE-000036-0	NCR00168	Lakewood Cogeneration, LP	CIP-007-6 R5.	03/02/2021		05/01/2021
	TFE	2021-TXRE-TFE-000139-0	NCR04109	Oncor Electric Delivery Company LLC	CIP-007-6 R1.1.	03/10/2021	03/18/2021	05/09/2021
	TFE	2021-RF-TFE-000083-0	NCR00168	Lakewood Cogeneration, LP	CIP-006-6 R1.3.	03/01/2021		04/30/2021
	TFE	2021-NPCC-TFE-000120-0 1	NCR00126	North Attleborough Electric Department	CIP-005-6 R1.4.	03/09/2021		06/10/2021
	MCR	2021-SERC-TFE-000115-1	NCR01166	Alabama Power Company	CIP-006-6 R1.3.	03/05/2021		05/04/2021
	TFE	2021-SERC-TFE-000119-0	NCR00004	Beaches Energy Services of Jacksonville Beach	CIP-007-6 R4.3.	03/09/2021	03/26/2021	05/08/2021

Page 1 of 1

INSTRUCTIONS

This tab shows requests for Technical Feasibility Exceptions (TFEs) and Material Change Reports (MCRs) awaiting your review. Open the TFE/MCR to review and then Approve or Disapprove the request.

- A Grey indicator means that an RFI has been sent to the Registered Entity and we are awaiting their response.
- A Orange indicator means that an RFI has been sent to the Registered Entity, they have responded, and we need to review.
- A Green indicator means that an RFI has been sent to the Registered Entity, they have responded, and we have reviewed.

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

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

- **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

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

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

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



- 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

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

- **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

- 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

- 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

- 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