

# WELCOME TO TECHNICAL TALK WITH RF

*Cybersecurity Awareness Month*

October 23, 2023



# TECHNICAL TALK WITH RF



Join the conversation at

[SLIDO.com](https://www.slido.com)

[#TechTalkRF](https://twitter.com/TechTalkRF)

# TECHNICAL TALK WITH RF

Follow us on



[Linkedin.com/company/reliabilityfirst-corporation](https://www.linkedin.com/company/reliabilityfirst-corporation)

A screenshot of the ReliabilityFirst Corporation LinkedIn profile. The header features a banner image of power lines against a sunset sky. The profile name is "ReliabilityFirst Corporation" with a notification bell icon. Below the name, it states "RF works to maintain the reliability, security and resilience of the electric grid in the Mid-Atlantic region" and "Utilities · Cleveland, OH · 3,970 followers · 101 employees". A section indicates "Brian & 85 other connections work here" with buttons for "Following", "Invite", and "More". Navigation tabs include "Home", "My Company", "About", "Posts", "Jobs", and "People". The "Posts" tab is active, showing a post from "ReliabilityFirst Corporation" (3,970 followers, 2d) with the text: "ReliabilityFirst staff participated in our organization's annual Day of Giving last week. Thank you to [BOYS & GIRLS CLUB OF CLEVELAND](#), [Providence House](#), [Shoes and Clothes for Kids](#), [Arkansas Foodbank](#), and [City Mission](#) for having us as w...see more". The post includes two images: a group photo of staff in front of a building and a photo of a roof being worked on.

# TECH TALK REMINDERS

Please keep your information up-to-date

- CORES, Generation Verification Forms, Entity Profile Questionnaires (quarterly)

Following an event, send EOP-004 or OE-417 forms to [disturbance@rfirst.org](mailto:disturbance@rfirst.org)

CIP-008-6 incident reports are sent to the [E-ISAC](#) and the [DHS CISA](#)

Check our [monthly CMEP update](#) and [quarterly newsletter](#):

- [2023 ERO Periodic Data Submittal schedule](#)
- Timing of Standard effectiveness

BES Cyber System Categorization (CIP-002-5.1 a)

- Assess categorization (low, medium, or high) regularly and notify us of changes

CIP Evidence Request Tool V7.0 is online, see [website](#)



# WELCOME TO TECHNICAL TALK WITH RF

*Cybersecurity Awareness Month*

October 23, 2023

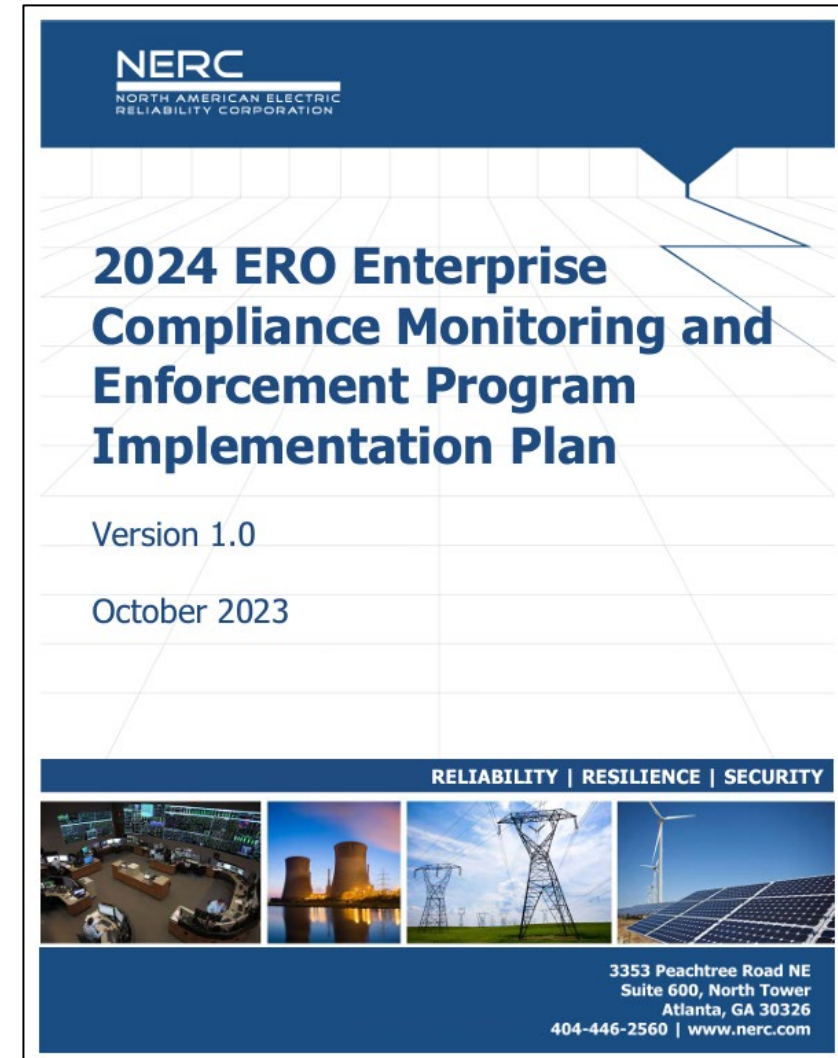


# TECH TALK ANNOUNCEMENT



## 2024 Compliance Monitoring and Enforcement Program Implementation Plan (CMEP IP)

The ERO Enterprise is pleased to release the [2024 CMEP IP](#) describing the risks that will be priorities for the ERO Enterprise's CMEP activities in 2024. The changes include a new physical security risk element, and the expansion of the cold weather risk element to extreme weather, which includes both hot weather and space weather events.



# TECH TALK ANNOUNCEMENT



## **RF Regional Standard BAL-502-RF-03**

### **Posted for Five-Year Review**

Comment Period: October 9 – November 7

Per the ReliabilityFirst Reliability Standards Development Procedure (Maintenance of Regional Reliability Standards section), the Standards Committee shall ensure that each Standard be reviewed at least once every five years from the effective date of the Standard (BAL-502-RF-03 having an effective date of Jan. 1, 2018). The review process shall be conducted by soliciting comments from the stakeholders. Click [here](#) for details or visit [www.rfirst.org](http://www.rfirst.org).

**[BAL-502-RF-03 Five-Year Review Survey Form](#)**

# TECH TALK ANNOUNCEMENT



**NARUC**  
National Association of Regulatory Utility Commissioners

## NARUC recognizes Cybersecurity Awareness Month for regulators

Lynn Constantini, deputy director at the NARUC Center for Partnerships and Innovation, was interviewed by the National Conference of State Legislatures for a podcast on cybersecurity on October 1<sup>st</sup>. During the podcast, Ms. Constantini discussed ways to safeguard energy systems from attacks, and the role state legislatures play through their oversight of public utility commissioners. Listen [here](#).

## Cybersecurity Awareness Month

This October, help spread awareness on ways to stay safe online.



Cybersecurity serves as a crucial defense against data breaches, identity theft, and various forms of cybercrime. Robust cybersecurity measures are imperative for organizations to safeguard both their valuable data and the trust of their customers.

 <p><b>Password</b></p> <p>Choose a safe password with:</p> <ul style="list-style-type: none"> <li>• At least 12 characters.</li> <li>• A combination of upper and lowercase letters, numbers, punctuation, and special symbols.</li> </ul>	 <p><b>Internet Connection</b></p> <p>Make sure to connect your devices to safe wifi, and use a VPN for protection in addition to a firewall and anti-virus.</p>	 <p><b>Firewalls and Anti-Viruses</b></p> <p>Keep your device's operational system protected from cyberattacks.</p>
 <p><b>Software Updates</b></p> <p>Update your computer and phone's software, as well as your internet browser.</p>	 <p><b>Watch Where You Click</b></p> <p>Check the email addresses that send you links for accuracy.</p>	 <p><b>Multi-Factor Authentication</b></p> <p>Enable this extra layer of protection in your accounts.</p>



# TECH TALK ANNOUNCEMENT

AMERICAN  
**MADE**

U.S. DEPARTMENT OF ENERGY



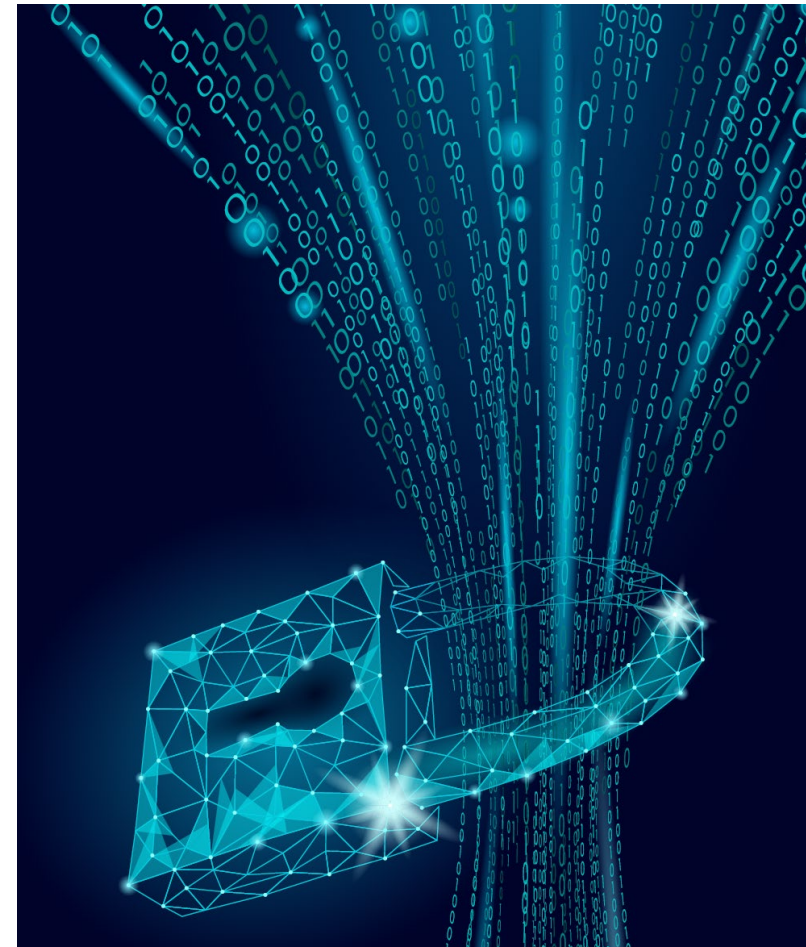
U.S. DEPARTMENT OF  
**ENERGY**

OFFICE OF  
**CYBERSECURITY, ENERGY SECURITY,  
AND EMERGENCY RESPONSE**

## Advanced Cybersecurity Technology (ACT)

The Rural and Municipal Utility Cybersecurity Program launched the [ACT 1 Prize](#) to help electric cooperative, municipal, and small investor-owned utilities protect against, detect, respond to, and recover from cybersecurity threats, and to increase their participation in cybersecurity threat information sharing programs.

Utilities that progress through the competition will receive cash prizes and technical assistance to make meaningful, impactful investments in staff training, governance processes, and cybersecurity tools and technologies. These investments will result in a more secure and resilient energy grid.

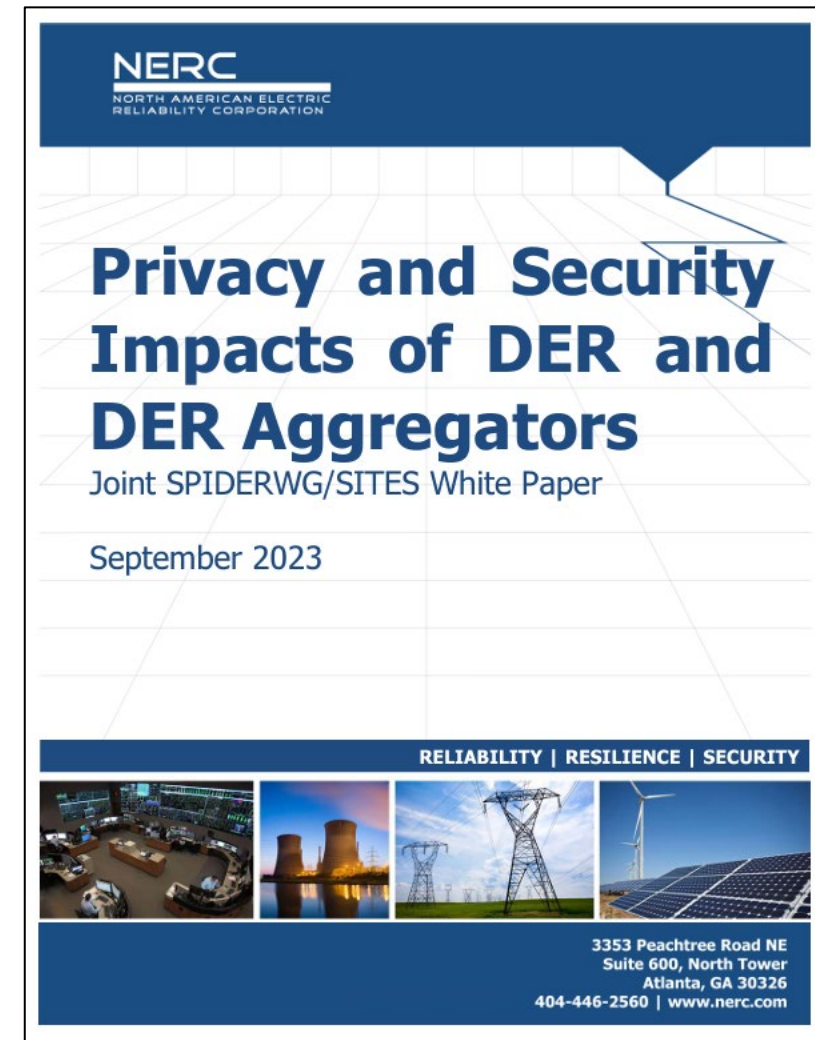


# TECH TALK ANNOUNCEMENT



## RSTC White Paper Approved: Privacy and Security Impacts of DER and DER Aggregators

This [document](#) explores the technical aspects of security controls that are available for Distributed Energy Resources (DERs) and DER aggregators. It includes examples of potential attacks that can be prevented by implementing these security controls. The paper also provides an overview of the security posture for the distribution landscape, with a focus on DERs and DER aggregators, and how it relates to NERC Reliability Standards.



# TECH TALK ANNOUNCEMENT



## Project 2021-03 CIP-002 Webinar

October 30, 12:00 – 3:00 p.m. Eastern

[NERC project page](#)

[Webex link](#)



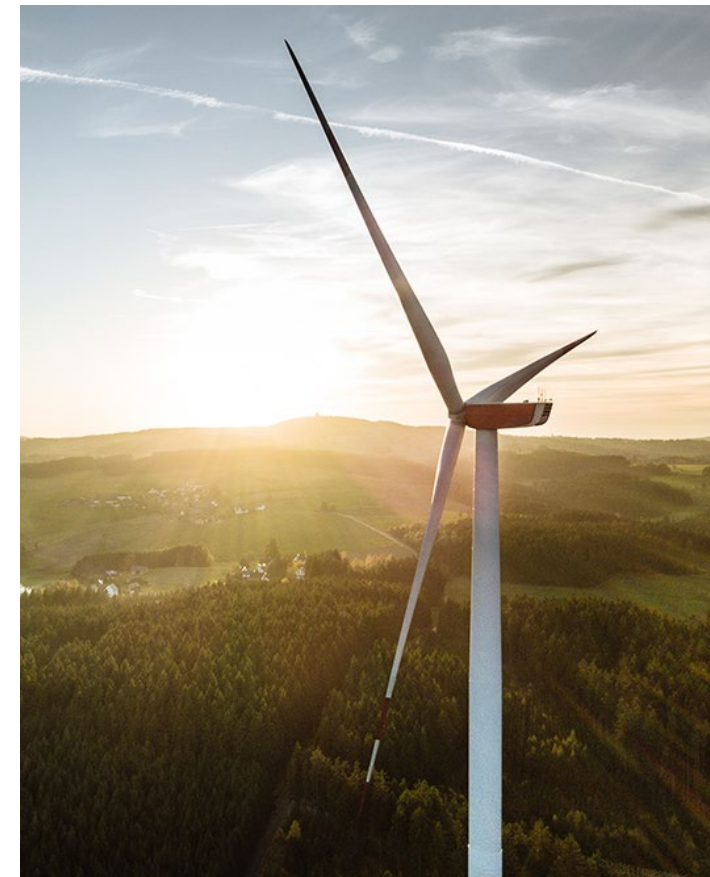
# TECH TALK ANNOUNCEMENT



## NERC-NATF-EPRI Annual Transmission Planning and Modeling Workshop

November 1-2, 1:00 – 5:00 PM Eastern

This year's seminar will focus on bulk power system load modeling, integrated system planning practices, IBR risk mitigation, and updates on the latest research and activities across the industry. [Webinar Flyer](#)



# TECH TALK ANNOUNCEMENT



**NERC**

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION



## **Preparing the Grid for Extreme Cold Weather Events: Lessons Learned and Recommendations from Winter Storm Elliott**

November 2, 2:00 – 3:30 p.m. EST

*What have we learned?*

*How was this event different from past winter storms?*

*What changes should be made to enhance reliability?*

**[Event Details and Registration](#)**



# TECH TALK REMINDER



## GridEx VII

November 14-15

Registration for [GridEx VII](#) is now closed for Lead Planners and Planners. The Master Scenario Events List is now available to all registrants in addition to recordings of all the GridEx VII training webinars. Planners preparing to participate are encouraged to reference the [GridEx VII Planner Recommendations](#) and the [GridEx VII FAQ](#).

For questions regarding E-ISAC membership, contact the Membership team at [memberservices@eisac.com](mailto:memberservices@eisac.com).

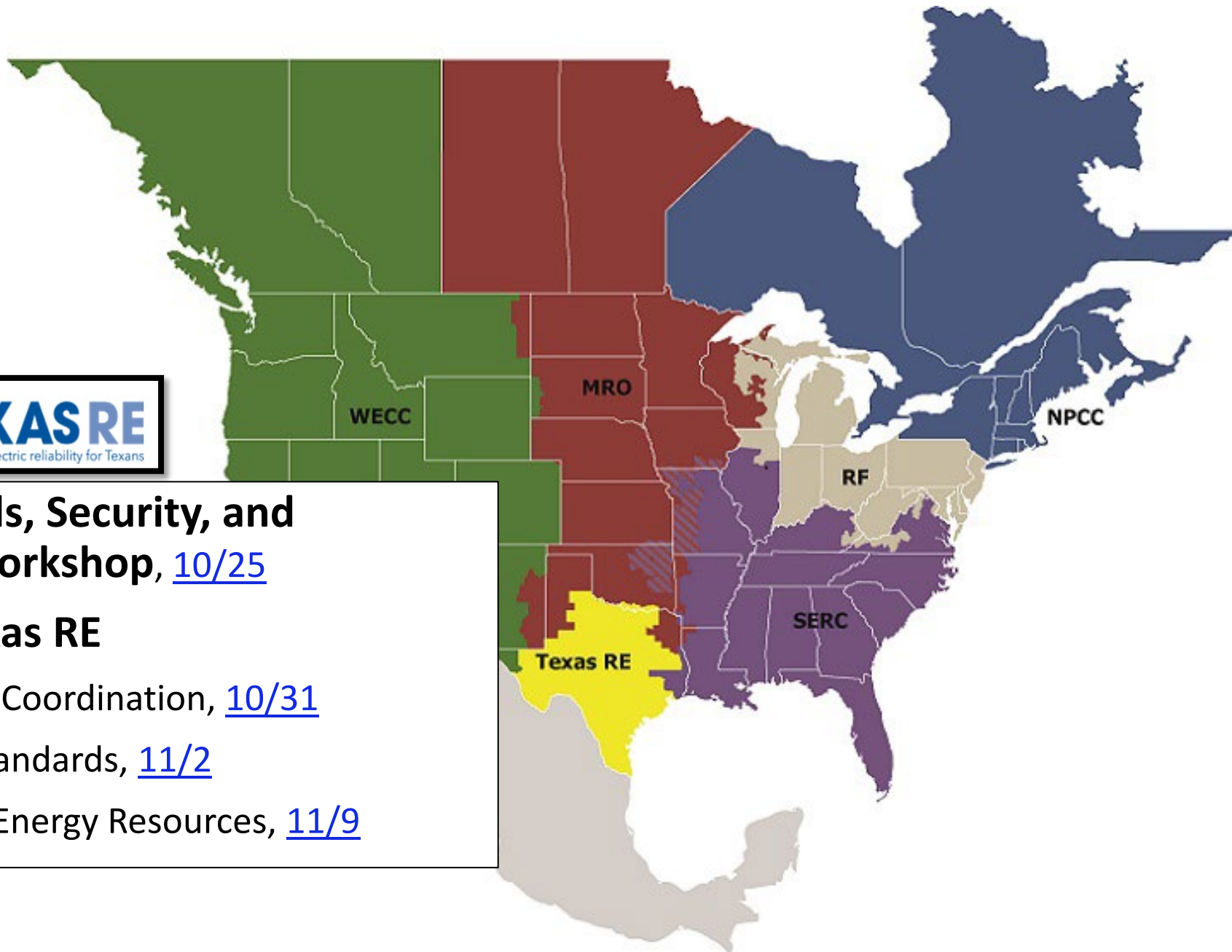




## Fall Standards, Security, and Reliability Workshop, [10/25](#)

### Talk with Texas RE

- Electric-Gas Coordination, [10/31](#)
- 2024 SOL Standards, [11/2](#)
- Distributed Energy Resources, [11/9](#)



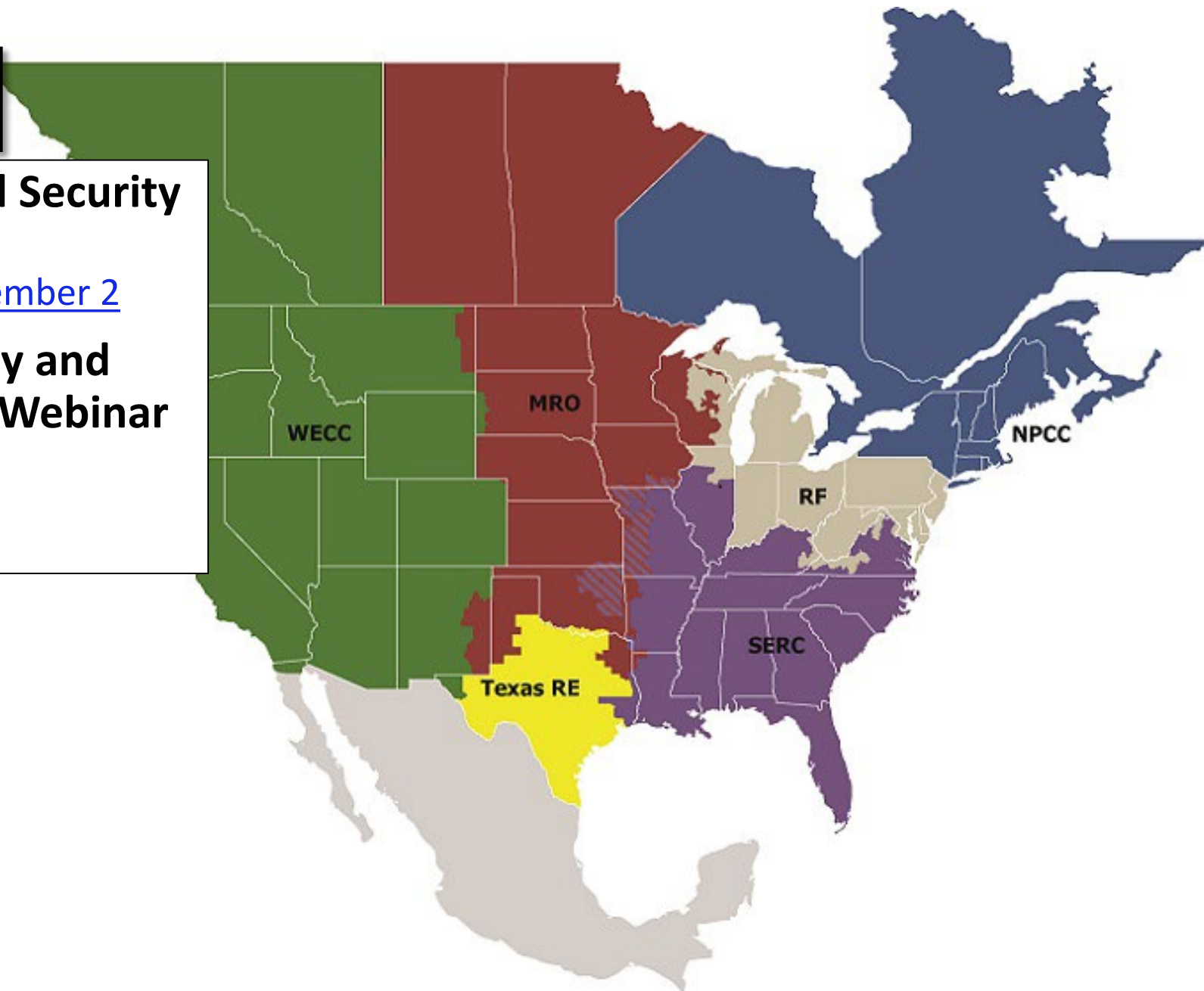


## Fall Reliability and Security Workshop

- [October 31 – November 2](#)

## Monthly Reliability and Security Monthly Webinar

- [November 16](#)





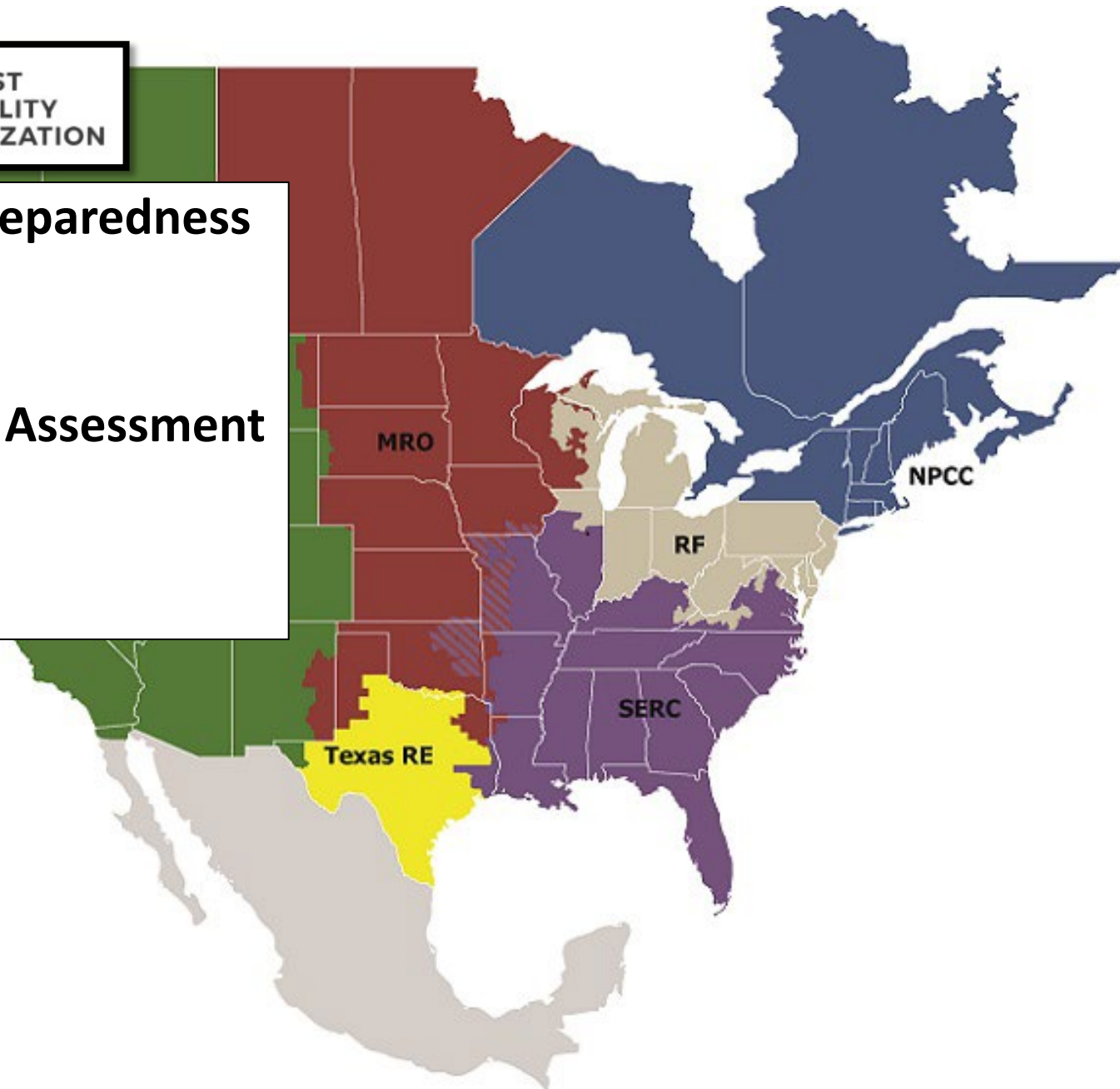


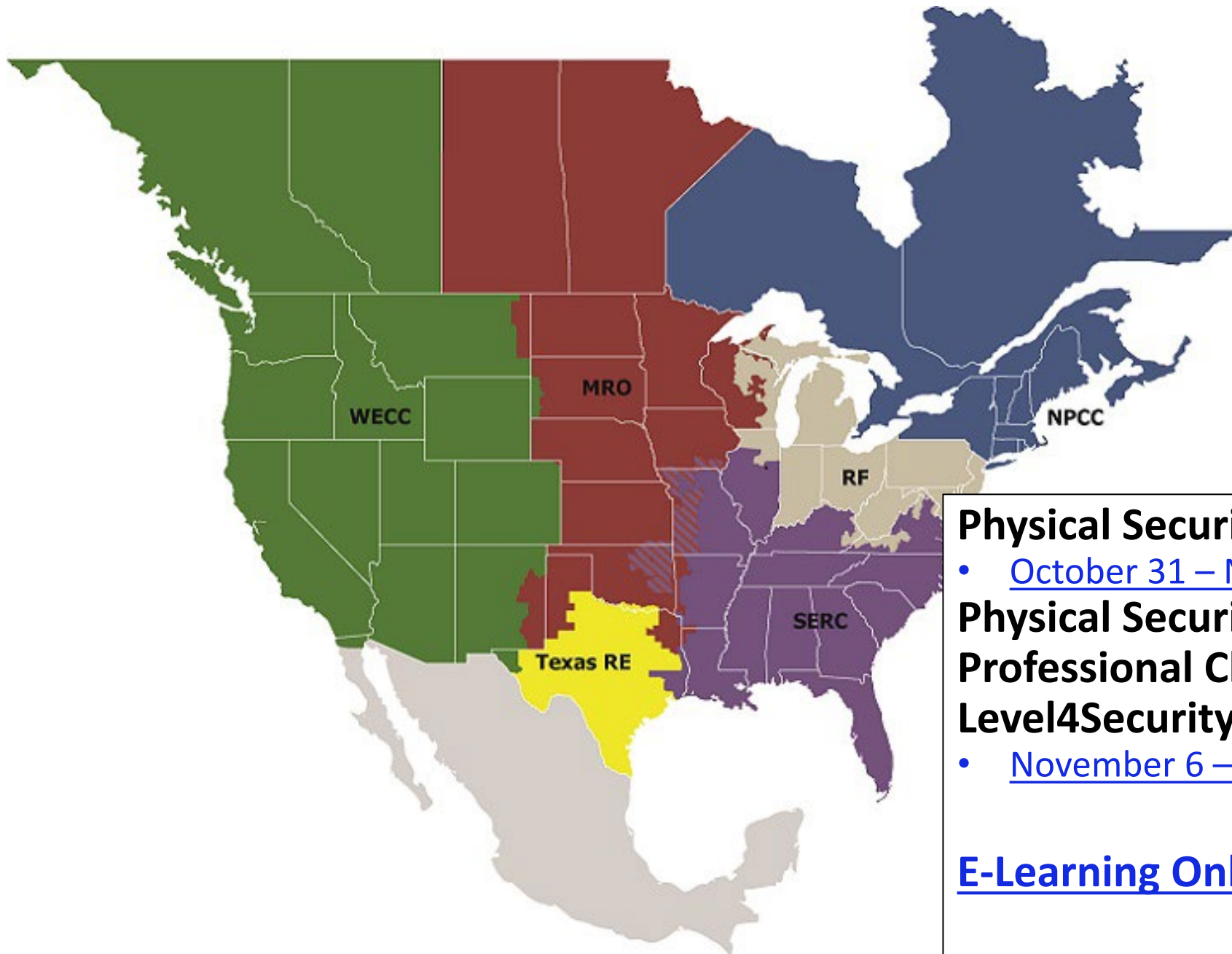
## Cold Weather Preparedness Workshop

- [October 26](#)

## Regional Winter Assessment Webinar

- [December 12](#)





## Physical Security Workshop

- [October 31 – November 2](#)

## Physical Security Professional Class – Level4Security

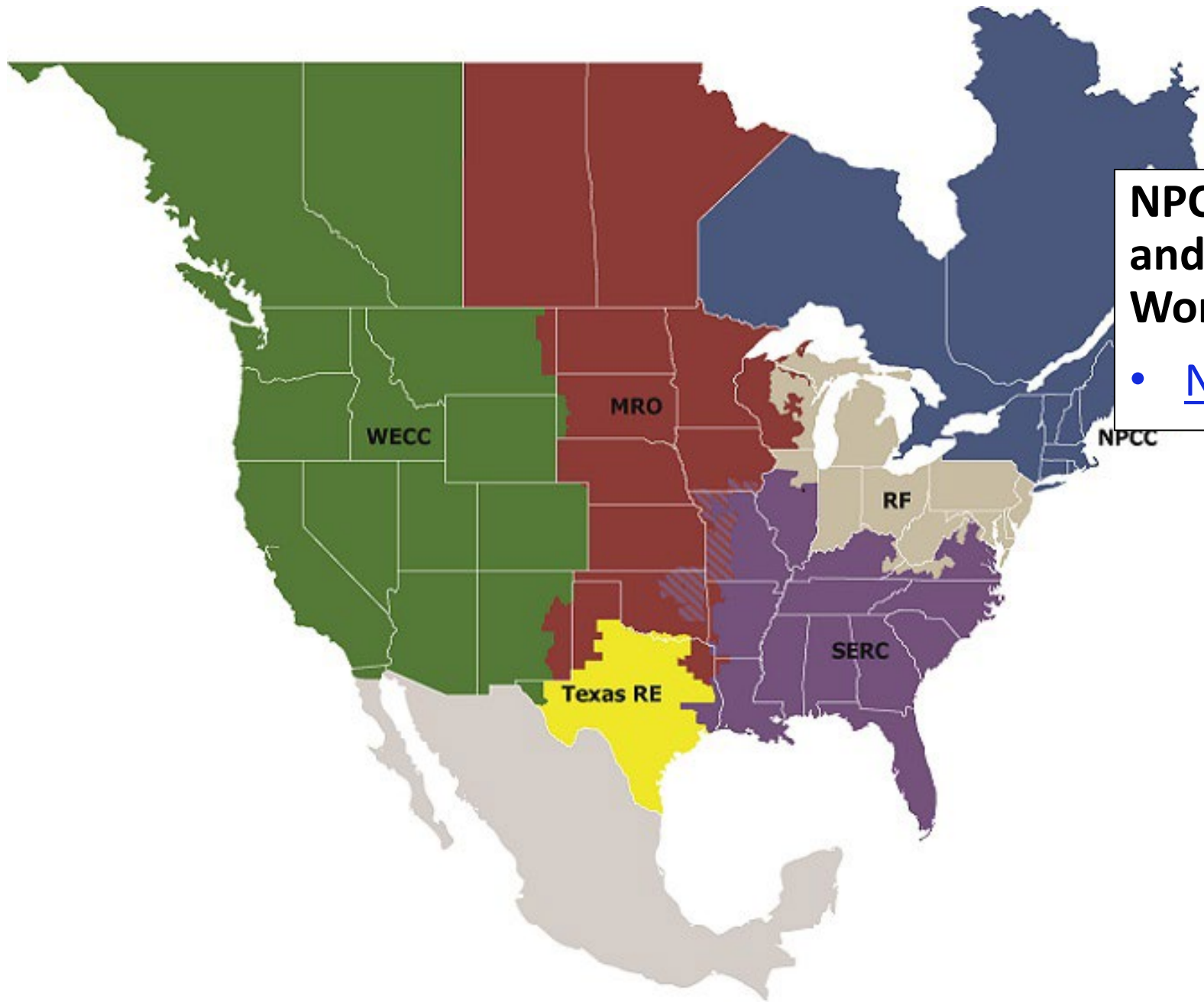
- [November 6 – 10](#)

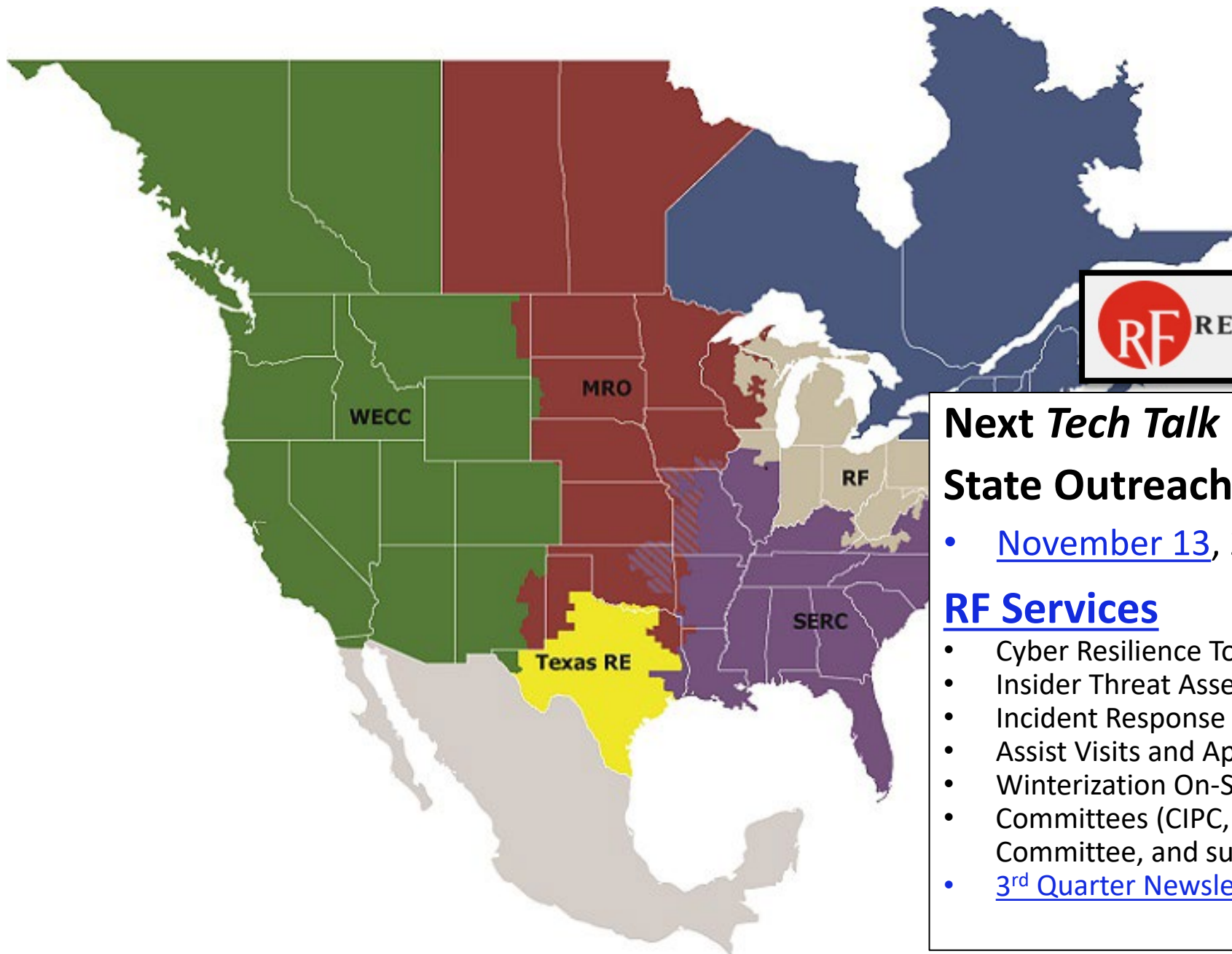
## [E-Learning Online Courses](#)



**NPCC Fall Compliance and Reliability Workshop**

- [November 8-9](#)





## **Next *Tech Talk with RF*** **State Outreach Edition**

- [November 13](#), 2:00 – 3:30 PM

### **RF Services**

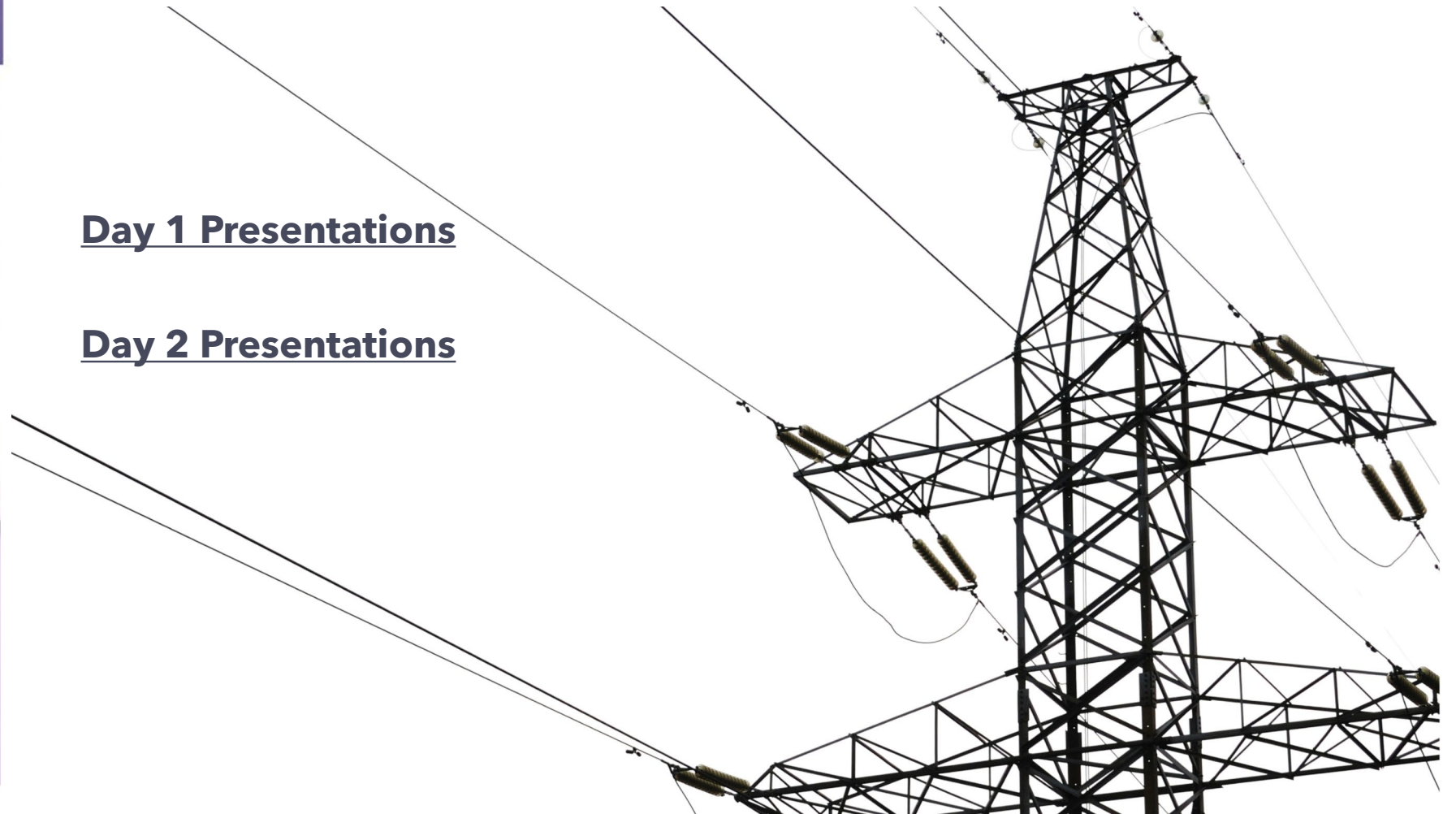
- Cyber Resilience Tool
- Insider Threat Assessment
- Incident Response Tabletops
- Assist Visits and Appraisals
- Winterization On-Site Visits
- Committees (CIPC, Reliability Committee, and subcommittees)
- [3<sup>rd</sup> Quarter Newsletter](#)

# ***Thank you for Attending RF Fall Workshop Sept 26-27 Omni William Penn, Pittsburgh***



Day 1 Presentations

Day 2 Presentations



# TECHNICAL TALK WITH RF



Join the conversation at

[SLIDO.com](https://www.slido.com)

[#TechTalkRF](https://twitter.com/TechTalkRF)

# TECH TALK REMINDER

*Tech Talk with RF* announcements are posted on our calendar on [www.rfirst.org](http://www.rfirst.org) under UPCOMING EVENTS



UPCOMING EVENTS [VIEW ALL](#)

October 23, 2023

**Technical Talk with RF**

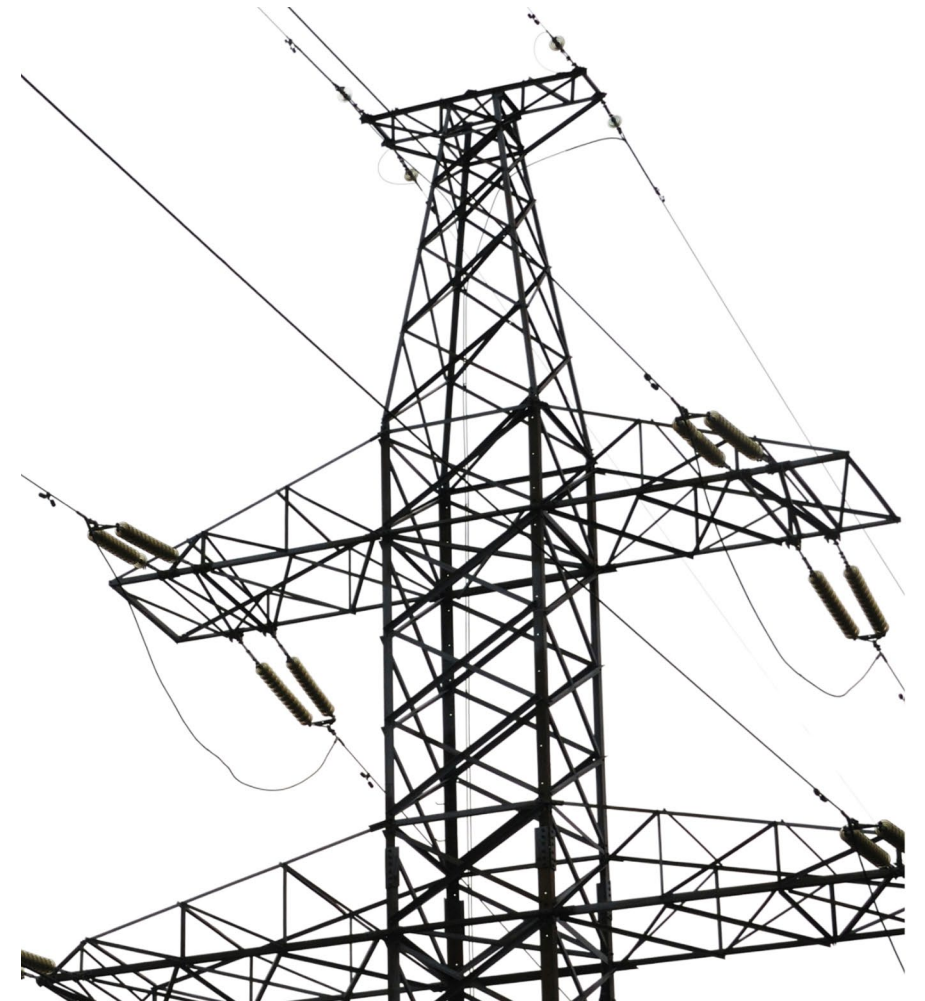
**CLICK HERE** 



# Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.





# AGENDA

---

## ***CYBERSECURITY AWARENESS MONTH***

### **DOE ANNOUNCEMENT - CYBERSECURITY TRAINING**

- CYNTHIA HSU - CYBERSECURITY PROGRAM MANAGER,  
RURAL AND MUNICIPAL UTILITIES, US DOE

### **BCS INFORMATION ACCESS MANAGEMENT**

- SHON AUSTIN - PRINCIPAL TECHNICAL AUDITOR,  
RELIABILITYFIRST

### **BES CYBER SYSTEMS (BCS) IN THE CLOUD**

- TOM ALRICH - INDEPENDENT CONSULTANT AND LEADER  
OF THE OPEN WEB APPLICATION SECURITY PROJECT  
SOFTWARE BILL OF MATERIALS FORUM PROJECT





U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Cybersecurity, Energy Security,  
and Emergency Response

# ReliabilityFirst TechTalk

Cynthia Hsu, Cybersecurity Program Manager, Rural and Municipal Utilities  
October 23, 2023



# CESER Mission

Strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions.

## Evolving Threats to Energy Infrastructure



# CESER advances the office's national security mission through:

---

- **Risk Assessment.** Identifying, analyzing, and prioritizing risks to the energy sector.
- **Risk Mitigation.** Developing policies, tools, and technologies and providing technical assistance to mitigate risks to the energy sector.
- **Sector Collaboration.** Strengthening the security of U.S. energy systems through enhanced public and private sector collaboration.
- **Preparedness and Response.** Facilitating energy sector preparedness, response, and restoration efforts in collaboration with other Federal agencies, the private sector, and state, local, tribal, and territorial communities and international partners.
- **Energy Supply.** Mitigating the impacts of energy supply disruptions on American businesses and consumers.

# Leadership



**Puesh M. Kumar**  
*Director*



**Robert Perry**  
*Acting Chief of Staff & Senior Advisor*



**Douglas MacIntyre**  
*Acting Principal Deputy Director & Deputy Director, Office of Petroleum Reserves*



**Mara Winn**  
*Deputy Director, Preparedness, Policy, and Risk Analysis*



**Ken Buell**  
*Deputy Director, Response & Restoration*

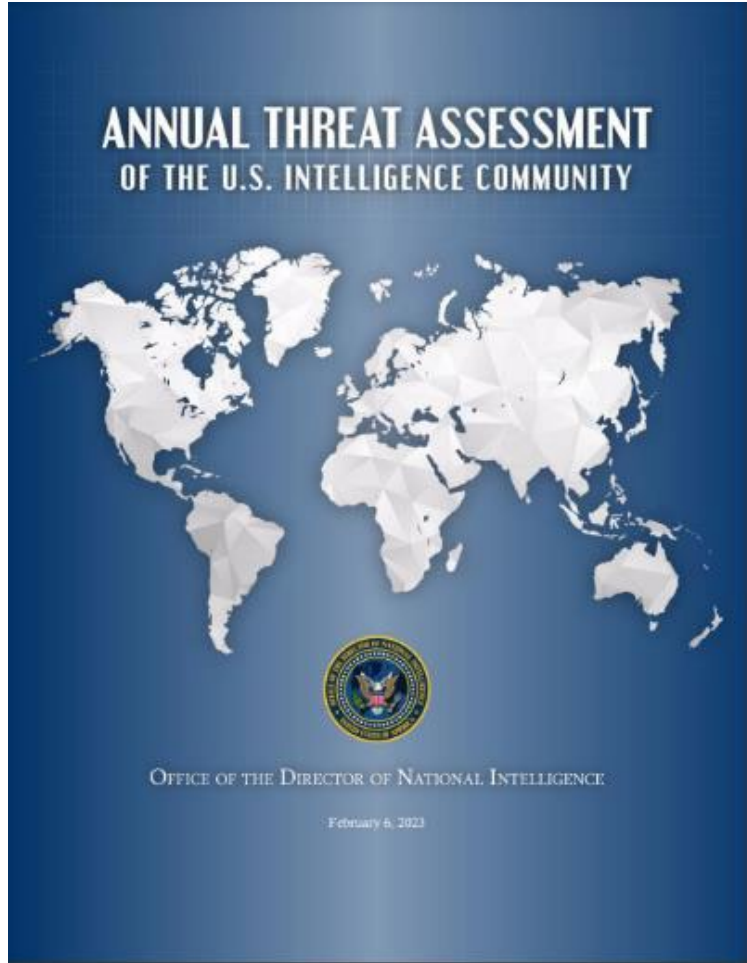


**Jason Shay**  
*Chief Operating Officer*



**Dan LaGraffe**  
*Deputy Director, Risk Management Tools & Technologies*

# Cybersecurity Threats



<https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3676-2023-annual-threat-assessment-of-the-u-s-intelligence-community>



“China almost certainly is capable of launching cyber attacks that would *disrupt critical infrastructure services within the United States*, including against *oil and gas pipelines* [...]”<sup>3</sup>



“Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as *disrupting an electrical distribution network for at least a few hours* [...]”<sup>1</sup>



“Iran’s opportunistic approach to cyber attacks makes *critical infrastructure owners* in the United States susceptible to being targeted [...]”<sup>3</sup>



“Transnational cyber criminals are increasing the number, scale, and sophistication of *ransomware* attacks, fueling a virtual ecosystem that *threatens to cause greater disruptions of critical services* [...]”<sup>2</sup>

*Annual Threat Assessment of the U.S. Intelligence Community*  
<sup>1</sup>2019, <sup>2</sup>2022, <sup>3</sup>2023

# Cybersecurity Threats

## Criminal Actions:

- business email compromise (BEC)
- ransomware

## Direct impacts on OT systems:

- Ukraine 2015
- Ukraine 2016

 The New York Times


### Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

May 13, 2021



[Colonial Pipeline Cyber Incident | Department of Energy](#)

 Bloomberg.com

### Russian Hackers Tried Damaging Power Equipment, Ukraine

...

... military intelligence agency launched a cyberattack on Ukrainian energy facilities, according to Ukrainian cybersecurity officials.



# Physical Security Threats

- Rogue actors and domestic violent extremists targeting critical energy infrastructure
- 97% resulted in no grid impact and 3% resulted in outages or other grid impacts, between 2020-2022
- Notable increase in repeat and clustered incidents

CNN

## [A vulnerable power grid is in the crosshairs of domestic extremist groups](#)

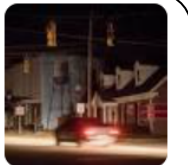
... fired at two power substations in Moore County, North Carolina, ... In 2022 there were 25 “actual physical attacks” reported on power...



The New York Times

## [Pair Charged With Plotting to Attack Baltimore Electrical Grid](#)

WASHINGTON – Federal law enforcement officials have arrested two ... the plot to jarring details of her personal and physical travails.



Information provided by E-ISAC



# Collaboration and Coordination is Essential

State, Local, Tribal, and Territorial (SLTT) Governments



Industry Trade Assoc.



Industry Councils



Energy Government Coordinating Council (EGCC)



NASEO NARUC NGA

# Information Sharing Across the Energy Sector

## Information Sharing and Analysis Centers (ISAC)



**The ESCC's Cyber Mutual Assistance Program**

The Electric Power and Natural Gas Industries  
Share Expertise to Counter Cyber Attacks

**CMA**  
Cyber Mutual Assistance

**Cyber Defense: Building on the Industry's Culture of Mutual Aid**

The North American energy grid is a complex interconnected network of generation, transmission, and distribution systems operated by thousands of organizations. Protecting the energy grid and ensuring a reliable and affordable supply of energy are the top priorities of the electric power and natural gas industries.

Building on the industries' culture of mutual assistance, and informed by lessons learned from major destructive cyber incidents overseas as well as by exercises held in North America, the ESCC directed the formation of the Cyber Mutual Assistance (CMA) Program. The Program is a natural extension of

[ESCC - CMA \(electricitysubsector.org\)](http://electricitysubsector.org)

Partners in Situational Awareness

**E-ISAC CRISP**  
CYBERSECURITY RISK INFORMATION SHARING PROGRAM

**Pacific Northwest**  
NATIONAL LABORATORY

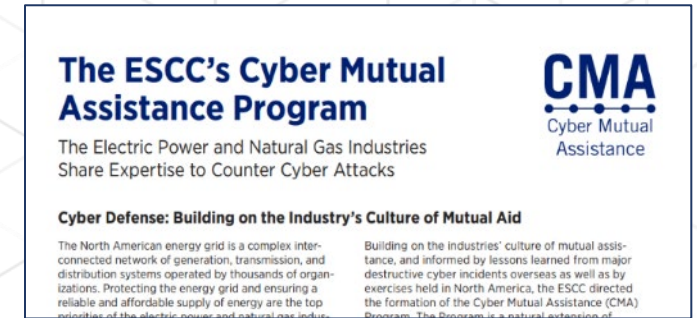
[CRISP \(eisac.com\)](http://eisac.com)

# Information Sharing Across the Energy Sector

## Information Sharing and Analysis Centers (ISAC)



[86615D01-1866-DAAC-99FB-02328D2044C3](https://www.naruc.org/86615D01-1866-DAAC-99FB-02328D2044C3) ([naruc.org](https://www.naruc.org))



[ESCC - CMA \(electricitysubsector.org\)](https://www.electricitysubsector.org)



[CRISP \(eisac.com\)](https://www.eisac.com)

# Risk Management Tools & Technology (RMT)

Today's research is tomorrow's capabilities

**Cybersecurity for Energy Delivery Systems (CEDS) Fact Sheets**

Office of Cybersecurity, Energy Security, and Emergency Response • Cybersecurity for Energy Delivery Systems (CEDS) Fact Sheets

Search:

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS) FACT SHEETS

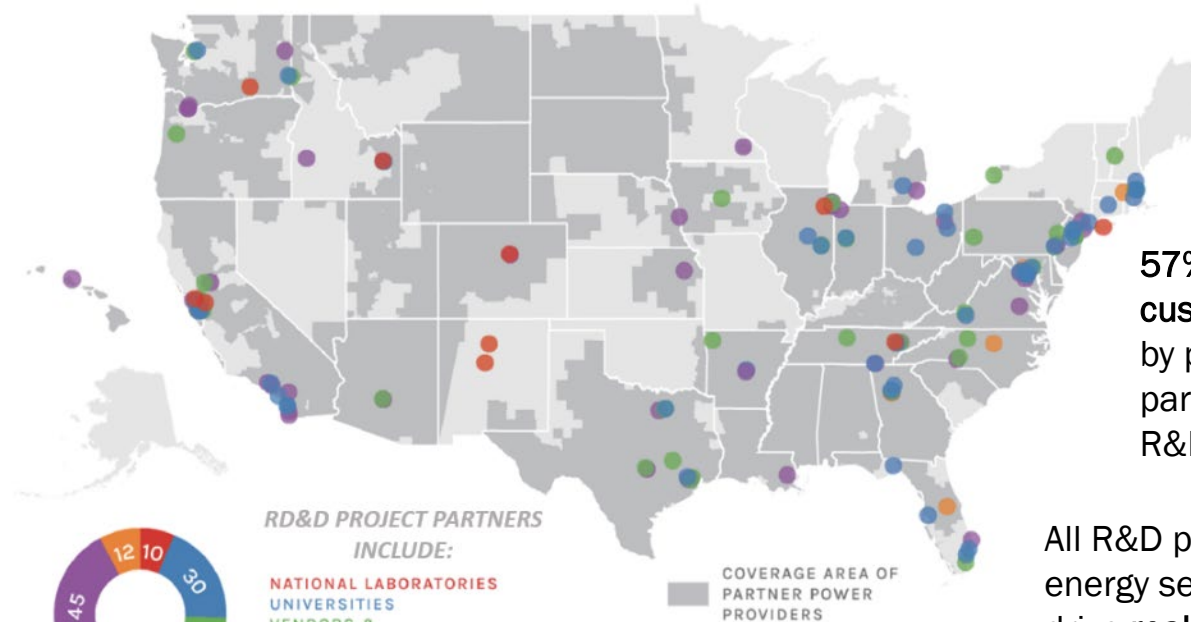
Status:  Active  Inactive

Prime Performer:  ABB, Inc.  ABB, Inc., Inc.

PROJECT NAME	PRIME PERFORMER	PROJECT PARTNERS	STATUS	PROJECT DESCRIPTION
Cyber Resilient Energy Delivery Consortium (CREDC)	CREDC	University of Illinois	Active	Resiliency, Workforce
A Conceptual Framework for the Assessment of Integrated Energy Storage Resources	CREDC	University of Illinois	Active	Renewable; ESR; Energy Storage; Resiliency
		University of		

Showing 1 to 10 of 170 entries

[Cybersecurity for Energy Delivery Systems \(CEDS\) Fact Sheets](#) | Department of Energy



57% of U.S. electricity customers are served by power providers participating in RMT R&D

All R&D projects included an energy sector partner to drive real-world solutions

More than 155 partners have participated in competitively funded projects

Delivered over 90 products, tools, and technologies since 2010 to reduce energy sector cyber risk

More than 1,500 utilities in all 50 states have purchased products developed under RMT research

# Cybersecurity Capability Maturity Model (C2M2)



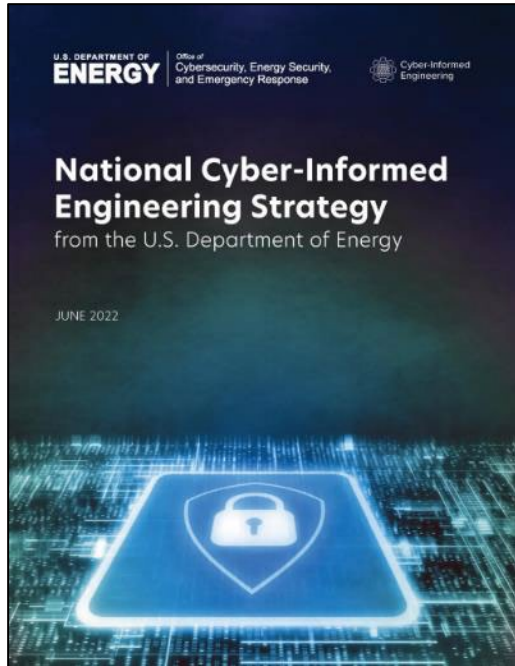
## Cybersecurity Capability Maturity Model

Scalable, sector-specific guidance and tools that organizations use to evaluate, prioritize, and improve their cybersecurity capabilities.

<https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>

# Risk Management Tools & Technology (RMT)

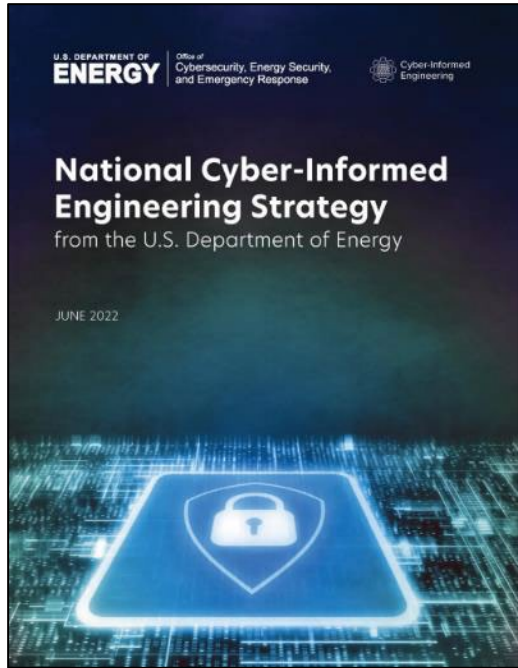
---



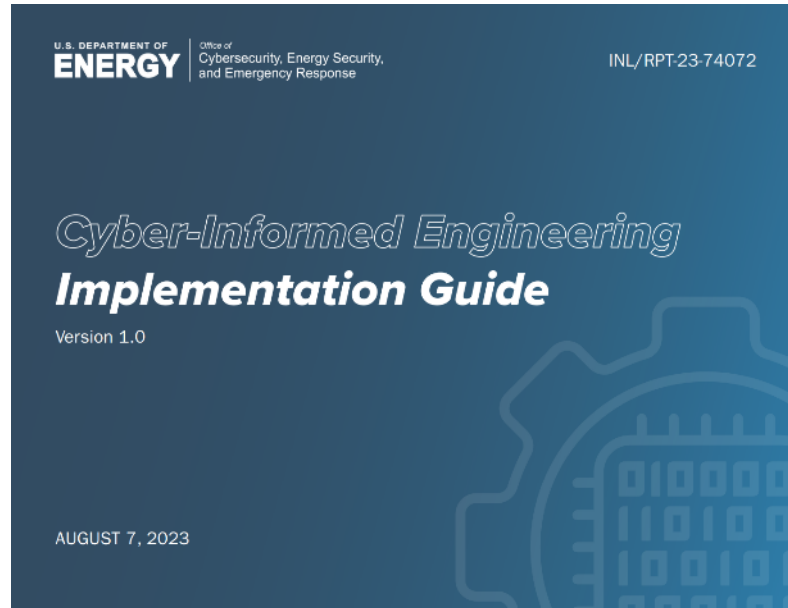
[FINAL DOE National CIE Strategy - June 2022\\_0.pdf](#)  
([energy.gov](https://energy.gov))

[https://inldigitallibrary.inl.gov/sites/sti/sti/Sort\\_67122.pdf](https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf)

# Risk Management Tools & Technology (RMT)



[FINAL DOE National CIE Strategy - June 2022\\_0.pdf](#)  
([energy.gov](https://energy.gov))



**PURPOSE** Describes the principles of Cyber-Informed Engineering (CIE) and outlines questions that engineering teams should consider during each phase of a system’s lifecycle to effectively employ these principles.

**PRIMARY USER** System or design engineers and technicians for critical energy infrastructure installations.

## WHY TARGET ENGINEERS?

CIE extends “secure-by-design” concepts beyond the digital realm to include the engineering of cyber-physical systems. CIE introduces cybersecurity considerations at the earliest stages of system design, long before the incorporation of software and security controls. It calls on engineers to identify engineering controls and design choices that could eliminate attack vectors for cyber actors or minimize the damage they could inflict.

This approach creates new opportunities for engineering teams—and not just cybersecurity teams—to secure the system using the physics and mechanics of engineering controls—not just digital monitoring and controls.

[https://inldigitallibrary.inl.gov/sites/sti/sti/Sort\\_67122.pdf](https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf)

# CESER Response and Restoration

## Facilitating the restoration of disrupted or damaged energy systems

- All Hazards: cyber, physical, environmental
- Working through FEMA's National Response Framework, built on the National Incident Management System
- Scalable, flexible, and adaptable coordination structures

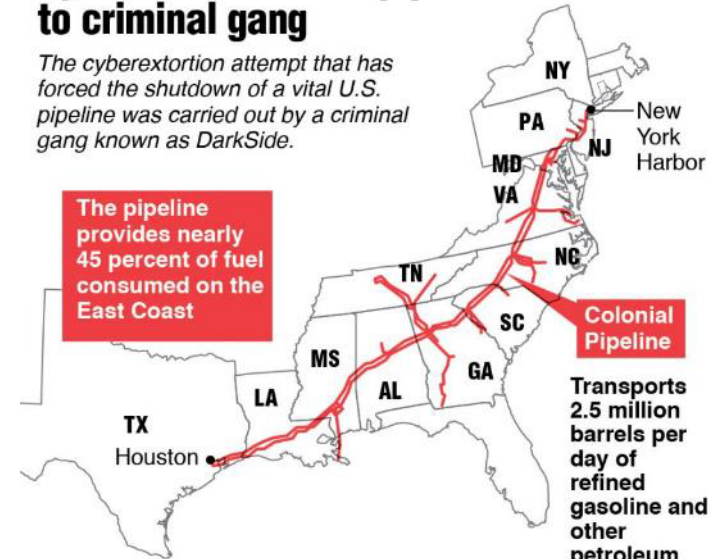
### Emergency Support Functions:

#### *How the Nation responds to disasters and emergencies*

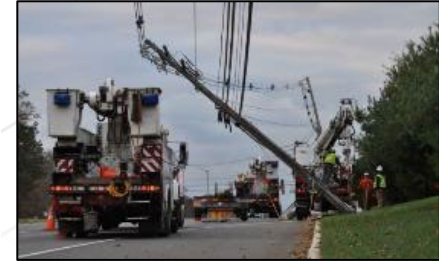
- |        |                                     |                       |  |
|--------|-------------------------------------|-----------------------|--|
| ▪ ESF1 | Transportation                      | ▪ ESF9                | Urban Search & Rescue                  |
| ▪ ESF2 | Communications                      | ▪ ESF10               | Oil & Hazardous Materials Response     |
| ▪ ESF3 | Public Works & Engineering          | ▪ ESF11               | Agriculture & Natural Resources        |
| ▪ ESF4 | Firefighting                        | ▪ <b>ESF12 Energy</b> |  |
| ▪ ESF5 | Emergency Management                | ▪ ESF13               | Public Safety & Security               |
| ▪ ESF6 | Mass Care, Housing & Human Services | ▪ ESF14               | Cross-Sector Business & Infrastructure |
| ▪ ESF7 | Resources Support                   | ▪ ESF15               | External Affairs                       |
| ▪ ESF8 | Public Health & Medical Services    |                       |  |

### Cyberattack on U.S. pipeline is linked to criminal gang

The cyberextortion attempt that has forced the shutdown of a vital U.S. pipeline was carried out by a criminal gang known as DarkSide.



Source: Colonial Pipeline Company, Shell Midstream Partners, AP  
Graphic: Staff, Tribune News Service





# 2022 Response Summary



Days  
Activated

169

38

Responders  
Deployed



• Three Hurricanes



• One Tropical Storm



• Severe Winter Weather



• Flooding



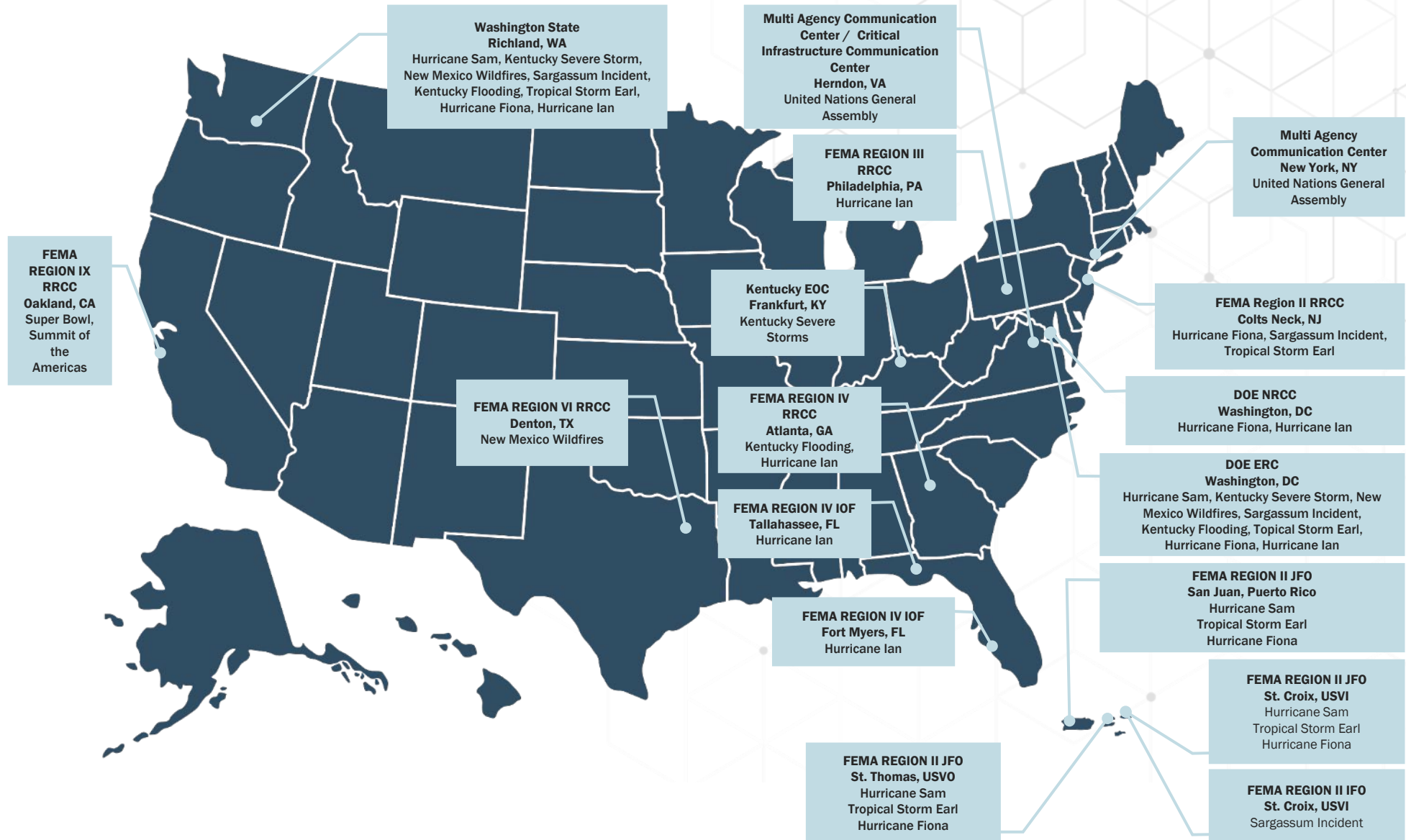
• Wildfires



• Sargassum Seaweed Overgrowth



• Four National Special Security Events



# CESER Capacity Building: Supported Resources

## State Governance, Planning, And Financing To Enhance Energy Resilience

Dec. 22, 2021 | Publications

This guide provides examples of state-wide resilience planning, and potential funding and financing.

### Introduction

From 2011 to 2020, the United States faced an average of **dollar disasters** annually at an average cost of \$93 billion and livelihoods, major natural disasters can devastate require expensive repairs and improvements. For this guide, we are defining resilience as the ability to withstand disasters effectively, and recover more quickly and to a more improved state.

Threats to energy infrastructure are not just physical. Cyberattacks on energy infrastructure are a growing concern. In 2019, energy companies are targeted by cybercriminals, just behind the manufacturing sectors, experiencing 11.1% of known cyberattacks. In 2019, or luck, many of those attacks did not affect energy supply. In 2021, Colonial Pipeline ransomware attack, which limited millions on the East Coast, underscores the potential threat to the energy sector.

The costs and impacts of disasters affecting energy infrastructure are not felt evenly across an economy or population. Lower-income communities, and communities on the front lines, change tend to bear a disproportionate burden in terms of resources needed to return to normalcy, health impacts, natural disasters and malicious attacks become more frequent, particularly to already-disadvantaged communities and shifting attention to pre-hazard mitigation – investing in advance of an incident. Energy resilience planning activities, as investing in hazard mitigation saves six times spent.



## State Action Guide for Energy Resilience Projects Under FEMA's Building Resilient Infrastructure and Communities (BRIC) Program and Other Hazard Mitigation Assistance (HMA) Programs

### Quick Guide

November 2022



U.S. DEPARTMENT OF ENERGY  
Office of Cybersecurity, Energy Security, and Emergency Response

## A Guide for Public Utility Commissions: Recruiting and Retaining a Cybersecurity Workforce

## Federal Funding Opportunities for Pre- and Post-Disaster Resilience

### GUIDEBOOK

Prepared for the National Association of Regulatory Utility Commissioners



## State of Virginia ENERGY SECTOR RISK PROFILE

U.S. DEPARTMENT OF ENERGY  
Cybersecurity, Energy Security, and Emergency Response

This State Energy Risk Profile examines the relative magnitude of the risks that the state of Virginia's energy infrastructure routinely encounters in comparison with the probable impacts. Natural and man-made hazards with the potential to cause disruption of the energy infrastructure are identified. Certain natural and adversarial threats, such as cybersecurity, electromagnetic pulse, geomagnetic disturbance, pandemics, or impacts caused by infrastructure interdependencies, are ill-suited to location-based probabilistic risk assessment as they may not adhere to geographic boundaries, have limited occurrence, or have limited historic data. Cybersecurity and other threats not included in these profiles are ever present and should be included in state energy security planning. A complete list of data sources and national level comparisons can be found in the Data Sources document.

### Virginia State Facts

POPULATION: 8.52 M  
HOUSING UNITS: 3.54 M  
BUSINESS ESTABLISHMENTS: 0.20 M

ENERGY EMPLOYMENT: 55,365 jobs  
PUBLIC UTILITY COMMISSION: Virginia State Corporation Commission  
STATE ENERGY OFFICE: Virginia Department of Mines, Minerals and Energy – Division of Energy  
EMERGENCY MANAGEMENT AGENCY: Virginia Department of Emergency Management  
AVERAGE ELECTRICITY TARIFF: 9.48 cents/kWh  
ENERGY EXPENDITURES: \$3,215/capita  
ENERGY CONSUMPTION PER CAPITA: 27.2 MMBtu (32nd highest out of 50 states and Washington, D.C.)  
GDP: \$532.9 billion

Data from 2020 or most recent year available. For more information, see the Data Sources document.

### Virginia Risks and Hazards Overview

- The natural hazard that caused the greatest overall property loss between 2009 and 2019 was **Flooding** at \$21 billion per year (leading cause nationwide at \$12 billion per year).
- Virginia had 108 Major Disaster Declarations, 134 Emergency Declarations, and 6 Fire Management Assistance Declarations for 5 events between 2013 and 2019.
- Virginia registered 16% fewer Heating Degree Days and 40% greater Cooling Degree Days than average in 2019.
- There are 2 Fusion Centers in Virginia. The Primary Fusion Center is located in North Chesterfield.

### Annualized Frequency of and Property Damage Due to Natural Hazards, 2009 – 2019

Hazard	Frequency - Annualized	Property Damage - Annualized (\$Million per year)
Drought	0	\$0
Earthquake (≥ 3.5 M)	<1	\$0
Extreme Heat	5	\$0
Flood	48	\$21
Hurricane	1	\$3
Landslide	1	\$0
Thunderstorm & Lightning	145	\$6
Tornado	10	\$10
Wildfire	1	\$1
Winter Storm & Extreme Cold	46	\$1

Data Source: NOAA and USGS

Produced by Department of Energy (DOE), Office of Cybersecurity, Energy Security, and Emergency Response (CESER) | MARCH 2021 | PAGE 1

## Department of Energy Emergency Response Hub

Access Situation Reports and Resources for Disasters

[SLTT Program Resource Library](#)

# CESER Exercises

## Clear Path

Annual all-hazards energy security and resilience exercise.

DOE has engaged over 1,400 energy sector and cross-infrastructure sector partners



## 2023 Clear Path Participating Organizations



## Liberty Eclipse

Annual ICS-focused energy cybersecurity exercise



### EXERCISE SCENARIO

Liberty Eclipse incorporates a scenario-based format informed by and derived from real and hypothetical, yet plausible, events. The exercise series focuses on cyber-attacks across multiple critical infrastructure sectors, including energy sectors and evaluates impacts within critical industrial control systems (ICS), as well as the potential for future physical effects on critical infrastructure. Exercise participants are given an opportunity to respond to scenario elements from the perspectives of their real-world roles and responsibilities to identify strengths and areas for improvement.

### EXERCISE GOAL

The overarching goal of Liberty Eclipse is to identify the energy sector's (both public and private) operational policies, plans, and procedures in response to a significant cybersecurity incident affecting critical infrastructure. To date, DOE has engaged over 800 energy sector and cross-infrastructure sector partners since 2018. Recognizing the strong support and engagement from partner organizations, DOE strives to ensure that each new edition of Clear Path presents an increasingly realistic and challenging exercise experience for all participants. Liberty Eclipse presents a diverse array of cyber exercise scenarios challenging response officials and allowing planners to build upon corrective actions and validate improvements made in response to lessons learned from previous exercises and real-world incidents.

### EXERCISE VALUE

Liberty Eclipse addresses the challenges that the energy sector may face during a major cyber-attack across the United States. By focusing on the collaboration between the electric and oil & natural gas (ONG) sectors, and between government and industry, DOE hopes to establish and reinforce relationships across the energy sector and its partners, to facilitate future preparedness and emergency response operations.

# Training and Workforce Development



DOE's CyberForce® Program seeks to inspire and develop the next generation of skilled cyber defenders for the energy sector through hands-on competitions, webinars, and a virtual career fair.



## WEBINAR SERIES

The Webinar Series was also added in 2021 to expand on our industry and academia partner engagement. These webinars will highlight upcoming news within the program as well as key topics of interest within cybersecurity.



## WORKFORCE PORTAL

The Workforce Portal will be the CyberForce Program's main hub for all things program related. Participants will have a chance to better understand their skills, engage in regular communication, check job boards, and be the first to hear about upcoming events and trainings.



## CYBERFORCE COMPETITION®

The CyberForce Competition is the original competition that started the program back in 2016. This is a defend/attack cyber-physical scenario.



## CONQUER THE HILL SERIES

The Conquer the Hill competition series provides smaller individual based competitions that narrow in on specific skills for participants.



## VIRTUAL CAREER FAIR

The CyberForce Program will be hosting a Virtual Career Fair for the participants of its collective programs on Wednesday, October 11, 2023.

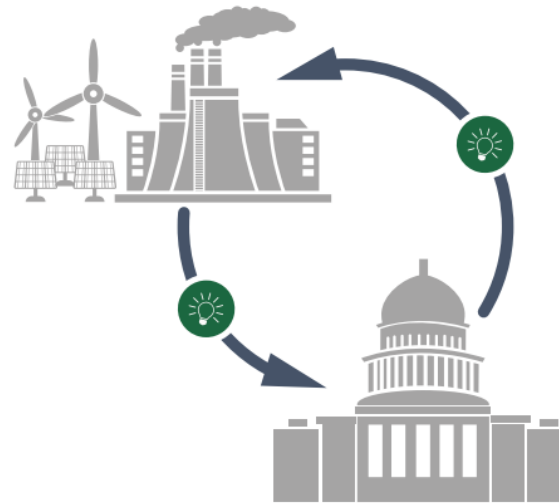
<https://cyberforce.energy.gov>

# Training and Workforce Development



- **3<sup>rd</sup> Cohort**
- **21 Alumni**

## Fellowship Goals



Serve as an information and idea exchange platform between government and energy sector experts, contributing to the bi-directional advancement of improved cybersecurity and information sharing capabilities and processes.

&



Familiarize and discuss the current state of cybersecurity operations, capabilities, gaps, constraints, and areas for mutual improvement to better defend our nation's critical energy infrastructure.

[OTDefender: Operational Technical Defender Fellowship \(inl.gov\)](https://inl.gov)

# Cybersecurity Training for the Utility Workforce



Register Now

<p><b>Columbus, OH</b> Oct 31 - Nov 2, 2023</p> <p>Cybersecurity Training for ...</p> <p>Columbus, OH Oct 31, 2023 - Nov 02, 2023</p> <p>Register Now</p>	<p><b>Orlando, FL</b> Nov 28 - 30, 2023</p> <p>Cybersecurity Training for ...</p> <p>Orlando, FL Nov 28 - 30, 2023</p> <p>Register Now</p>	<p><b>Kansas City, MO</b> Dec 5 - 7, 2023</p> <p>Cybersecurity Training for ...</p> <p>Kansas City, MO Dec 5 - 7, 2023</p> <p>Register Now</p>
---	--	--

Registration Coming Soon

<p><b>San Diego, CA</b> Jan 17 - 19, 2024</p> <p>Cybersecurity Training for ...</p> <p>San Diego, CA Jan 17 - 19, 2024</p> <p>Registration Coming Soon</p>	<p><b>Dallas, TX</b> Jan 23 - 25, 2024</p> <p>Cybersecurity Training for ...</p> <p>Richardson, TX Jan 23 - 25, 2024</p> <p>Registration Coming Soon</p>	<p><b>Buffalo, NY</b> Apr 23 - 25, 2024</p> <p>Cybersecurity Training for ...</p> <p>Amherst, NY Apr 23 - 25, 2024</p> <p>Registration Coming Soon</p>
--	--	--

**U.S. DEPARTMENT OF ENERGY**  
Office of  
Cybersecurity, Energy Security,  
and Emergency Response



AGENDA CPE CREDIT HOURS SUGGESTIONS ON WORKSHOP SELECTIONS INSTRUCTORS HOTELS LOCATION MORE...

**Columbus, OH**  
Oct. 31 - Nov. 2, 2023

U.S. DEPARTMENT OF ENERGY  
Office of Cybersecurity, Energy Security, and Emergency Response

**INL**  
Idaho National Laboratory

## Cybersecurity Training for the Utility Workforce - Columbus

Columbus, OH  
October 31, 2023 - November 02, 2023 · Hyatt Regency Columbus

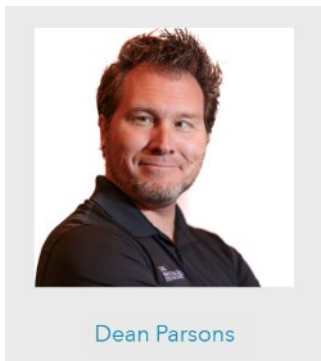
REGISTER

<https://www.eventleaf.com/c/CybersecurityTrainingUtilityWorkforce>

# Day 1: Chose From Two Full-Day Options

## ICS Foundations (6 CPEs)

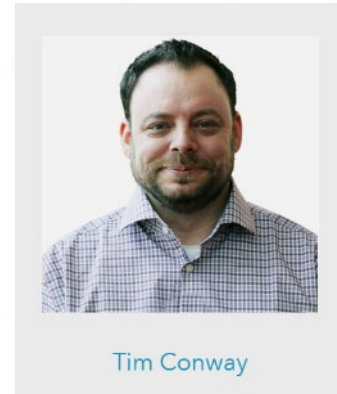
This course serves the purpose of introducing people into the field of industrial control systems (ICS) / operational technology (OT) and the cybersecurity considerations unique to securing these environments.



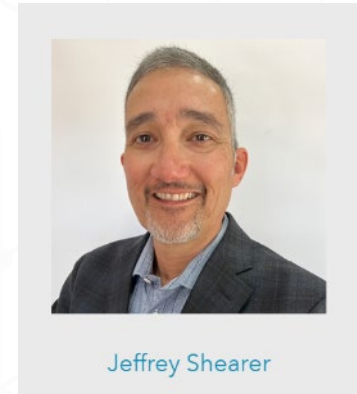
<https://www.sans.org/profiles/dean-parsons/>

## DOE CyberStrike (6.5 CPEs)

Participants are guided through hands-on exercises to gain an understanding of the methodology cyber adversaries use to target operational processes for remote attack.



<https://www.sans.org/profiles/tim-conway/>

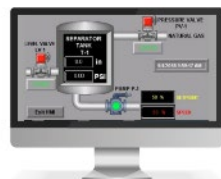


<https://www.sans.org/profiles/jeffrey-shearer/>

# DOE CyberStrike™

## CyberStrike™ LIGHTS OUT

PRACTICAL TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS



The CyberStrike™ LIGHTS OUT training workshop offers participants a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine.

### Hands-on Exercises

- Open-Source Intelligence
- Denial of Service
- Passive Man in the Middle Attack
- Firmware Analysis
- Controlling the Human Machine Interface
- Bypassing the Human Machine Interface
- Active Man in the Middle Attack
- Defender Mitigations

### Tools Used During the Workshop

- Kali Linux
- Hping3
- EditorMetasploit
- VNC Viewer
- Wireshark
- MiniMega
- OpenPLC
- Nmap
- Ettercap

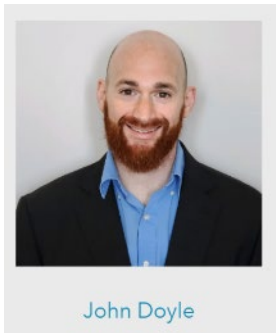
[CyberStrike Training - INL](#)



# Day 2: Select from Four Half-Day Options or...

## CTI in Times of Conflict (3 CPEs)

Learn about major threat trends observed during the past year and specifically related to the Ukraine/Russia conflict.



<https://www.sans.org/profiles/john-doyle/>

## Defending Against State Sponsored Attacks (3 CPEs)

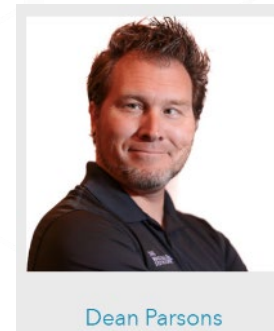
This lab-heavy workshop provides four approaches to foil attackers in a repeatable and verifiable way. Participants will learn how to rapidly harden systems in a low risk evidence-based approach.



<https://www.sans.org/profiles/jon-gorenflo/>

## ICS Security for Leaders and Managers (3 CPEs)

This session empowers leaders and managers responsible for securing critical infrastructure, and operational technology / industrial control systems OT/ICS environments.



<https://www.sans.org/profiles/dean-parsons/>

## OSINT-Practical Open-Source Intelligence Techniques for Defense (3 CPEs)

This talk will cover key OSINT skills that analyst can use to improve their situational awareness and insights and will cover OPSEC considerations, Image Analysis, working with large datasets and Dark Web investigation.

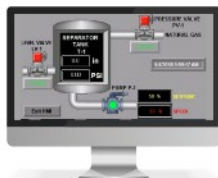


<https://www.sans.org/profiles/mick-douglas/>

# Day 2: Select the Full-Day CyberStrike Option

## CyberStrike™ LIGHTS OUT

PRACTICAL TRAINING FOR ENERGY SECTOR OWNERS & OPERATORS



The CyberStrike™ LIGHTS OUT training workshop offers participants a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine.

### Hands-on Exercises

- Open-Source Intelligence
- Denial of Service
- Passive Man in the Middle Attack
- Firmware Analysis
- Controlling the Human Machine Interface
- Bypassing the Human Machine Interface
- Active Man in the Middle Attack
- Defender Mitigations

### Tools Used During the Workshop

- Kali Linux
- Hping3
- EditorMetasploit
- VNC Viewer
- Wireshark
- MiniMega
- OpenPLC
- Nmap
- Ettercap

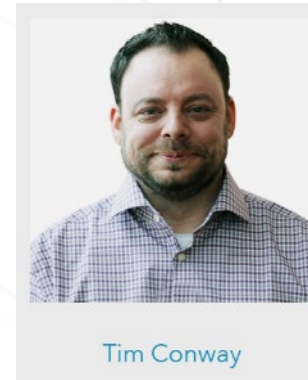
[CyberStrike Training - INL](#)

# Day 3: One Full-Day Option

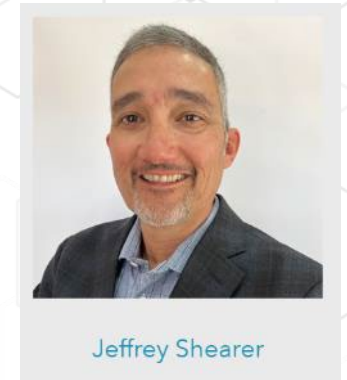
## Red Team / Blue Team Competition (6 CPEs)

Participants will work through a series of interactive learning scenarios that enable Operational Technology security professionals to develop and master the real-world, in-depth skills they need to defend real-time systems.

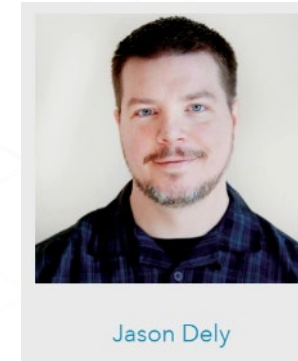
It is designed as a challenge competition and is split into separate levels so that advanced players may quickly move through earlier levels based on their expertise. The Grid Netwars experience has been themed for the electricity industry and the scenario has been coordinated to align with industry exercise events.



<https://www.sans.org/profiles/tim-conway/>



<https://www.sans.org/profiles/jeffrey-shearer/>



<https://www.sans.org/profiles/jason-dely/>

# Good to Know

---

- Registration is ***FREE – there is no cost to attend.***
- Open to all electric utility staff (including IOUs, cooperatives, public power, tribal, and territory utilities)
- Participants are responsible for their own travel, lodging, and meal costs.
- Each of the 6 training events will cover the same material.
- To minimize travel expenses there is a training event located in each of the six NERC regions.

This training series is organized by CESER and its Rural and Municipal Utility Cybersecurity (RMUC) Program using funding provided by the historic [Bipartisan Infrastructure Law](#) (BIL). The BIL appropriates more than \$62 billion to DOE to invest in American manufacturing and workers; expand access to energy efficiency and clean energy; deliver secure, reliable, clean, and affordable power to more Americans; and demonstrate and deploy the technologies of tomorrow through clean energy demonstrations.

# 40124: Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program

## Funding:

\$250 million over 5 years (FY22-26)

## Objectives:

1. Deploy cybersecurity technology, operational capability, or services that enhance the security posture of electric utilities through improvements in the ability to **protect** against, **detect**, **respond** to, or **recover** from a **cybersecurity threat**.
2. Increase the participation of eligible entities in cybersecurity **threat information sharing** programs.

## ACT 1 Prize



Winning utilities can receive up to \$200,000 in cash and 60-120 hours of technical assistance

<https://www.herox.com/ACT1Prize>

RMUC Program  
Funding  
Opportunity  
Announcement  
(FOA)

Anticipated to  
be released  
before the end  
of 2023

# RMUC Program Eligibility and Priorities

---

## Eligibility:

- Rural electric cooperatives (~900)
- Public Power utilities (~2,000)
  - a utility owned by a political subdivision of a State
  - a utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State
- Not-for-profits in partnership with rural or municipal electric utilities (unknown number)
- Investor-owned electric utilities that sell < 4,000,000 MWh/year (~22-50)

# RMUC Program Eligibility and Priorities

## Eligibility:

- Rural electric cooperatives (~900)
- Public Power utilities (~2,000)
  - a utility owned by a political subdivision of a State
  - a utility owned by any agency, authority, corporation, or instrumentality of 1 or more political subdivisions of a State
- Not-for-profits in partnership with rural or municipal electric utilities (unknown number)
- Investor-owned electric utilities that sell < 4,000,000 MWh/year (~22-50)

## Priority Given to Eligible Entities:

- with limited cybersecurity resources;
- that own assets critical to the reliability of the bulk-power system (BPS); or,
- that own defense critical electric infrastructure (DCEI)

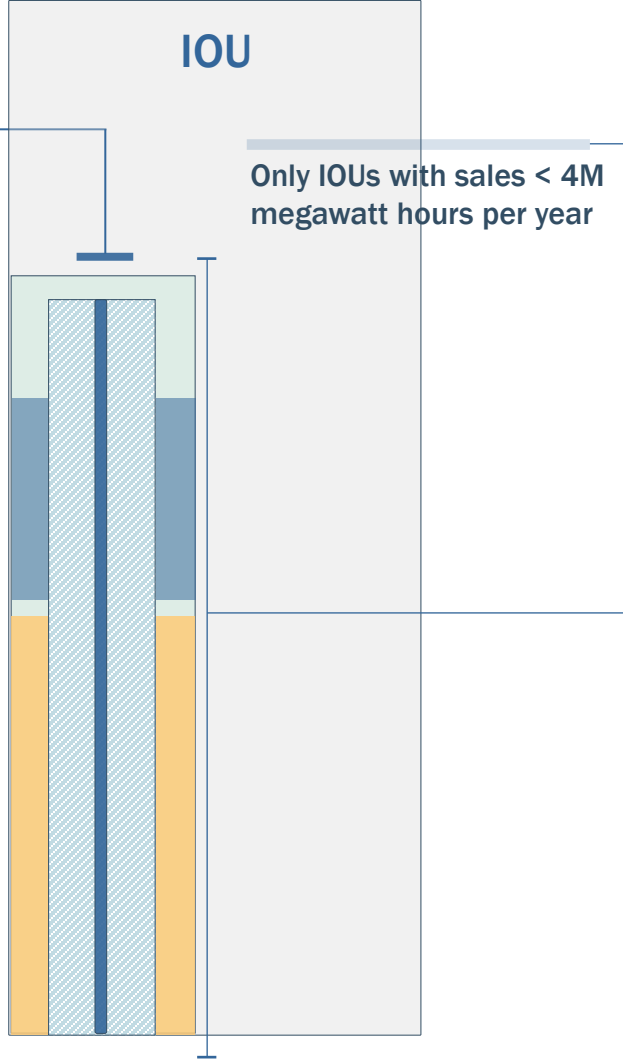
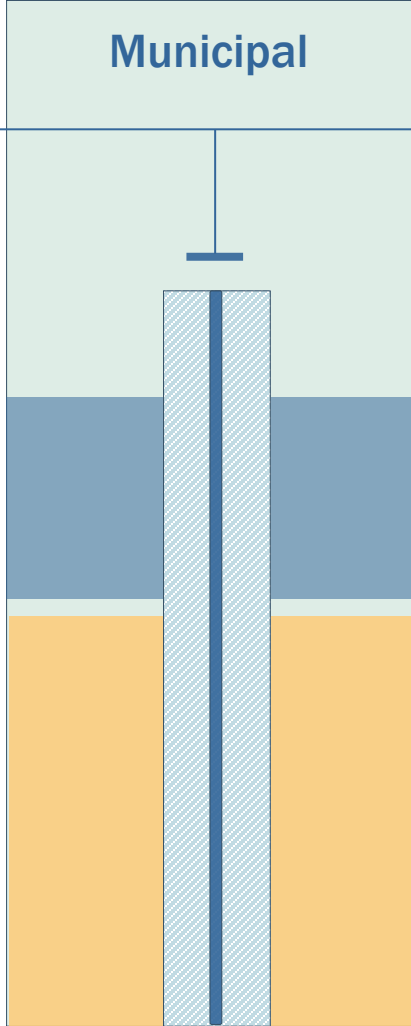
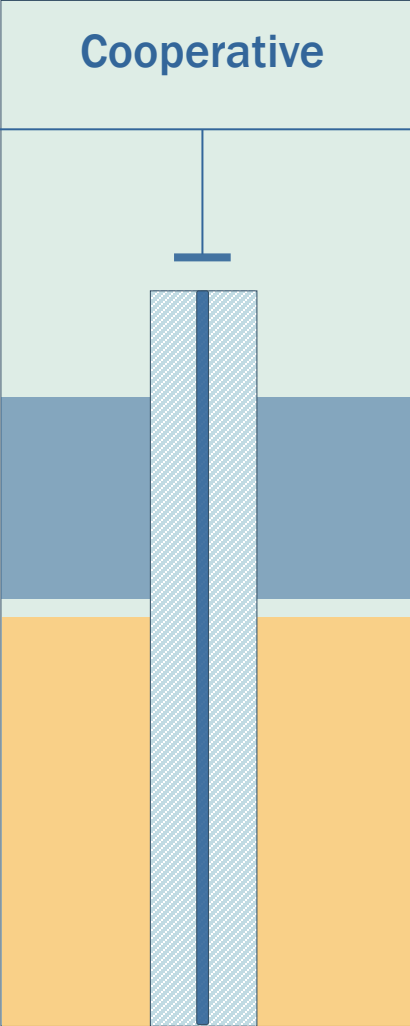
# RMUC Priorities

Not-for-profit entity that is in a partnership with six (6) or more cooperative and/or municipal utilities.

**Serving Military Installations**  
Own Defense Critical Electric Infrastructure

**Utilities critical to reliability of bulk power system**

**Utilities with limited cybersecurity resources**





# Advanced Cybersecurity Technology (ACT) 1 Prize



Empowering utilities with limited cybersecurity resources to make critical investments in staff training, governance processes, and technologies to harden their systems against threats.

<https://www.herox.com/ACT1Prize>

# ACT 1 Prize: Three Phases

---

Three increasingly competitive phases; each phase concludes with a prize.

- 1. Commitment Phase:** Utilities prepare submission packages that describe their resources, need for improving their cybersecurity posture, and commitment to participating in the ACT 1 Prize.
- 2. Planning Phase:** Utilities work with technical assistance (TA) providers to complete system assessments, identify areas for training, understand potential risks and solutions, and draft a roadmap for implementation.
- 3. Implementation Phase:** Utilities work with TA providers to make progress toward completing their implementation roadmap.

# ACT 1 Prize: Cash Awards and Technical Assistance

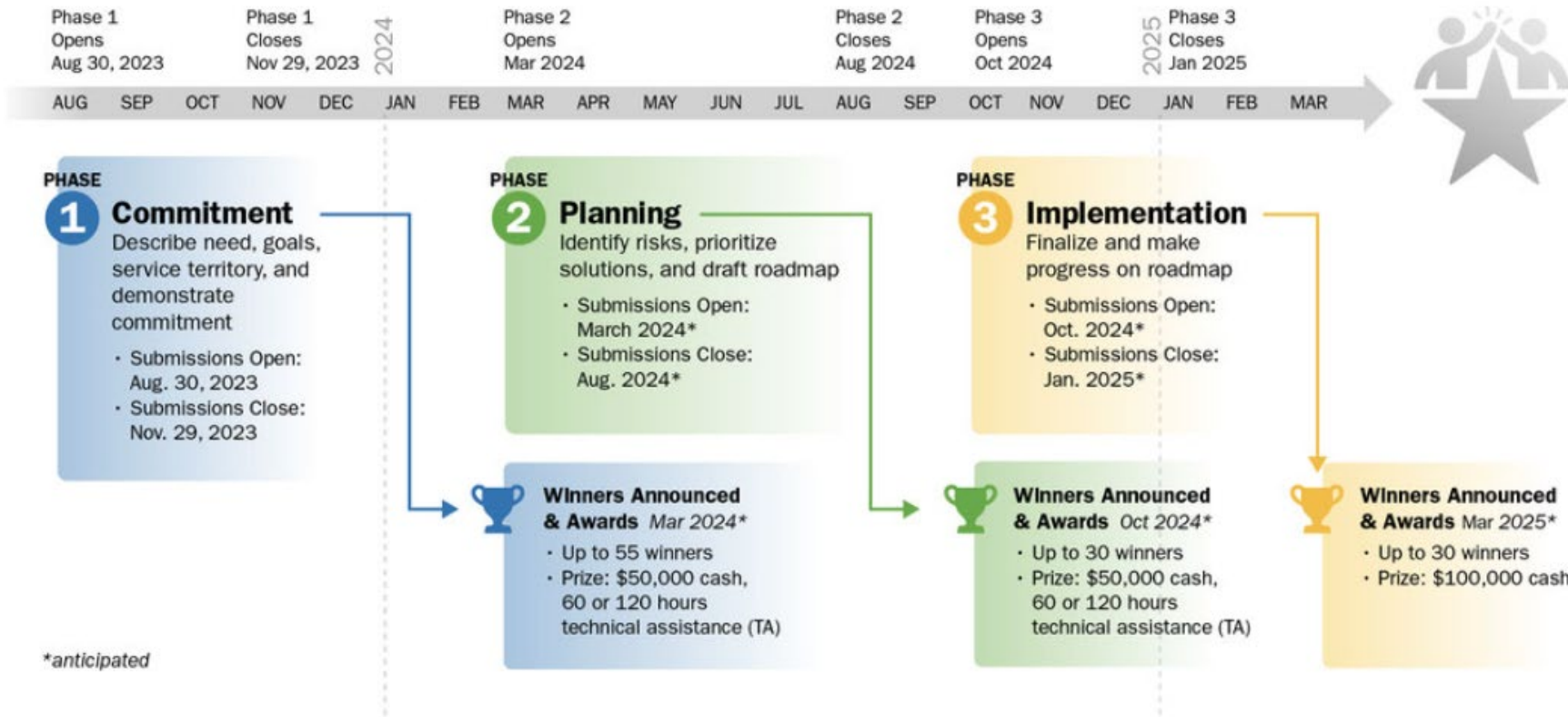
Prize Phase	LIMITED CYBERSECURITY RESOURCES Track	MILITARY Track
Commitment	<ul style="list-style-type: none"> <li>• \$50,000</li> <li>• Up to 60 hours of TA</li> <li>• Up to 50 winners</li> </ul>	<ul style="list-style-type: none"> <li>• \$50,000</li> <li>• Up to 120 hours of TA</li> <li>• Up to 5 winners</li> </ul>
Planning	<ul style="list-style-type: none"> <li>• \$50,000</li> <li>• Up to 60 hours of TA</li> <li>• Up to 25 winners</li> </ul>	<ul style="list-style-type: none"> <li>• \$50,000</li> <li>• Up to 120 hours of TA</li> <li>• Up to 5 winners</li> </ul>
Implementation	<ul style="list-style-type: none"> <li>• \$100,000</li> <li>• Up to 25 winners</li> </ul>	<ul style="list-style-type: none"> <li>• \$100,000</li> <li>• Up to 5 winners</li> </ul>
<b>Total potential cumulative award*</b>	<ul style="list-style-type: none"> <li>• <b>\$200,000</b></li> <li>• <b>120 hours of TA</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>\$200,000</b></li> <li>• <b>240 hours of TA</b></li> </ul>

# Advanced Cybersecurity Technology (ACT) 1 Prize



Rural & Municipal Utility Cybersecurity Program  
**Advanced Cybersecurity Technology Prize**

Applications Due:  
 November 29, 2023



[s://www.herox.com/ACT1Prize](https://www.herox.com/ACT1Prize)

# RMUC Program

---

For more information follow the RMUC Program website:

[Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance \(RMUC\) Program | Department of Energy](#)

Or join the email list at

**CESER.RMUC@hq.doe.gov**

RMUC Program Funding Opportunity Announcement anticipated before end of 2023.

# CESER Contact Information

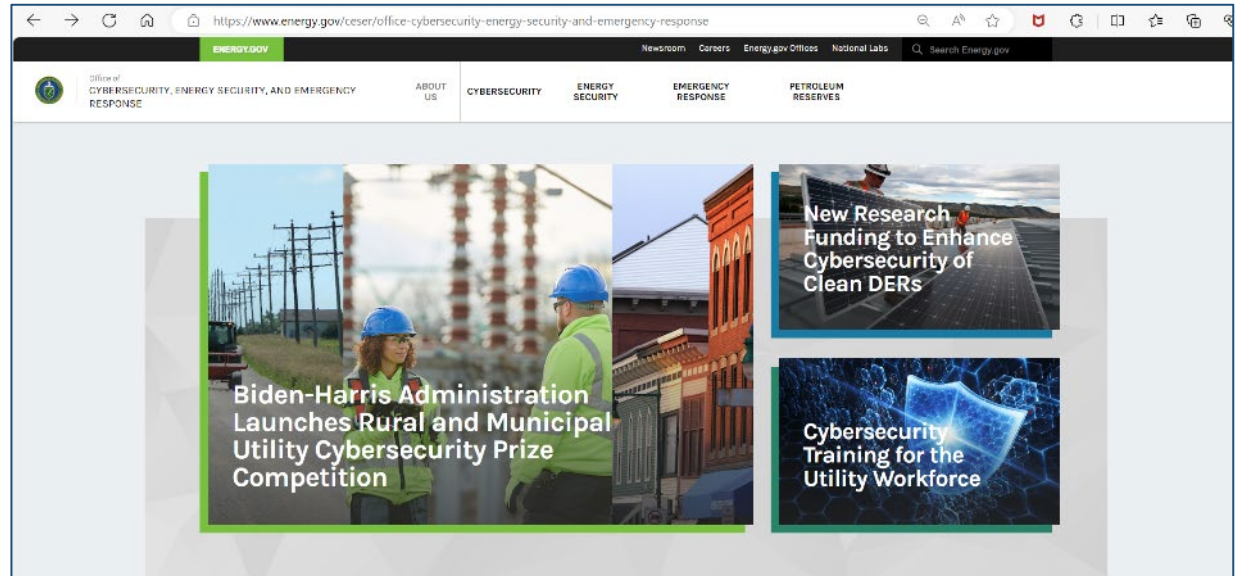
## Rural and Municipal Utility Cybersecurity (RMUC) Program



**Dr. Cynthia Hsu**  
Cybersecurity Program Manager,  
Rural and Municipal Utilities  
[cynthia.hsu@hq.doe.gov](mailto:cynthia.hsu@hq.doe.gov)  
202-209-3817



**Fania Barwick**  
Implementation Manager,  
RMUC Program  
[fania.barwick@hq.doe.gov](mailto:fania.barwick@hq.doe.gov)  
240-243-3949





@DOE\_CESER



[linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response](https://www.linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response)



[energy.gov/CESER](https://energy.gov/CESER)

U.S. DEPARTMENT OF  
**ENERGY**

*Office of*  
Cybersecurity, Energy Security,  
and Emergency Response

# PROTECTING BES CYBER SYSTEM INFORMATION (BCSI)

Shon Austin, Principal Technical Auditor

October 23, 2023





# LEARNING OBJECTIVES

- After this presentation you will understand the purpose, expectations, challenges, and **Commonly Accepted**\* of the revisions to CIP-004-7 and CIP-011-3 standards for protecting BCSI

\* Commonly Accepted are suggested by ERO staff but are NOT required by the standard

# C.I.A. TRIAD



# PURPOSE OF CIP-011

- “To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).”
- But why is this necessary?

“For me personally, cloud security isn’t a worry. My data is such a mess that no one would find anything anyway.”

~ Anonymous



# BACKGROUND

- Revisions
  - Industry catalyst for change
  - FERC response
  - Increased flexibility
- Future direction
  - Less of an administrative obligation
  - Growing need to store BCSI in cloud environments
  - Vendor systems are migrating to cloud-only environments

# CIP-011-3

## (Cyber Security- Information Protection)

### STANDARD KEY CHANGES

- Revised CIP-011-3 Requirement R1
  - Still requires an Information Protection Program (IPP)
    - Part 1.1 identify BCSI
      - What is and what is not BCSI
    - Part 1.2 methods to mitigate the risks of the loss of confidentiality of BCSI

# WHAT AUDITORS EXPECT

Primary evidence:

- Documented Information Protection Program(s)

Supporting evidence:

- Evidence of IPP implementation
  - Where are you storing BCSI
- BCSI Training materials
- Labels / Classification

# POSSIBLE CHALLENGES

- Failure to address BCSI:
  - Storage
  - Transit
  - Use



# COMMONLY ACCEPTED

- Keep an accurate inventory of all BCSI assets in a cloud environment
- Document those individuals and systems who can “obtain” the BCSI assets in the cloud
- Carefully document who can “use” the encryption keys for cloud-based BCSI

# CIP-004 R6

## (Cyber Security-Personnel & Training)

### REQUIREMENT KEY CHANGES

- Transferred authorization of BCSI access from Requirement R4 to a new Requirement, R6
- R6 explains terms:
  - Access
    - Capability to concurrently obtain and possess the ability to use BCSI
  - Provisioned access
    - Needed access is granted to authorized individuals to BCSI

# WHAT AUDITORS EXPECT

Primary evidence:

- Documented BCSI access management program

Supporting evidence:

- List BCSI Authorizers
- List authorization / termination record
- Provisioned authorized access

# POSSIBLE CHALLENGES

- Provisioned access not authorized
- Failure to document or implement a process to remove an individual's ability to use provisioned access to BCSI

# COMMONLY ACCEPTED

- Develop process for CIP-004-7 R4, R5 and R6 and CIP-011-3 R1 jointly



# QUESTIONS & ANSWERS

Shon Austin

# BES CYBER SYSTEMS IN THE CLOUD

**TOM ALRICH** - Independent Consultant and leader of the open web application security project software bill of materials forum project

**LEW FOLKERTH** - ReliabilityFirst , Principal Reliability Consultant



# WHICH WAY TO THE CLOUD?

Tom Alrich

Tom Alrich LLC

RF Tech Talk October 23, 2023



# Summary

- These slides are taken directly from the paper, “Allowing medium and high impact BES Cyber Systems in the cloud”. Tom has reproduced that paper in full in his blog, <https://tomalrichblog.blogspot.com/>.
- Tom will send a PDF of the document to anyone who emails him at [tom@tomalrich.com](mailto:tom@tomalrich.com).

# What's the problem?

- Currently, while low impact BES Cyber Systems (BCS) can be freely deployed in the cloud today, and while medium and high impact BCSI can be stored in the cloud starting 1/1/2024, medium and high impact BCS (as well as EACMS) cannot be deployed in the cloud at all. That situation is not currently expected to change.
- However, there is almost universal agreement among NERC, the NERC Regions, NERC entities, (probably) FERC, security vendors, and the cloud service providers (CSPs) themselves that this situation must change.

# Why is this happening?

- No CIP requirement explicitly forbids deploying medium and high impact BCS in the cloud. In fact, none of the CIP requirements even mentions the cloud.
- However, if a NERC entity deploys any medium or high impact BCS in the cloud, they will have to demonstrate during an audit that they have remained compliant with every CIP requirement that applies to medium and/or high impact BCS.
- And for the entity to remain compliant, they will have to demonstrate that the CSP is compliant with most of the CIP Standards, which is not feasible for the CSP.

# Tom's Proof of Concept

# Overall Approach – Two Tracks

- There will be two “tracks” for NERC CIP compliance: Track 1 for “On-premises BCS” and Track 2 for “Cloud BCS”.
- Track 1 will be almost identical to the current CIP-004 to CIP-013 standards. All on-premises BCS will follow this track, meaning there should be few if any changes required to their existing CIP compliance programs.
- Track 2 will apply to systems implemented in the cloud will also follow a new standard (CIP-015?) that will apply only to medium or high impact BCS implemented in the cloud. This standard will function a lot like CIP-013, in that it will require a NERC entity with medium and/or high impact Cloud BCS to develop a cloud security risk management plan.
- CIP-003 may be unchanged and will apply to both on-premises and cloud based low impact BCS.

# Changes to CIP-002 – Where Tracks 1 & 2 Diverge

The following could be added to CIP-002 R1 (phrases and words in red are new):

- **1.4.** Identify each of the high impact **Cloud** BES Cyber Systems according to Attachment 1, Section 4, if any, **associated with** each asset;
- **1.5.** Identify each of the medium impact **Cloud** BES Cyber Systems according to Attachment 1, Section 5, if any, **associated with** each asset; and
- **1.6.** Identify each asset that is associated with a low impact **Cloud** BES Cyber System according to Attachment 1, Section 6, if any (a discrete list of low impact Cloud BES Cyber Systems is not required).

# Change to existing BCS Definition

The definition of BCS needs to be changed to read something like, “If deployed in an on-premises environment\*, a BES Cyber System is one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a NERC functional entity.”

\* “On-premises” needs to be defined. It might be called “non-cloud” instead.

# New Cloud\* BCS Definition

Identifying Cloud BCS will be the first step in Track 2 - not identifying Cyber Assets and BCAs, as in Track 1. Therefore, the definition of Cloud BCS needs to incorporate the provisions included in the BCA definition. Suggestion:

“A System\* that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.”

\* System and Cloud need to be defined.



# Changes to CIP-002 Attachment 1

- Since sections 1-3 of Attachment 1 deal with classification of high, medium, and low impact BCS respectively (i.e., on premises BCS), there need to be two or three new sections that deal with classification of high, medium, and (possibly) low impact Cloud BCS.
- The impact classification of the BCS has nothing to do with where it is deployed, so none of the “bright line criteria” in Attachment 1 need to change for Cloud BCS.

# Changes to CIP-002 Attachment 1 (2)

## *New Section 4:*

The first line of Section 4 should read, “**Each Cloud BES Cyber System used by and located at any of the following:**” Following that should be the list of four types of high impact Control Centers found in Section 1.

## *New Section 5:*

This section should begin, “**Each Cloud BES Cyber System...**” Other than that, Section 5 should exactly mirror Section 2.

## *New Section 6:*

The section should begin, “**Cloud BES Cyber Systems not included in Sections 4 or 5 above...**” Other than that, Section 6 should exactly mirror Section 3.

# New CIP Standard(s) for Cloud BCS

- Because CIP-004 through CIP-013 will remain unchanged for on-premises BCS, none of them needs to be substantially changed, other than to acknowledge that now there are also Cloud BCS.
- CIP-003 needs to allow for low impact Cloud BCS. Once that change is made, it seems likely that the requirements in CIP-003 will still be valid as written.
- However, the revised BCSI requirements which take effect 1/1/24, CIP-004 R6 and CIP-007 R1, need to be left in effect.
- In the place of the existing CIP-004 through CIP-013, there needs to be a new CIP standard or standards (CIP-015?) that applies only to Cloud BCS. Other than the two new BCSI requirements, none of the other requirements in CIP-004 through -014 should remain in Track 2.

## New CIP Standard(s) for Cloud BCS (2)

- The new Standard should be a lot like CIP-013: It requires the NERC entity to develop and implement a risk management plan. Here, it is a cloud BCS risk management plan.
- Unlike CIP-013, the new Standard should require:
  1. That the CSP be assessed by NERC or a NERC-designated organization every year, and
  2. Verify that the results of the assessment meet criteria in the entity's cloud risk management plan.

Thank you!

Tom's blog: <https://tomalrichblog.blogspot.com/>

Tom's email: [tom@tomalrich.com](mailto:tom@tomalrich.com)

# THANK YOU

***Join us for our next Tech Talk -  
State Energy Policy Edition  
November 13<sup>th</sup>***

John Moura, NERC - Interregional  
Transfer Capability Studies

Shane Watts, PJM - Emerging  
Technologies

**[Webinar Link](#)**

