A DIVISION OF NERC
E-ISAC
ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Operations

Manny Cancel, Senior Vice President NERC and CEO E-ISAC

Technology and Security Committee
Open Meeting
May 10, 2023

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

Agenda

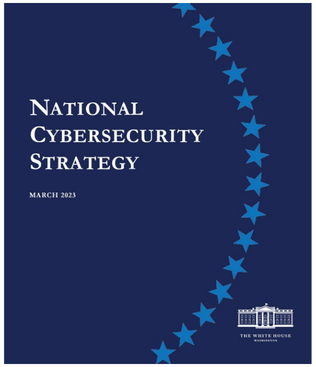
- Cyber Strategy
- Threat Landscape
- New E-ISAC Products
- Energy Threat and Analysis Center (ETAC)

Cyber Strategy

- U.S. Office of the Director of National Intelligence (ODNI) Annual Threat Assessment
- Canadian Centre for Cybersecurity Threat Assessment
- National Cybersecurity Strategy

Annual Threat Assessment
INTELLIGENCE COMMUNITY ASSESSMENT

CANADIAN CENTRE FOR CYBER SECURITY
ISSN 2816-9182
National Cyber Threat Assessment
2023 2024
Communications Security Establishment
Centre de la sécurité des télécommunications
Canada



NATIONAL CYBERSECURITY STRATEGY
MARCH 2023
THE WHITE HOUSE
WASHINGTON

Summary of Threat Assessments

Nation states possess the capability to disrupt critical infrastructure in North America and continue to target the electricity sector

- Russia remains a top cyber threat as it employs its espionage, influence, and attack capabilities
- China is one of the most dynamic cyber threats and continues to demonstrate increasing sophistication and adaptive techniques
- Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat
- North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat

Cyber Strategy

Summary of National Cyber Strategy

Complex threat environment and evolving technologies demand a more intentional, more coordinated, and more well-resourced approach to cyber defense

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

Threat Landscape

Cyber

- Adversaries are capable and adaptive
- Operational Technology (OT) continues to be targeted
- Ransomware remains a persistent threat
- Vendors and other third parties are targeted and compromised

Physical

- Serious incidents in Q1 2023 decreased in comparison with previous quarter
- Number of incidents in Q1 2023 still represents elevated frequency with respect to historical trends
- The E-ISAC assesses the physical security threats and risks will continue throughout the year

E-ISAC Products and Services

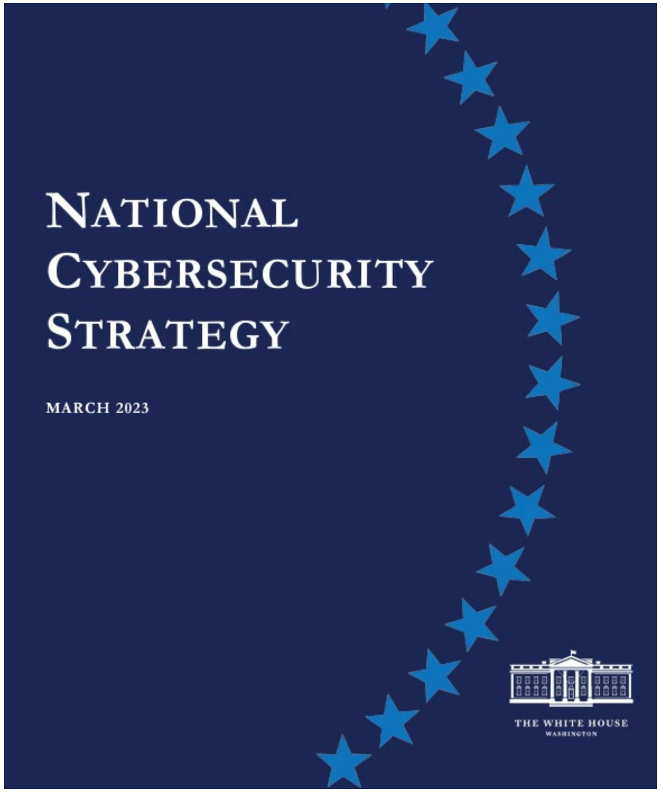
Cyber

- Threat hunts
- Summary of Key Threats for Security Executives
- CRISP
- Clearinghouse
- Dark web/Ransomware forum Monitoring
- Shodan searches

Physical

- Physical Security Resource Guide
- Avenues of Approach and Firing Positions at Substations
- Monthly Online Threat Summary
- Drone Detection Pilot: Trend Analysis and Key Findings
- Summary of Member and Partner Weekly Postings
- Open Source Intelligence Report

ETAC



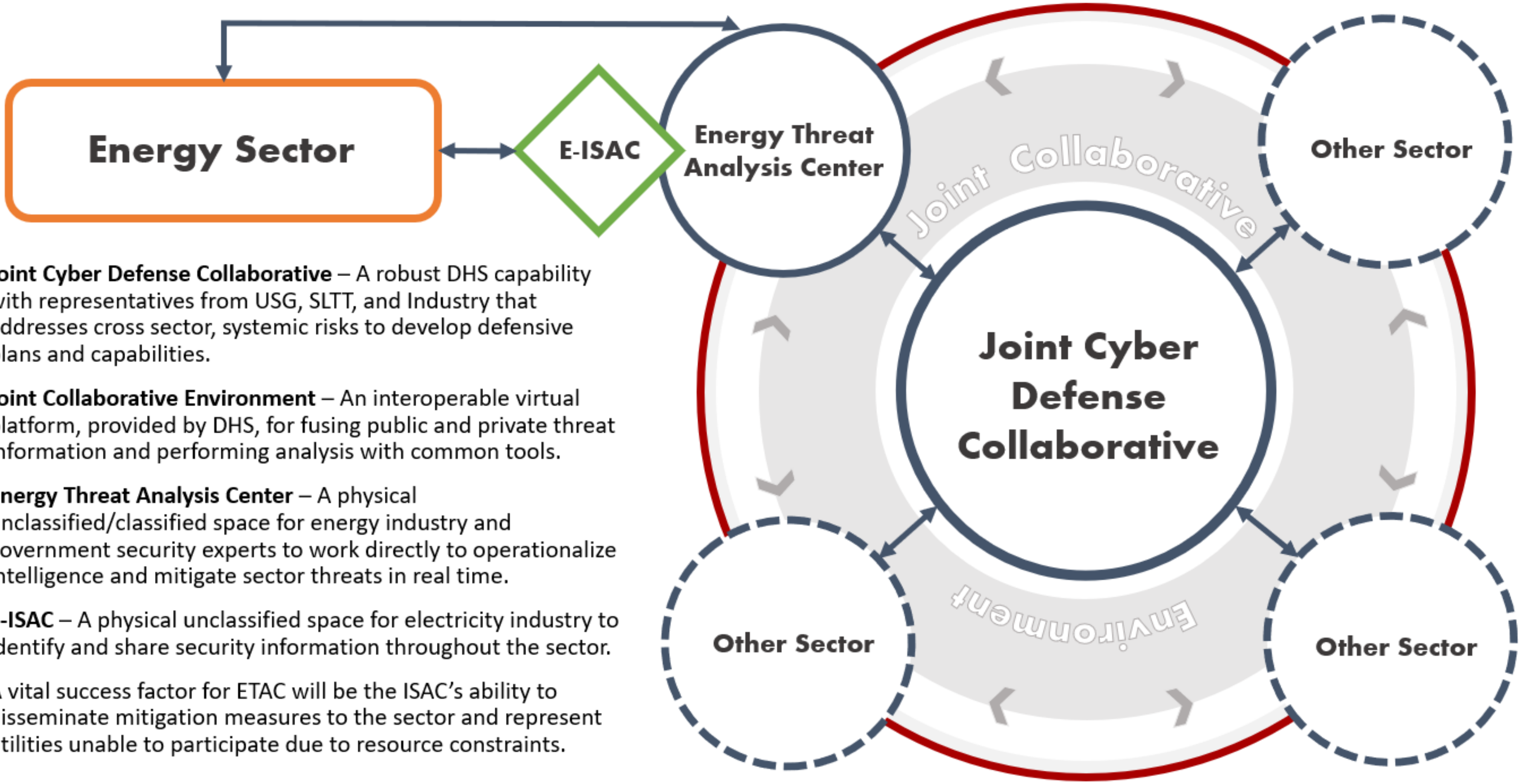
NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE
WASHINGTON

- Unique operational collaboration model
  - Referenced in U.S. national cyber strategy
- A spoke to Joint Cyber Defense Collaborative (JCDC) hub
- Provides link between industry, intelligence community, DOE, and labs
- E-ISAC a full partner with four IOUs in current pilot
- E-ISAC serves as industry CIPAC co-chair

ETAC Ecosystem


Energy Sector
E-ISAC
Energy Threat Analysis Center
Joint Collaborative Environment
Other Sector
Joint Cyber Defense Collaborative
Other Sector
Other Sector

Joint Cyber Defense Collaborative – A robust DHS capability with representatives from USG, SLTT, and Industry that addresses cross sector, systemic risks to develop defensive plans and capabilities.

Joint Collaborative Environment – An interoperable virtual platform, provided by DHS, for fusing public and private threat information and performing analysis with common tools.

Energy Threat Analysis Center – A physical unclassified/classified space for energy industry and government security experts to work directly to operationalize intelligence and mitigate sector threats in real time.

E-ISAC – A physical unclassified space for electricity industry to identify and share security information throughout the sector.

A vital success factor for ETAC will be the ISAC's ability to disseminate mitigation measures to the sector and represent utilities unable to participate due to resource constraints.

2022 ETAC Pilot Activities

- Industry and government collaboration began in January 2022
- Ukraine – Russia War collateral threats collaboration
- Equipment supply chain threats
- Operational Technology threats
- ETAC governance and capability development
- Monthly Analysts to Analysts (A2A) exchanges

Future Activities

- Establish formal governance
- Open physical location for unclassified and classified access
- Onboard additional entities
- Prioritize threats for analysis
- Develop research questions

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Business Technology Update

Stan Hoptroff, Vice President, Business Technology
Angus Willis, Director of IT Core Infrastructure and Support
LaCreacia Smith, Senior PMO Manager
Technology and Security Committee Open Meeting
May 10, 2023

RELIABILITY | RESILIENCE | SECURITY

Agenda

2023 WPP in Action

- Align Project Update
- NERC’s Infrastructure Team
- NERC’s Journey to the Cloud (Fast Follower)

Align – What We Achieved

Moving to a common platform has provided:

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

What We Learned

- Importance of security (cost and value)
- Allow time for business process harmonization
- Importance of overcoming differences within our model with common business processes
- Importance of modifying project processes to accommodate a fully virtual team
- Importance of change management
- Plan for change of ownership with vendors
- New automation for Inherent Risk Assessment and Compliance Oversight Plan required additional time and investment

2017 Starting Point

- Disparate systems and business processes
  - Web Compliance Data Management System - Five Regions
  - Compliance Information Tracking System - Three Regions
  - MK Insight - ReliabilityFirst
  - Compliance Reporting and Tracking System - NERC
  - Microsoft Productivity Applications
    - MS SharePoint
    - MS Excel
    - MS Outlook
    - MS Access

Align Financials

- Align implementation spend: $8.0M (2017-2022)
- Revised business case estimate April 2020: $7.5M
  - Revised business case variance breakdown: $470k (6.3 percent)
- Additional cost drivers include:
  - 2022: Release 4 and 4.5 required functionality – no legacy solution
  - 2022: Performance optimization and reporting database
  - 2021: Stakeholder requested enhancements for Release 1-3

Canada: Key Features Summary

- Enforcement Processing
- Canadian Regulator Access
- Audits, Spot Checks and Scheduling
- Self-Reports
- Notifications
- Periodic Data Submittals and Self-Certifications
- Reports and Dashboards

Align-Canada

- Ontario: In Production
- In Progress: Manitoba, Saskatchewan, Alberta, British Columbia, Nova Scotia
- Quebec, New Brunswick have their own systems
- Work Effort:
  - Imported standards
  - Data segmentation (provincial views only; no FERC access)
  - User interface and reports
  - Historical data migration (planned)

Align Ticket Metrics

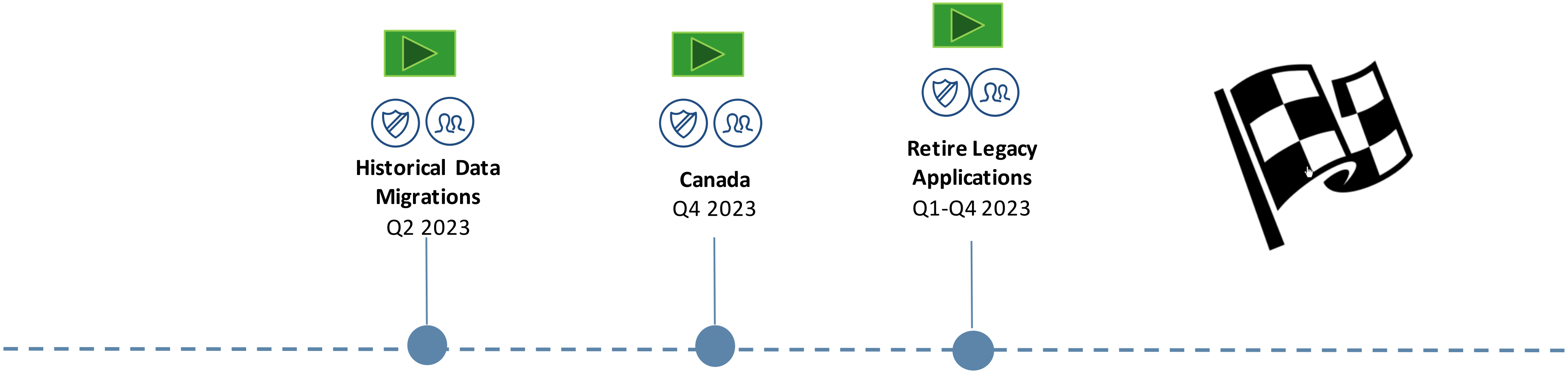
METRIC	Historical	Current
Daily Volume	6	5
Average Open	29	24
Time to Resolve		
• < 2 days	-	17%
• 3 – 14 days	-	55%
• >14 days	-	28%

Ticket Types: Account Access, Training, Defects / Enhancements

Observations / Notes:

- Focused on resolving underlying account access issues and have seen 50% drop in this ticket type
- Enhancements / Defects and Help / Training ticket types increased as more functionality was released, equalizing daily volumes and open ticket totals

Align Timeline



Historical Data Migrations
Q2 2023

Canada
Q4 2023

Retire Legacy Applications
Q1-Q4 2023

AUDIENCE IMPACT KEY

Registered Entities

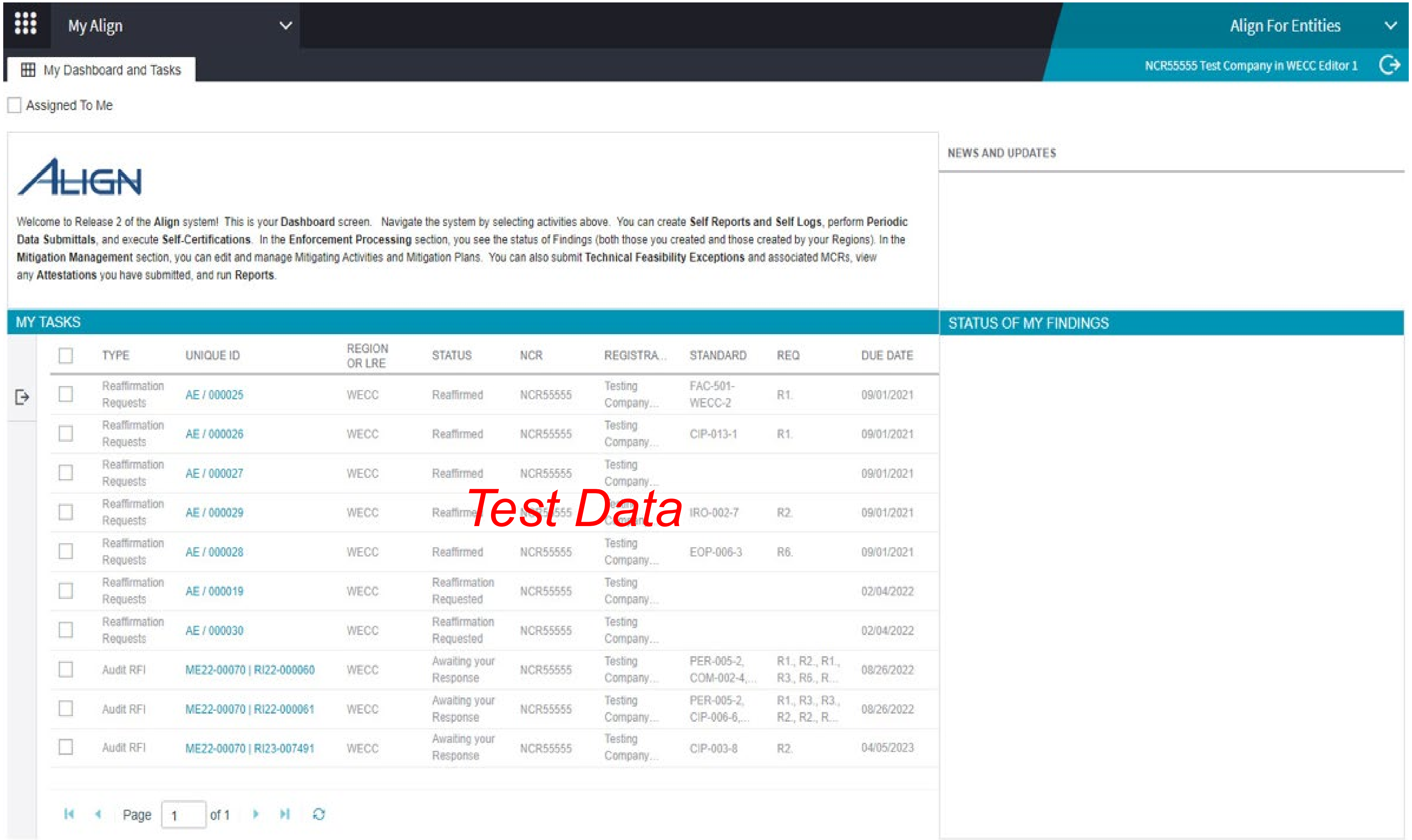
ERO Enterprise Staff

▶ *In progress*

✓ *Complete*

Align Registered Entity View

Entity – Dashboard



□ Assigned To Me

ALIGN

Welcome to Release 2 of the **Align** system! This is your **Dashboard** screen. Navigate the system by selecting activities above. You can create **Self Reports and Self Logs**, perform **Periodic Data Submittals**, and execute **Self-Certifications**. In the **Enforcement Processing** section, you see the status of Findings (both those you created and those created by your Regions). In the **Mitigation Management** section, you can edit and manage Mitigating Activities and Mitigation Plans. You can also submit **Technical Feasibility Exceptions** and associated MCRs, view any **Attestations** you have submitted, and run **Reports**.

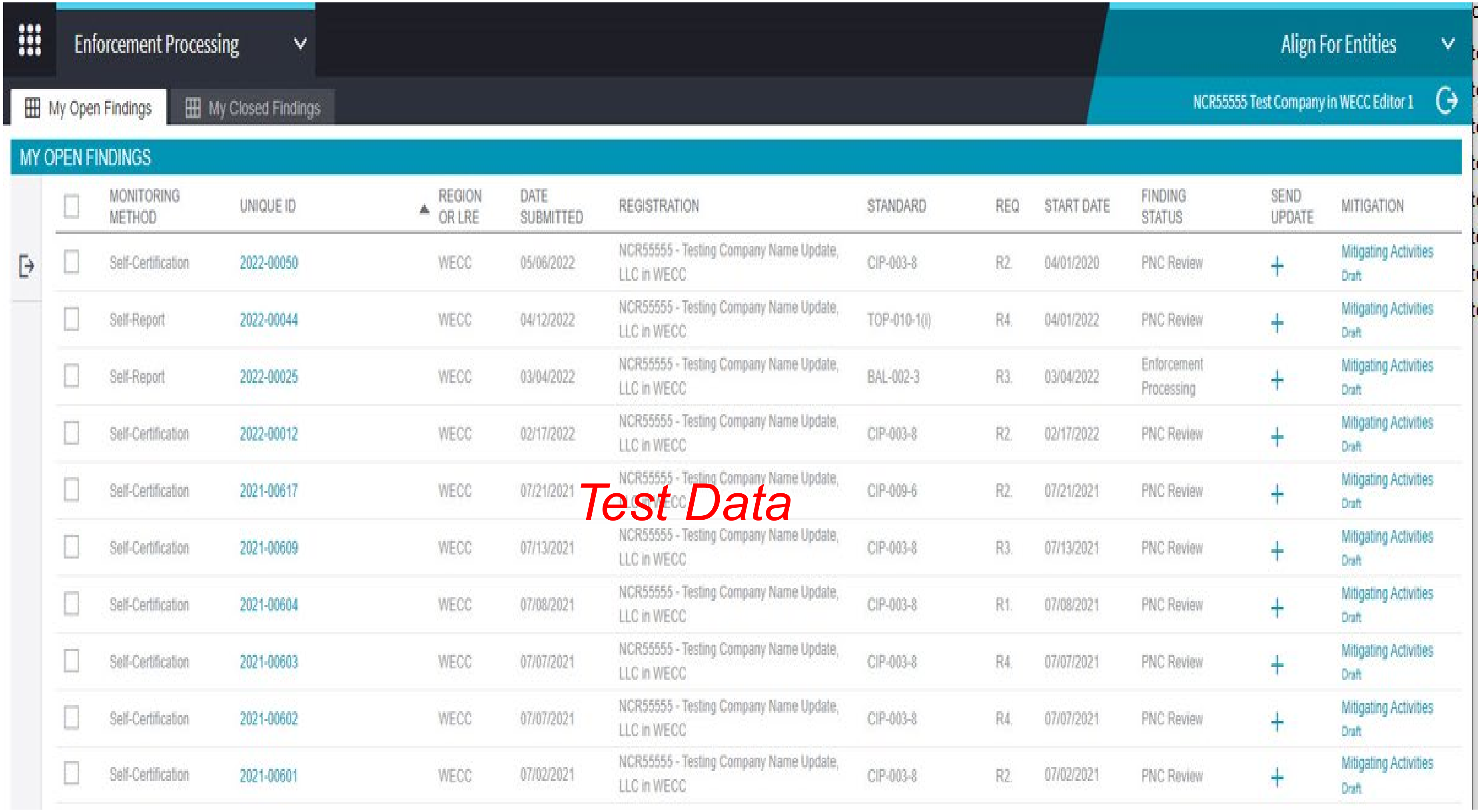
MY TASKS

□	TYPE	UNIQUE ID	REGION OR LRE	STATUS	NCR	REGISTRA...	STANDARD	REQ	DUE DATE
□	Reaffirmation Requests	AE / 000025	WECC	Reaffirmed	NCR55555	Testing Company...	FAC-501-WECC-2	R1.	09/01/2021
□	Reaffirmation Requests	AE / 000026	WECC	Reaffirmed	NCR55555	Testing Company...	CIP-013-1	R1.	09/01/2021
□	Reaffirmation Requests	AE / 000027	WECC	Reaffirmed	NCR55555	Testing Company...			09/01/2021
□	Reaffirmation Requests	AE / 000029	WECC	Reaffirmed	NCR55555	Testing Company...	IRO-002-7	R2.	09/01/2021
□	Reaffirmation Requests	AE / 000028	WECC	Reaffirmed	NCR55555	Testing Company...	EOP-006-3	R6.	09/01/2021
□	Reaffirmation Requests	AE / 000019	WECC	Reaffirmation Requested	NCR55555	Testing Company...			02/04/2022
□	Reaffirmation Requests	AE / 000030	WECC	Reaffirmation Requested	NCR55555	Testing Company...			02/04/2022
□	Audit RFI	ME22-00070 | RI22-000060	WECC	Awaiting your Response	NCR55555	Testing Company...	PER-005-2, COM-002-4,...	R1., R2., R1., R3., R6., R...	08/26/2022
□	Audit RFI	ME22-00070 | RI22-000061	WECC	Awaiting your Response	NCR55555	Testing Company...	PER-005-2, CIP-006-6,...	R1., R3., R3., R2., R2., R...	08/26/2022
□	Audit RFI	ME22-00070 | RI23-007491	WECC	Awaiting your Response	NCR55555	Testing Company...	CIP-003-8	R2.	04/05/2023

Page 1 of 1

Test Data

Entity – Open Findings

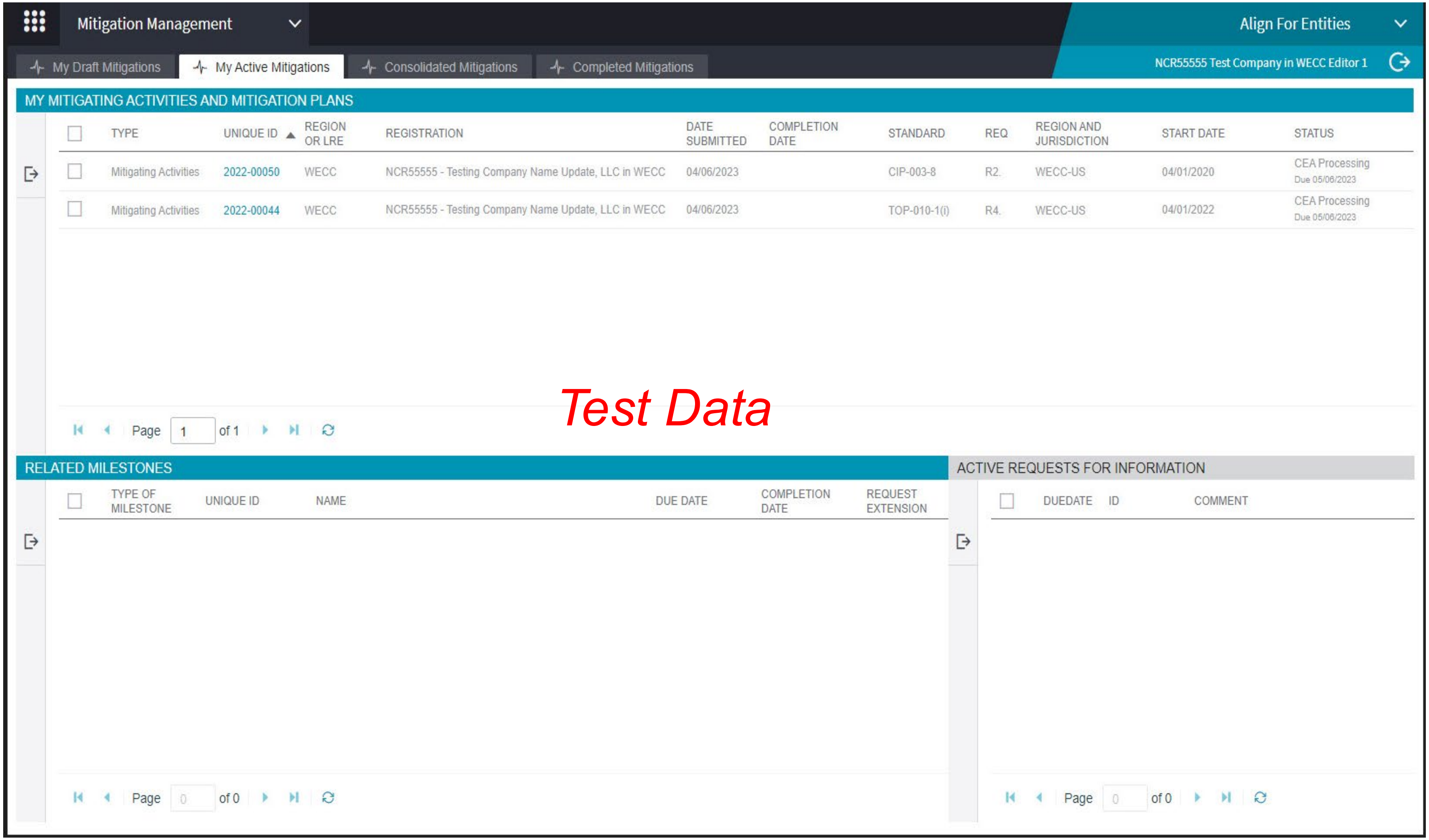


MY OPEN FINDINGS

□	MONITORING METHOD	UNIQUE ID	REGION OR LRE	DATE SUBMITTED	REGISTRATION	STANDARD	REQ	START DATE	FINDING STATUS	SEND UPDATE	MITIGATION
□	Self-Certification	2022-00050	WECC	05/06/2022	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R2.	04/01/2020	PNC Review	+	Mitigating Activities Draft
□	Self-Report	2022-00044	WECC	04/12/2022	NCR55555 - Testing Company Name Update, LLC in WECC	TOP-010-1(i)	R4.	04/01/2022	PNC Review	+	Mitigating Activities Draft
□	Self-Report	2022-00025	WECC	03/04/2022	NCR55555 - Testing Company Name Update, LLC in WECC	BAL-002-3	R3.	03/04/2022	Enforcement Processing	+	Mitigating Activities Draft
□	Self-Certification	2022-00012	WECC	02/17/2022	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R2.	02/17/2022	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00617	WECC	07/21/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-009-6	R2.	07/21/2021	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00609	WECC	07/13/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R3.	07/13/2021	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00604	WECC	07/08/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R1.	07/08/2021	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00603	WECC	07/07/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R4.	07/07/2021	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00602	WECC	07/07/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R4.	07/07/2021	PNC Review	+	Mitigating Activities Draft
□	Self-Certification	2021-00601	WECC	07/02/2021	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R2.	07/02/2021	PNC Review	+	Mitigating Activities Draft

Test Data

Entity – Active Mitigations



MY MITIGATING ACTIVITIES AND MITIGATION PLANS

□	TYPE	UNIQUE ID ▲	REGION OR LRE	REGISTRATION	DATE SUBMITTED	COMPLETION DATE	STANDARD	REQ	REGION AND JURISDICTION	START DATE	STATUS
□	Mitigating Activities	2022-00050	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	04/06/2023		CIP-003-8	R2.	WECC-US	04/01/2020	CEA Processing Due 05/06/2023
□	Mitigating Activities	2022-00044	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	04/06/2023		TOP-010-1(i)	R4.	WECC-US	04/01/2022	CEA Processing Due 05/06/2023

Page 1 of 1

Test Data

RELATED MILESTONES

□	TYPE OF MILESTONE	UNIQUE ID	NAME	DUE DATE	COMPLETION DATE	REQUEST EXTENSION

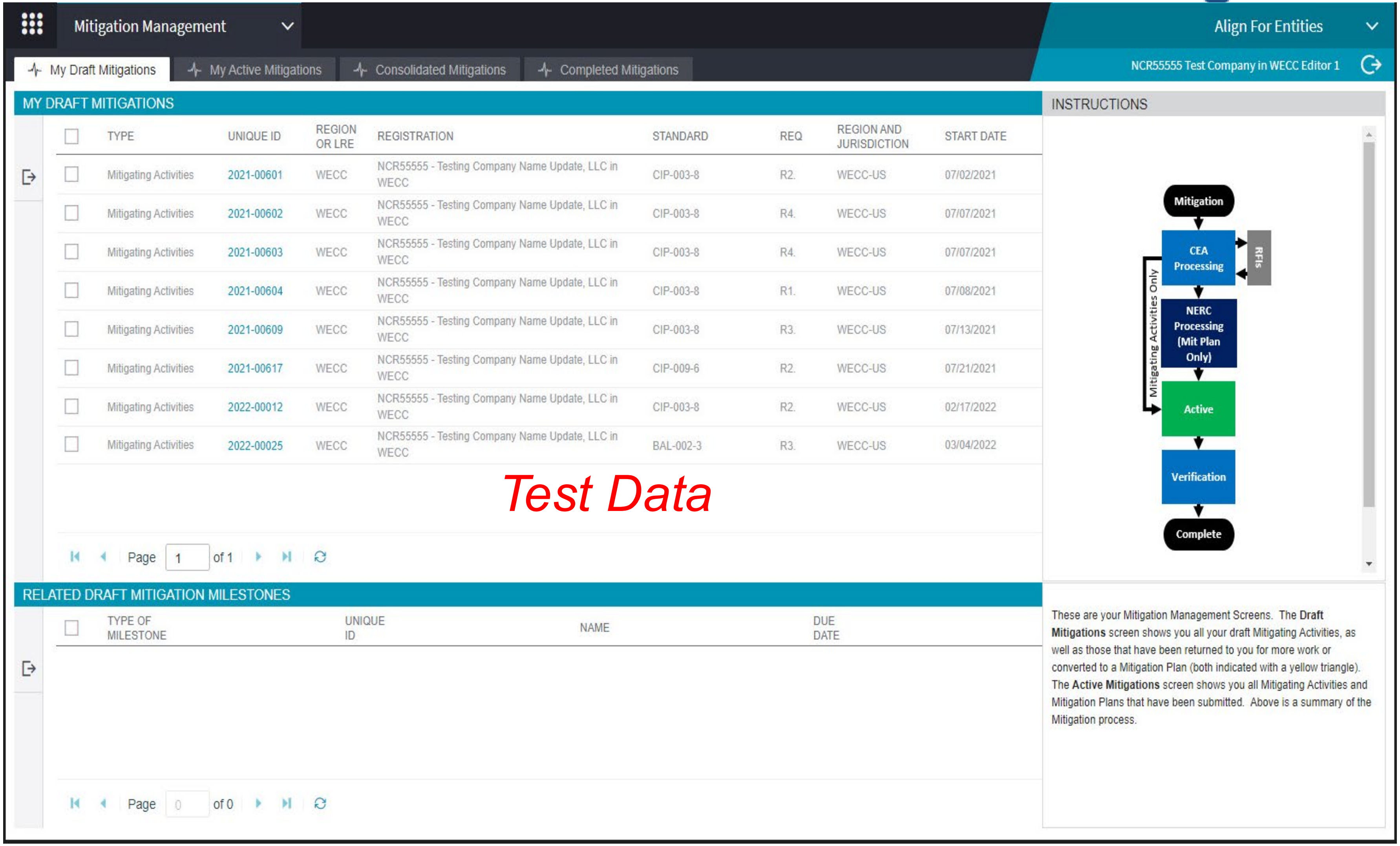
Page 0 of 0

ACTIVE REQUESTS FOR INFORMATION

□	DUEDATE	ID	COMMENT

Page 0 of 0

Entity – Draft Mitigations



MY DRAFT MITIGATIONS

□	TYPE	UNIQUE ID	REGION OR LRE	REGISTRATION	STANDARD	REQ	REGION AND JURISDICTION	START DATE
□	Mitigating Activities	2021-00601	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R2.	WECC-US	07/02/2021
□	Mitigating Activities	2021-00602	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R4.	WECC-US	07/07/2021
□	Mitigating Activities	2021-00603	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R4.	WECC-US	07/07/2021
□	Mitigating Activities	2021-00604	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R1.	WECC-US	07/08/2021
□	Mitigating Activities	2021-00609	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R3.	WECC-US	07/13/2021
□	Mitigating Activities	2021-00617	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-009-6	R2.	WECC-US	07/21/2021
□	Mitigating Activities	2022-00012	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	CIP-003-8	R2.	WECC-US	02/17/2022
□	Mitigating Activities	2022-00025	WECC	NCR55555 - Testing Company Name Update, LLC in WECC	BAL-002-3	R3.	WECC-US	03/04/2022

Test Data

Page 1 of 1

RELATED DRAFT MITIGATION MILESTONES

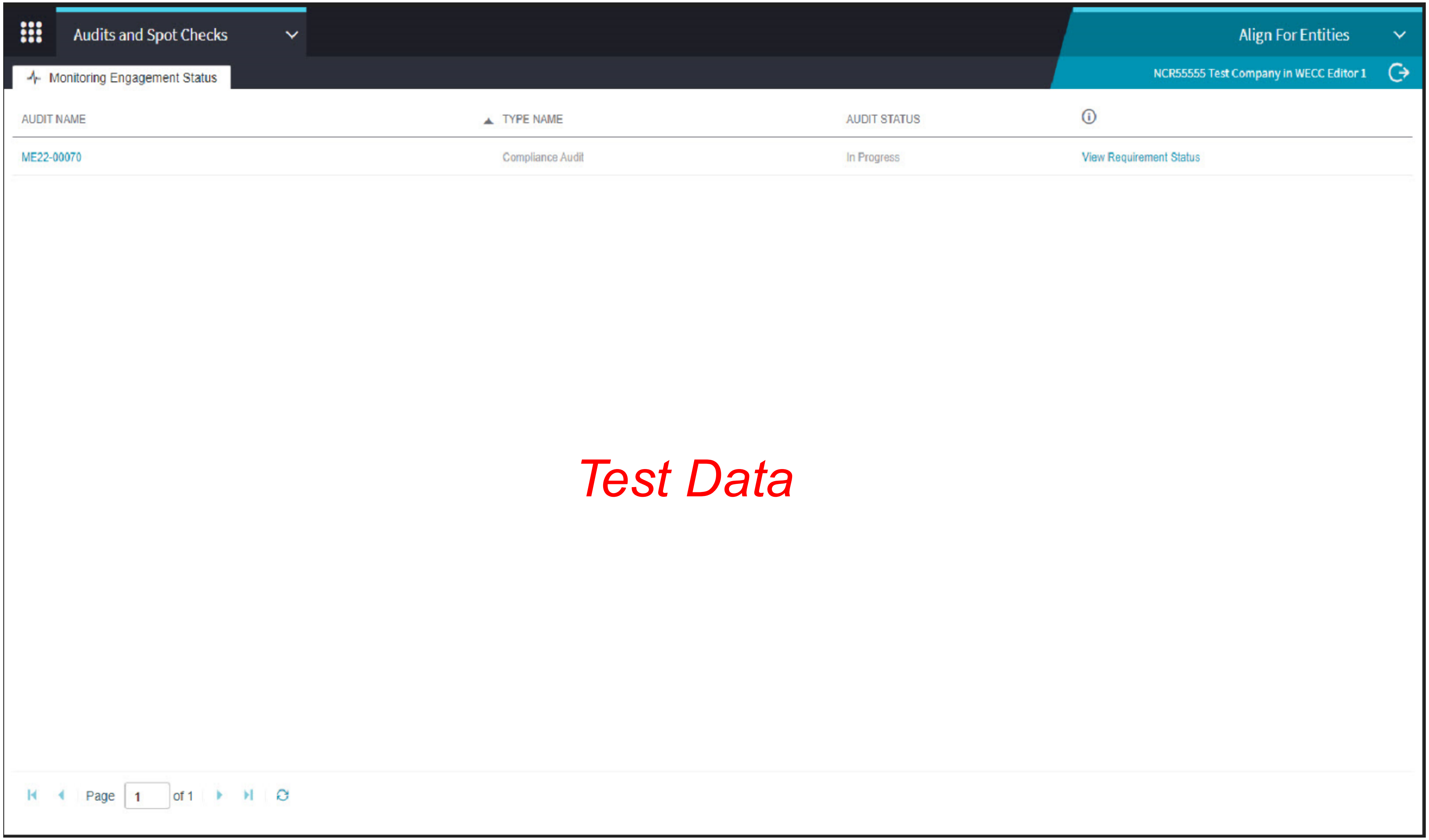
□	TYPE OF MILESTONE	UNIQUE ID	NAME	DUE DATE

Page 0 of 0

INSTRUCTIONS

These are your Mitigation Management Screens. The **Draft Mitigations** screen shows you all your draft Mitigating Activities, as well as those that have been returned to you for more work or converted to a Mitigation Plan (both indicated with a yellow triangle). The **Active Mitigations** screen shows you all Mitigating Activities and Mitigation Plans that have been submitted. Above is a summary of the Mitigation process.

Entity – Active Engagements


Audits and Spot Checks
Align For Entities
Monitoring Engagement Status
NCR55555 Test Company in WECC Editor 1
Page 1 of 1

AUDIT NAME	TYPE NAME	AUDIT STATUS	ⓘ
ME22-00070	Compliance Audit	In Progress	View Requirement Status

Test Data

Infrastructure Services Team

Infrastructure

FTE **Angus Willis**
Director, Infrastructure

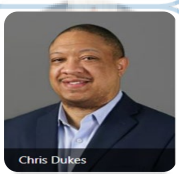
FTE **Michael Si**
Principal, System Admin

C **Mack Marchand**
System Architect

FTE **Melinda Nicius**
Sr. Database Admin

FTE **Dung Nguyen**
System Admin

FTE **Chris Dukes**
Sr. System Admin



Network

FTE **Terence Lockette**
Sr. Network Engineer

Quality Assurance

FTE **Aviance Clay**
Manager, Quality Assurance

C **David Jones**
Quality Assurance, Testing

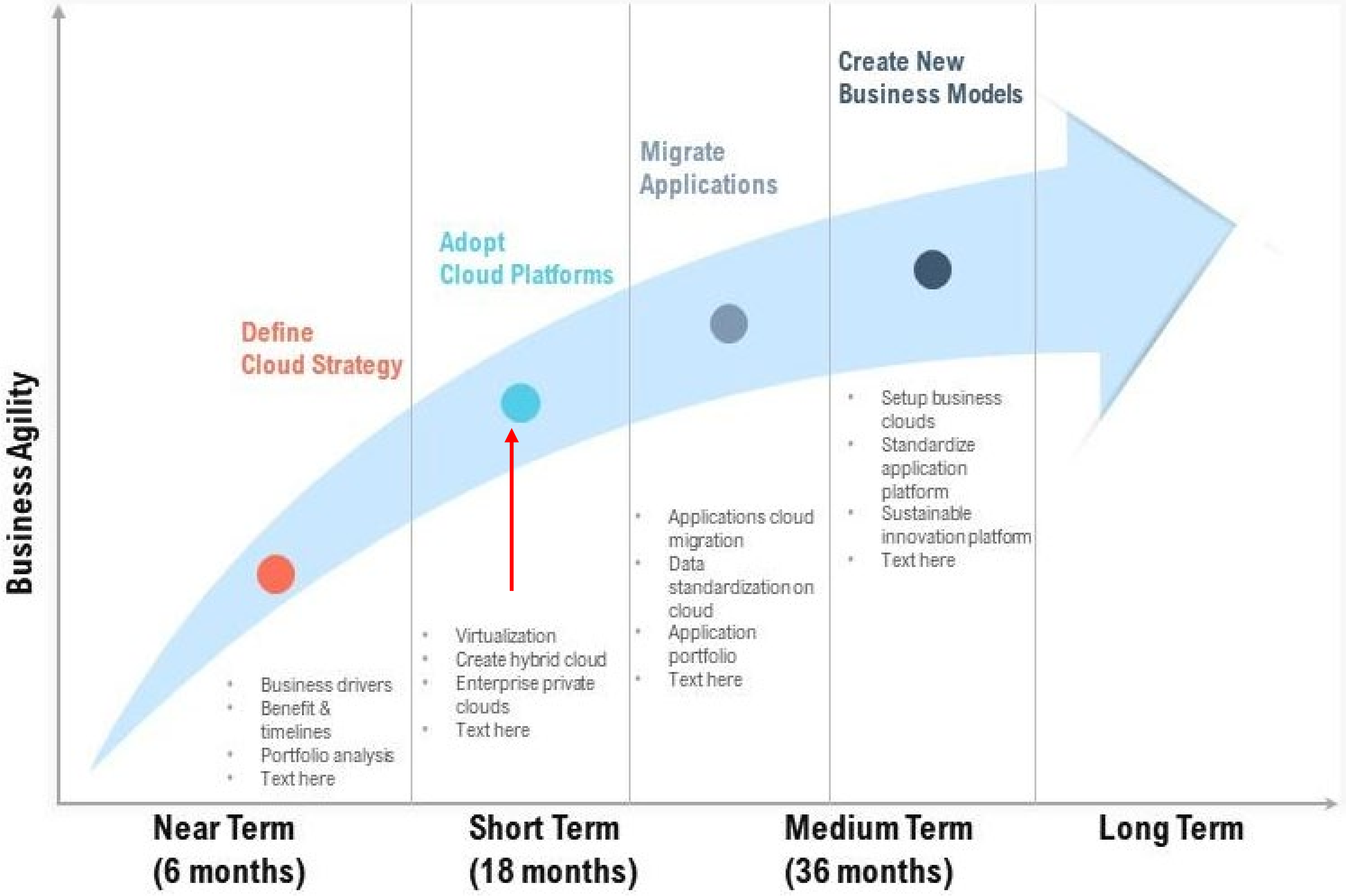
C **Theo Henton**
Quality Assurance, Testing

C **Robert Pugh**
Infrastructure Patching

Cloud Adoption Strategy

- Business Challenges and Drivers
- Cost-Efficiencies
- Risk Reduction through improved reliability, increased performance, enhanced security
- Faster Implementation Cycles
- Promotes Scalability
- Upgrades and Maintenance
- Enhanced Security through cloud platform interoperability for XDR (Extended Detection and Response) cyber events

Where are we?



- Business drivers
- Benefit & timelines
- Portfolio analysis
- Text here

- Virtualization
- Create hybrid cloud
- Enterprise private clouds
- Text here

- Applications cloud migration
- Data standardization on cloud
- Application portfolio
- Text here

- Setup business clouds
- Standardize application platform
- Sustainable innovation platform
- Text here

Journey to the Cloud - Completed

- MS Exchange and Outlook
- NERC.com
- EasyVista (trouble and request management system)
- Mobile Device Management
- Microsoft InTune End Point Device Management
- Microsoft Infrastructure Security Patching

Journey to the Cloud - Planned

- Office 365 Productivity Applications
- SharePoint
- Microsoft Dynamics – Application Platform (2024)
- ERO Enterprise Portal – Application Access (2024)
- Microsoft Purview Data Loss Prevention (DLP)
- Microsoft TEAMS Phone Calling

Questions and Answers