



## E-ISAC Update

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

Matthew Duncan, Director of Intelligence, NERC

Laura Brown, Director, E-ISAC Strategy, Policy, and Programs, NERC

Technology and Security Committee Open Meeting

May 11, 2022

**TLP:WHITE**

**RELIABILITY | RESILIENCE | SECURITY**



A DIVISION OF NERC



# E-ISAC

ELECTRICITY  
INFORMATION SHARING AND ANALYSIS CENTER

# Security Threat Landscape

Matthew Duncan, Director, Intelligence  
Technology and Security Committee Open Meeting  
May 11, 2022

**TLP:WHITE**

**RELIABILITY | RESILIENCE | SECURITY**





# SHIELDS UP



- Potential Risks to Industry
- Latest Industrial Control System (ICS) Threats
- Additional Russian Cyber Threats
- Russian Physical Security Threats
- Other Geopolitical Threats
- Physical Security Threat Landscape
- Collective Defense



**JOINT  
CYBERSECURITY  
ADVISORY**

Co-Authored by:

**TLP:WHITE** Product ID: AA22-011A  
January 11, 2022



Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

- **2022 U.S. Annual Threat Assessment - Russia**
  - “Russia views cyber disruptions as a foreign policy lever to shape other countries’ decisions, as well as a deterrence and military tool.”
  - Mis- and Disinformation
  - Attacks against critical infrastructure
- Previous Russian activity against industrial control systems (ICS) and operational technology (OT)



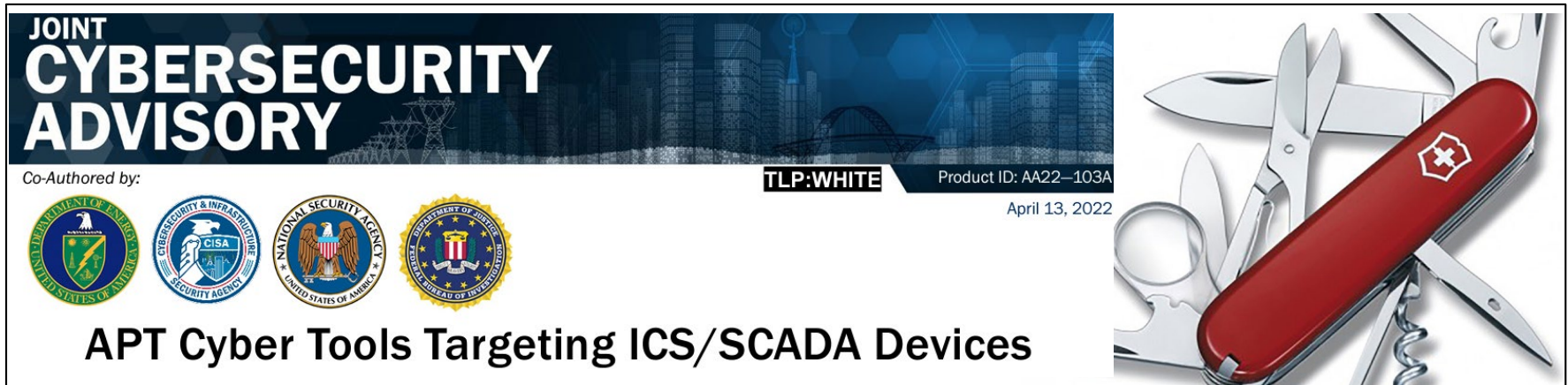
# Industroyer2: Industroyer reloaded

This ICS-capable malware targets a Ukrainian energy company

**(e)::r** ESET Research





**CERT-UA**  
Computer Emergency Response Team of Ukraine

- High Confidence attribution to **Sandworm (Russian GRU)** by ESET
  - Targets IEC-104 protocol (*North American ICS mostly use DNP3*)
  - Attack used ICS-capable malware and disk wipers
  - Destructive actions scheduled for April 8
  - Campaign interrupted, no outages reported
- No Industroyer2 activity observed in North America



**JOINT  
CYBERSECURITY  
ADVISORY**

Co-Authored by:

**APT Cyber Tools Targeting ICS/SCADA Devices**

**TLP:WHITE** Product ID: AA22-103A  
April 13, 2022

- **PIPEDREAM (DRAGOS)/INCONTROLLER (MANDIANT) Tool**
  - ‘Swiss Army Knife’ that automates exploits against ICS devices
- Mitigations
  - Ensure ICS visibility and threat detection
  - Maintain knowledge and control of all assets in OT
  - Additional research and sharing needed

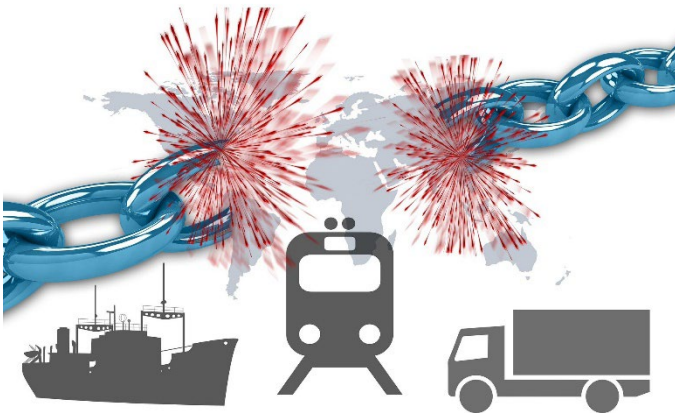


- **Destructive Malwares observed in Ukraine**
  - CADDYWIPER, WhisperGate, HermeticWiper, IsaacWiper
  - No reports to E-ISAC of this activity in North America
- **European Wind Turbine cyber related events – no outages**
  - Satellite communications disruption of Enercon wind turbines (Viasat)
  - Nordex
  - Deutsche Windtechnik
- **Uninterruptible Power Supplies (UPS) Targeting**





- **Russia/Ukraine Crisis** - Monitoring events that could create physical security threats/impacts to the grid, including:
  - Supply chain and economic disruptions; increased threat risk.
  - Online chatter discussing the sabotage of electrical infrastructure in Ukraine to inspire/mobilize domestic violent extremists to target the grid.







### *China*

- “Broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks.” (*2022 Annual Threat Assessment*)
- Diversity of tradecraft and toolsets and improved operational techniques
- Ongoing espionage campaign blending zero-day and Log4Shell exploits against U.S. state government networks



### *Iran*

- MuddyWater conducting cyber espionage, targeting government and private-sector across sectors (telecoms, government, & oil and natural gas)



### **Ransomware**

- Rapid exploitation of vulnerabilities, phishing, and credential harvesting
- Gangs developing code designed to stop industrial processes (*FBI*)

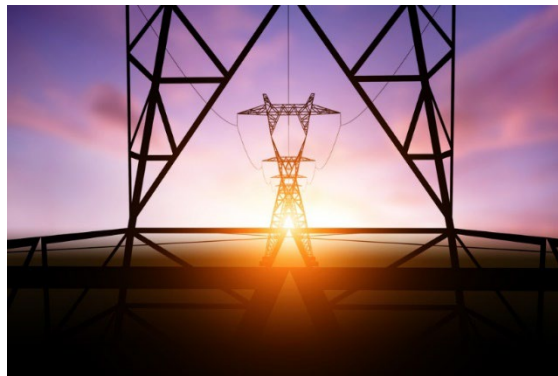


- **Domestic violent extremists** - Frequent extremist online chatter discussing the targeting of electricity
- **Drones** - Ongoing and emerging threat to electrical assets due to evolving technology, threat actor interest and increasing commercial use.
- **Activism** - Continued opposition to industry, especially to new construction, pipelines, and fossil fuel plants, which can include sabotage and destruction.
- **Insider Threat** - Continued concerns over an Insider Threat using cyber and physical attack vectors.





- Energy Threat Analysis Center (ETAC) and Joint Cyber Defense Collaborative (JCDC) participation
- Active CRISP community engagement
- Small/Medium Utility Weekly Report
- Coordination with ERO, including Reliability Coordinators
- Engagement of the Electricity Subsector Coordinating Council (ESCC), Physical Security Advisory Group (PSAG) and new Cyber Security Advisory Group (CSAG)



A stylized map of North America is shown in shades of blue and grey. A solid blue horizontal band runs across the middle of the map, serving as a background for the title text.

## Questions and Answers



# GridEx VI Findings and Recommendations

Laura Brown, Director, E-ISAC Strategy, Policy, and Programs, NERC  
Technology and Security Committee Open Meeting  
May 11, 2022

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY





- Distributed Play (E-ISAC members and partners)
  - Audience: E-ISAC members and partners, to include electricity industry, government agencies, other relevant organizations
  - Goal: exercise emergency response and recovery plans in response to simulated cyber and physical security attacks and other contingencies affecting North America's electricity system
- Executive Tabletop (invitation only)
  - Audience: industry and government executives from the ESCC, EGCC, and impacted entities
  - Goal: highlight the extraordinary operational measures necessary in response to severe combined cyber and physical attacks



- Scenario impacted North American west coast
- Conducted virtually
- Key themes:
  - Operational coordination with Telecommunications and Gas
  - Shared consensus on use of Grid Security Emergency Orders
  - Security of inverter-based resources
  - Narrative warfare/misinformation, disinformation
- Lessons learned report published April 7



- **Continue to build effective communications procedures and systems to share operational and security information**
  - The sector needs to enhance processes and procedures around communications roles and responsibilities
  - The sector needs to reach greater mutual understanding of what information would be shared and how it will be shared during a crisis
- **Key players to address the recommendations:**
  - Industry (NERC, NERC members, the ESCC)
  - Government (DOE)



- **Clarify the differing crisis communications roles of the Electricity Subsector Coordinating Council and Reliability Coordinators (RC) with government and their members, including Canadian members**
  - RCs and utilities would be responsible for ensuring timely and effective communication and action
- **Key players to address the recommendation:**
  - Industry (RCs, utilities, the ESCC)
  - Government (U.S. and Canada, federal, provincial, local)



- **Continue to enhance routine and emergency operations coordination between the electricity industry and natural gas providers**
  - Establish a joint working group to consider the impact of natural gas supply shortfalls on electricity generation through a range of scenarios, including the impact to resilience from a single energy source net-zero policy
- **Key players to address the recommendation:**
  - Industry (ESCC, Oil and Natural Gas SCC)



- **Strengthen operational coordination between the electricity industry and communications providers**
  - Consider technical alternatives in case of telecommunications disruptions
  - Identify telecommunications needs for the electricity sector
  - Coordinate with the communications sector to identify alternate capabilities/solutions to address those needs
- **Key players to address the recommendations:**
  - Industry (ESCC, Telecommunications Sector)
  - Government



- **Continue to reinforce government relationships between United States and Canada to support industry response**
  - The participation of senior Canadian federal and provincial officials reflected the cross-border scope of the scenario. Participants gained a better understanding of the roles of Canada's provincial and federal governments during a grid emergency and how they differ from those of their U.S. counterparts.
- **Key players to address the recommendations:**
  - Government

- GridEx VI Recommendations Action Plan
  - Identify organizations, individuals, timelines
  - Track progress leading up to GridEx VII
- GridEx VII
  - Identify volunteer subject matter experts in coming months
  - Apply lessons learned from GridEx VI

A stylized map of North America, including the United States, southern Canada, and northern Mexico. The map is rendered in shades of blue and grey. A solid blue horizontal band crosses the middle of the map, serving as a background for the title text.

## Questions and Answers

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# ERO Enterprise Align Project

Stan Hoptroff, Vice President, Business Technology

Lonnie Ratliff, Senior Manager, Cyber and Physical Security Assurance

Technology and Security Committee Open Meeting

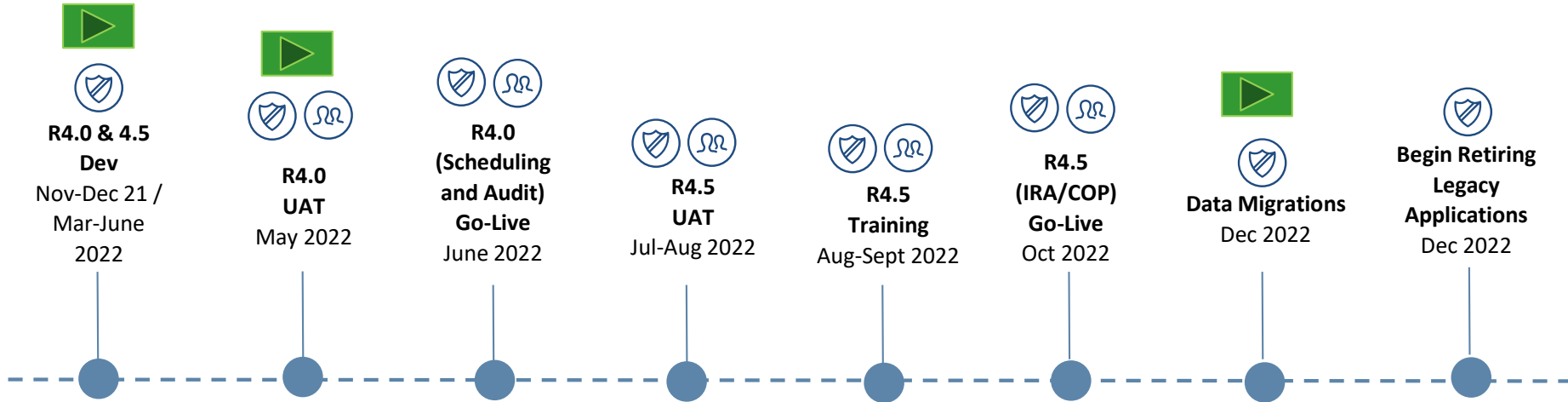
May 11, 2022

**RELIABILITY | RESILIENCE | SECURITY**



- Align Project Timeline
- Align Release 3 Functionality
- Align Release 4 and 4.5 Functionality
- Canadian Update
- Current Challenges
- How to Stay Informed





**AUDIENCE IMPACT KEY**

Registered Entities	ERO Enterprise Staff

*In progress*

*Complete*

- Audit Scope
- Audit Notification Package
  - Audit Notification Letter
  - Pre-Audit survey
- Compliance Monitoring and Enforcement Program (CMEP) Staff Working Papers
  - Secure Evidence Locker Reference Number
  - Auditor/Enforcement Staff Notes
- Regional Notes
  - Compliance Culture
- Findings Created
  - Potential Noncompliances, Areas of Concern, and Recommendations
- Audit Report Generation

- Enhancements
  - Audit
  - Scheduling
- Registered Entity Inherent Risk Assessment
- Compliance Oversight Plan

IRA and COP		Align for Regions						
IRA Status		IRA CO	Compliance Oversight Plan	Compliance Oversight Plan CO	Risk Factors	Risk Elements	ERP Questionnaire Library	
ENTITY NAME	CO GROUP	LRE/ARE	CREATE NEW / OPEN IRA	IRA STATUS	QUESTIONNAIRE STATUS	DUE DATE IRA REFRESH	LATEST IRA FINALIZATION DATE	
NCR00082 - Plains End II, LLC in WECC		LRE	<a href="#">Open IRA</a>	In Progress	Questionnaire submitted for CEA Review			
NCR00086 - Boise-Kuna Irrigation District in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire Sent to Entity	04/06/2022		
NCR00125 - DGC Operations, LLC in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire not created			
NCR00209 - Energy Northwest - Columbia in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire not created			
NCR00250 - Energy Northwest - Energy/Business Services in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire not created			
NCR00254 - Colorado Energy Management - BIV in WECC		LRE	<a href="#">Open IRA</a>	Initiated	Questionnaire Sent to Entity			
NCR00257 - NaturEner Power Watch, LLC in WECC		LRE	<a href="#">Open IRA</a>	Initiated	Questionnaire not created			
NCR00296 - Colorado Energy Management - CPP in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire not created			
NCR00339 - Colorado Energy Management - RMP in WECC		LRE	<a href="#">Open IRA</a>	Initiated	Questionnaire not created			
NCR00377 - Nevada Gold Energy LLC in WECC		LRE	<a href="#">Open IRA</a>	CEA Approval	Questionnaire Sent to Entity			
NCR00418 - NAES Corporation - White Creek Wind 1 in WECC		LRE	<a href="#">View IRA</a> +	Complete	Questionnaire not created			
NCR00769 - Clearway Energy Operating, LLC in WECC		LRE	<a href="#">Open IRA</a>	CEA Review	Questionnaire not created			
NCR01143 - Southwest Power Pool, Inc. in WECC		LRE	<a href="#">Open IRA</a> <a href="#">View IRA</a>	Initiated	Questionnaire not created			

TEST DATA

IRA and COP						Align for Regions
IRA Status	IRA CO	Compliance Oversight Plan	Compliance Oversight Plan CO	Risk Factors	Risk Elements	ERP Questionnaire Library
ENTITY NAME	COG GROUP	LRE/ARE	CREATE / EDIT COP	COP STATUS	LATEST COP FINALIZATION DATE	
NCR00082 - Plains End II, LLC in WECC		LRE	Open COP	Complete	03/29/2022	
NCR00086 - Boise-Kuna Irrigation District in WECC		LRE	Open COP	CEA Approval		
NCR00086 - Boise-Kuna Irrigation District in WECC		LRE	Open COP	CEA Review		
NCR00086 - Boise-Kuna Irrigation District in WECC		LRE	Open COP	CEA Approval		
NCR00086 - Boise-Kuna Irrigation District in WECC		LRE	Open COP	CEA Review		
NCR00125 - DGC Operations, LLC in WECC		LRE	Open COP	CEA Review		
NCR00209 - Energy Northwest - Columbia in WECC		LRE	Open COP	CEA Approval		
NCR00250 - Energy Northwest - Energy/Business Services in WECC		LRE	Open COP	Complete	03/29/2022	
NCR00254 - Colorado Energy Management - BIV in WECC		LRE	Open COP	Initiated		
NCR00257 - NaturEner Power Watch, LLC in WECC		LRE	Open COP	CEA Review		
NCR00296 - Colorado Energy Management - CPP in WECC		LRE	Open C			
NCR00339 - Colorado Energy Management - RMP in WECC		LRE	+			
NCR00377 - Nevada Gold Energy LLC in WECC		LRE	Open COP	Initiated		

TEST DATA

Click to edit the COP

IRA Management

Maintain Risk Factors | Maintain Risk Elements | IRA - Risk Factor Questionnaire Library

Select Function | Select CEA | Search...

NAME	RISK FACTOR LANGUAGE ↑	CEA	FUNCTIONS
⚠ Balancing Authority (BA) Coordination	⚠		🔗 BA, RSG
⚠ CIP - Impact Rating Criteria	⚠		🔗 BA, DP, GO, GOP, RC, TO,
⚠ Critical Transmission	⚠	📄 FRCC, MRO, NCEA, NERC, NPCC, RF, SERC, SPPRE, TXRE,	🔗 BA, PCPA, RC, TO, TOP, T
⚠ ICCP Connectivity	⚠	📄 FRCC, MRO, NCEA	🔗 BA, GO, GOP, RC, TO, TOI
⚠ Largest Generation Facility	⚠		🔗 GO, GOP
⚠ Load	⚠		🔗 DP, TO, TSP
⚠ Planned Facilities	⚠		🔗 GO, RP, TO, TP
⚠ RAS/SPS	⚠		🔗 DP, GO, RC, TO, TOP
⚠ Situational Awareness and	⚠		🔗 BA, DP, GO, GOP, LSE, RC

Rows per page: 25

TEST DATA

- Determined level of effort for most requirements
- Created draft project schedule for implementing all provinces with BASE functionality
  - Manitoba & Saskatchewan (MRO) – September 2022
  - Alberta & British Columbia (WECC) – November 2022
  - Nova Scotia (NPCC) –Q1 2023

- **Project Fatigue:** Maintaining team and stakeholder engagement on a multi-year project
- **People:** Parallel efforts with the support of R1-R3 with R4 development/QA, data migration and Canada
- **Technical:** Finding the right balance between our unique business needs and the platform (extensions and future upgrades)
- **Cost Management:** Balancing available funds and business requirements (enhancements) and R4 business complexity



## 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

# **Align Team Members Across the ERO**

Standards & Engineering	Enforcement	Registration	Compliance Assurance	Legal, Internal Audit	Policy & External Affairs
Soo Jim Kim	Sonia Mendonca	Jim Stuart	Mechelle Thomas	Tina Buzzard	Janet Sena
Latrice Harkness	Teri Stasko	Ryan Stewart	Tiffany Whaley	Monica Bales	Kimberly Mielcarek
Kimberlin Harris	Sara Minges	Kevin Koloini	Lonnie Ratliff	Shamai Elstein	Michelle Marx
Nasheema Santos	Simran Ahuja	Chris Scheetz	Jamie Calderon	Stefan Bergere	Amy Klagholz
Cindy Jackson	Farzaneh Tafreshi	Steve Masse	Jeremy Withers	Nina Jenkins-Johnston	Kristin Iwanechko
Linda Jenkins	Kaiesha Morgan		Heather Miller	Ed Kichline	Katie Cain
Levetra Pitts	Farzaneh Tafreshi		Daniel Bogle	Kristin Miller	Hugo Perez
			Kiel Lyons		
			Craig Struck		
			Yvette Landin		
			Fahad Ansari		

MRO		NPCC	SERC	
Sara Patrick	Jeff Norman	Damase Herbert	Andrew Williamson	Mike Kuhl
Desiree Sawyer	Tasha Ward	Dan Kidney	Janice Carney	Teresa Glaze
Marissa Falco	Ken Gartner	Duong Le	Melinda Montgomery	Carlos Valiente
Julie Sikes	Richard Burt	Jason Wang	Todd Curl	Rafael Lerdo
Michael Taube		Kimberly Griffith	Rick Dodd	Lou Stramaglio
Rob Quinlan		Michael Bilheimer	Serge Beauzile	Tim Ponseti
Jeremy Mattke		Michael Stuetzle	Clay Shropshire	Kenneth Lindler
Adam Flink		Jacqueline Jimenez	Robert Vaughn	
Richard Samec		Ben Eng	Kevin Spontak	
Ryan McNamara		Jennifer Wallace Farrell	Estella Wingfield	
William Steiner		Mina Ellis	Shawna Speer	
Janice Anderson		Aaron Hornick	Stephen Brown	
Michael Spangenberg		Faisal Nahian	Nick DePompei	
Jess Syring		Scott Nied	Ravindra Dasappa	

RF	TRE		WECC	
Jeff Craigo	Jim Albright	Sridhar Pushpavanam	Jillian Lesser	Steve Goodwill
Zack Brinkman	Dennis Glass	Tammy Thomas	Mailee Cook	Tom Williams
George Spila	Devin Kitchens	Brook Rodaway	Michael Dalebout	Mark Rogers
Mark Kidney	Ben Gregson	Derrick Davis	Ruchi Shaw	Trent Wilson
Dionne Kuykendall	Erick Newnam	Keith Smith	Tom Golson	Tyler Whiting
Dirk A. Baker	Jeff Hargis	Machelle Castro	Angie Shapiro	Aldo Nevarez
Anthony Jablonski	Curtis Crews	JW Richards	Jessica King	Barry Bauer
Bob Folt	John Horishny	Rochelle Brown	Holly Peterson	John Graminski
Shawn Barrett	Eryn Lorcher	Joseph Younger	Phil O'Donnell	Julie Blair
Matt Thomas	Kenath Carver		Brittany Crosby	Deb McEndaffer
Patrick O'Connor	AJ Smullen		Kevin Paletskih	Kim Israelsson
Ron Ross	Rachel Coyne		Heather Laws	Duane Cook
Bob Yates			Ben Aldous	Mike Connelly
Kristen Senk			Steve Noess	
Jim Kubrak				
Shawn Liggett				

Information Technology			Finance	HR, Facilities, Training
Andy Rodriguez	Stan Hoptroff	LaCreacia Smith	Meg Leonard	Jeff Shade
Brenton Matthews	Jeffrey Travis	Marvin Santerfeit	Autumn Diaz	Emma Agola
Dan Chanda	Daniel Frank	Dan Nagar	Erika Chanzas	George Rankin
Victor Myers	Aviance Clay	Hasan Zulfiqur	Andy Sharp	Wanda Peoples
Jeremy Bryant	Jeff Hicks	Don Prince	Erin Carter	Emma Marvil
Maria De Souza	Ed Hodge	Terence Lockette	Anya Josephson	Lisa Ellis
Griffin Cologne	Chris Dukes	Trevor Davis	Jane Hughes	
Suzanne Smith-Wigfall	Michael Si	David Jones		
Melinda Nicius	Dung Nguyen	Keneal Bygrave		
Dee Humphries	Dan Hazelwood	Rebekah Clemons		
Justin Lofquist	Robert Myers			



# Questions and Answers

Moving to a common platform has provided:

- **A more secure** method of managing and storing 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



# **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 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

### 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

## 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

## 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