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

# National Cybersecurity Education Colloquium (NCEC)

Dr. Cynthia Hsu, Cybersecurity Program Manager, Rural and Municipal Utilities

September 20, 2023

# BLUF

Cybersecurity Workforce Strategy for CESER

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# BLUF



## Cybersecurity Workforce Strategy for CESER

Current premise:

Energy asset owners and operators need the resources and staff
with the knowledge, skills, and abilities
to successfully adapt and respond
to a constantly changing cybersecurity threat landscape.

# What problem(s) are we trying to solve?

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?

# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?
- Not training the right audience(s)
- Recruitment issue
  - Potential candidates not interested
  - Human resources infrastructure

# CESER Mission

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



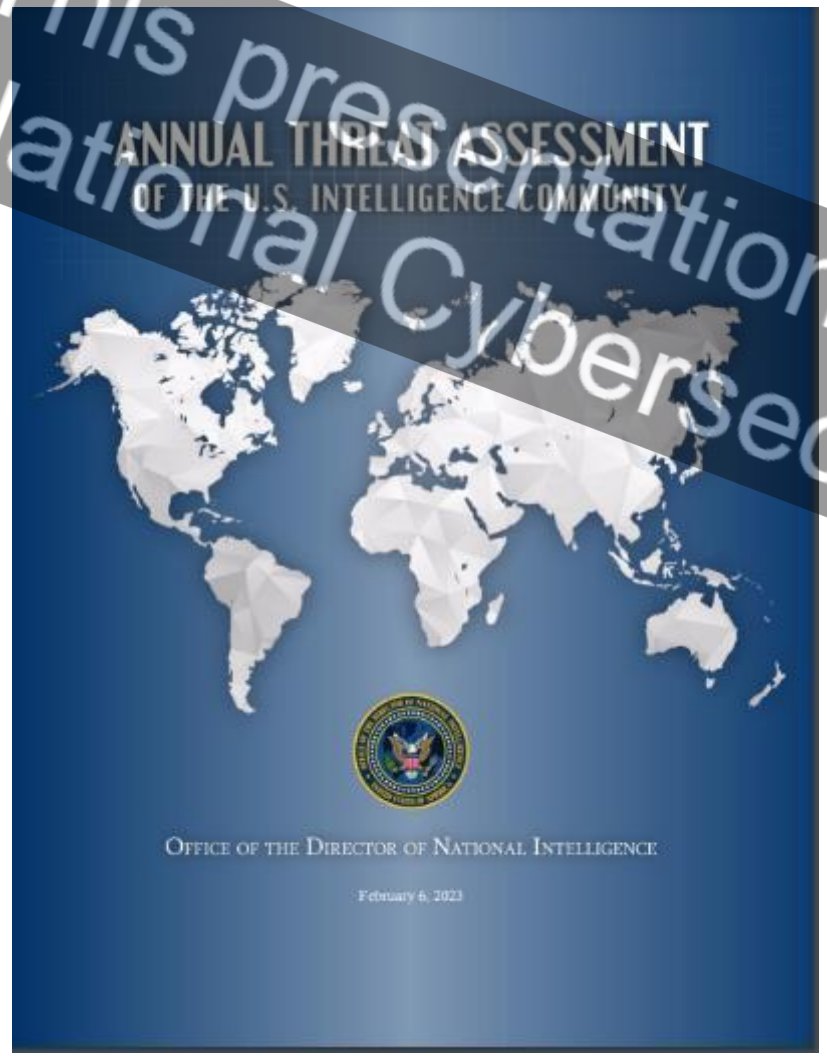
## Evolving Threats to Energy Infrastructure

# CESER Priorities

- **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.

# Cybersecurity Threats






- "**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 [...]*" [3]
- "**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 [...]*"[1]
- "**Iran's** opportunistic approach to cyber attacks makes *critical infrastructure owners* in the United States susceptible to being targeted *[...]*"[3]
- "**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 [...]*"[2]

*Annual Threat Assessment of the U.S. Intelligence Community*
[1]*2019,* [2]*2022,* [3]*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

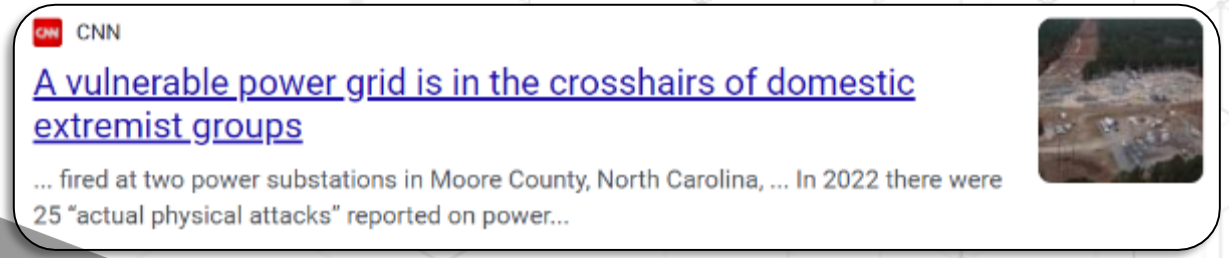
**Russian Hackers Tried Damaging Power Equipment, Ukraine**

...

... 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



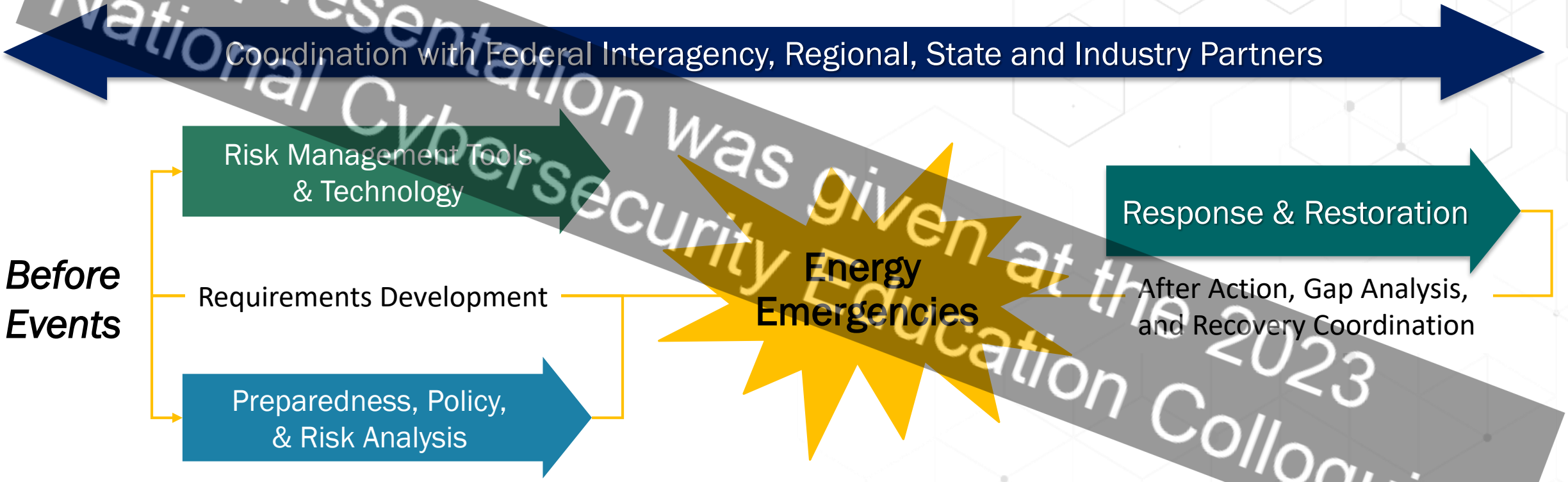




Information provided by E-ISAC

# How We Work: Energy Risk Management






DOE is the ***Sector Risk Management Agency*** for the Energy Sector
DOE is the federal coordinating agency for Emergency Support Function #12 (Energy)

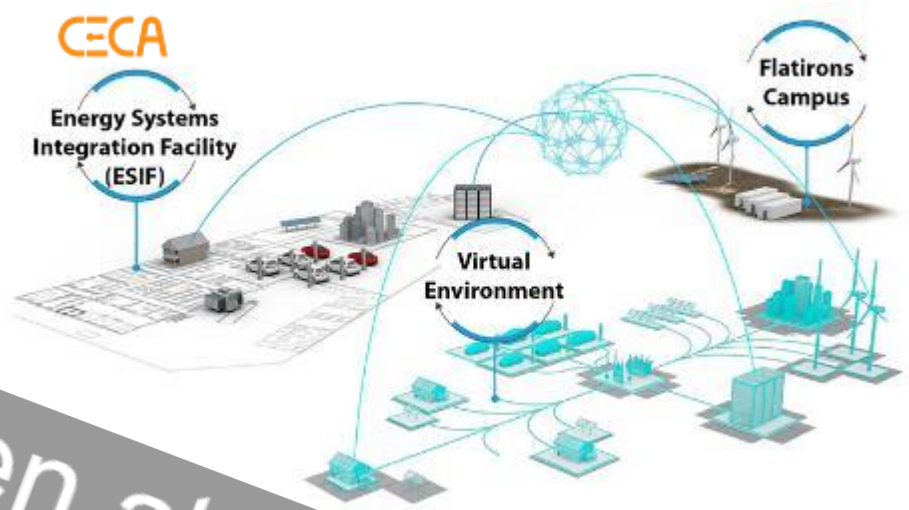
# CESER Tools & Technologies



CESER leads research, development and demonstration of tools, technologies, and techniques that help mitigate and manage cyber and physical risks to critical energy systems.

This includes:

- **All-hazards Tools and Technologies** to address natural and human made physical risks to energy systems such as extreme weather, climate change, seismic activity, electromagnetic pulse (EMP) and geomagnetic disturbances (GMD)
- **Cyber Tools and Technologies** that enable innovative protection, detection, and response solutions to address energy delivery systems and supply chain cybersecurity risks and enable situational awareness and information sharing.



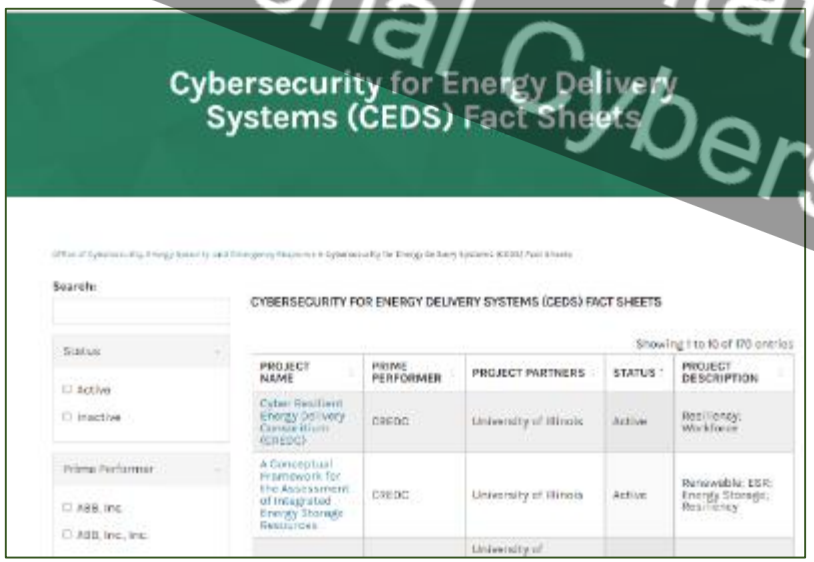

**Clean Energy Cybersecurity Accelerator (CECA)**
Test Range


**Cyber Testing for Resilient Industrial Control Systems (CyTRICS)**
Testing Methodology

# CESER Tools & Technologies



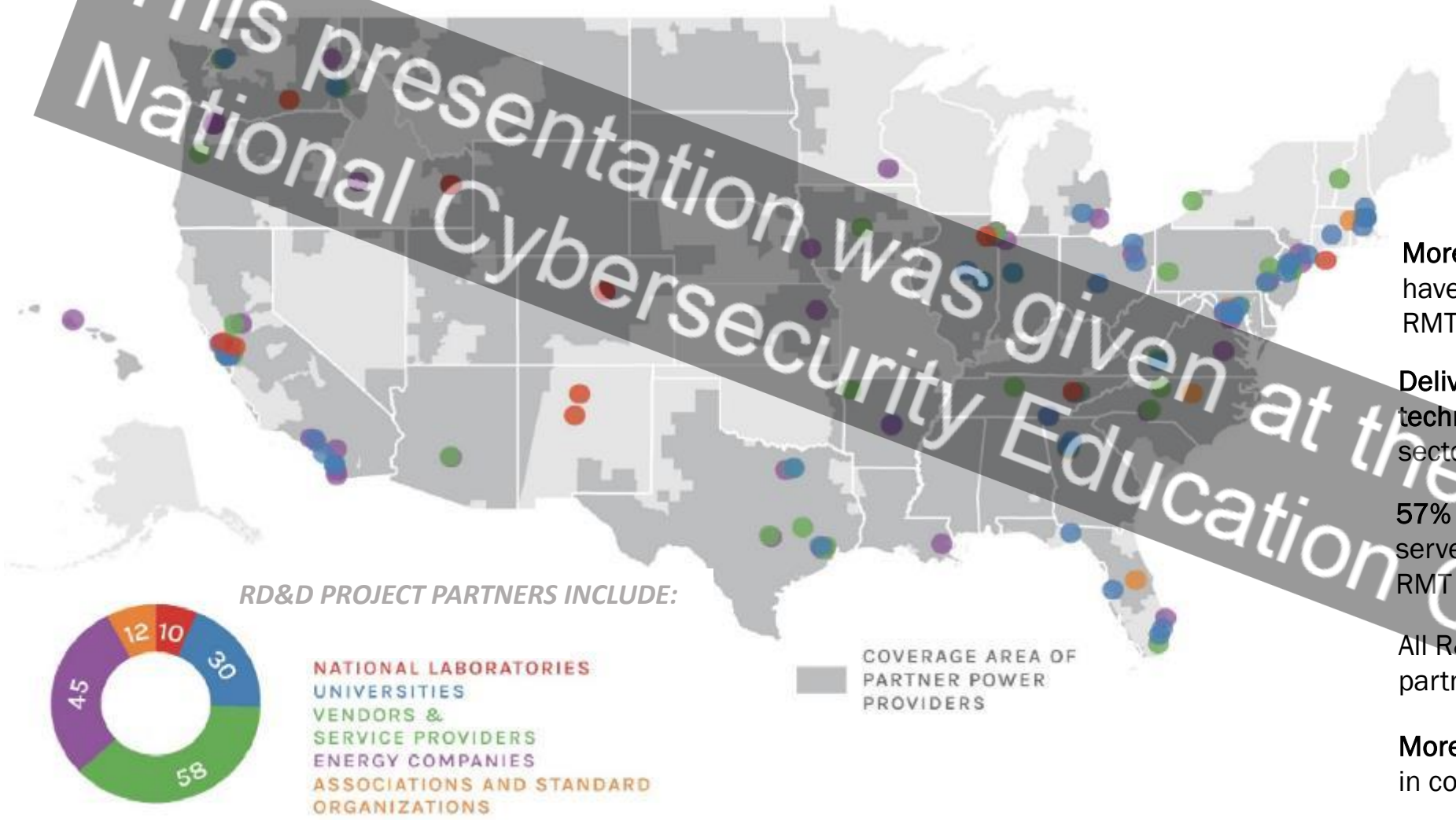
**Today's research is tomorrow's capabilities**




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

# Cyber Research, Development, and Deployment






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

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

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

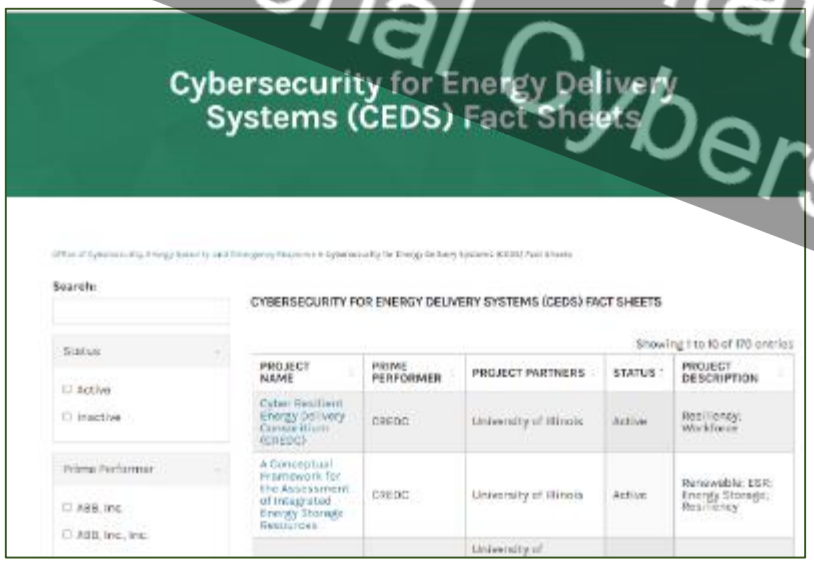
All R&D projects included an energy sector partner to drive **real-world solutions**

**More than 155 partners** have participated in competitively funded projects

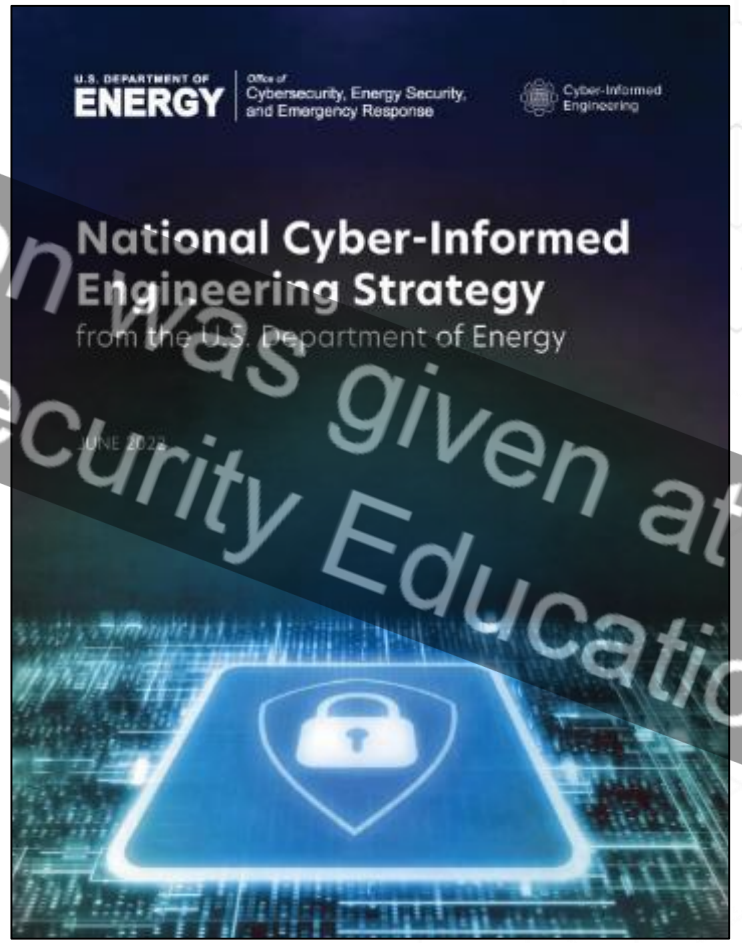
# CESER Tools & Technologies



Today's research is tomorrow's capabilities




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

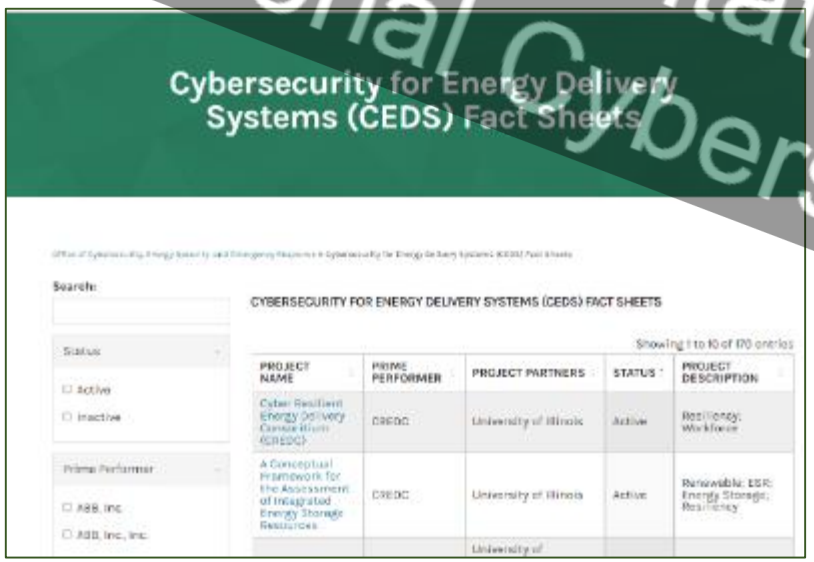



[FINAL DOE National CIE Strategy - June 2022_0.pdf (energy.gov)]

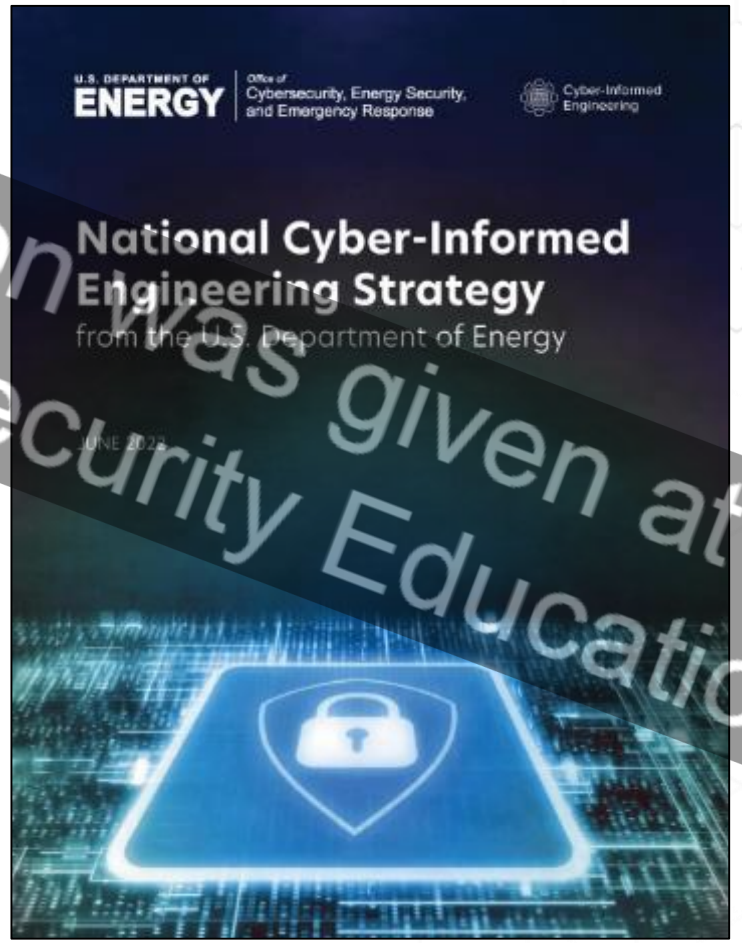
# CESER Tools & Technologies



Today's research is tomorrow's capabilities




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




[FINAL DOE National CIE Strategy - June 2022_0.pdf (energy.gov)]

C2M2

Cybersecurity Capability Maturity Model

# 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

# C2M2 Model: 10 Domains

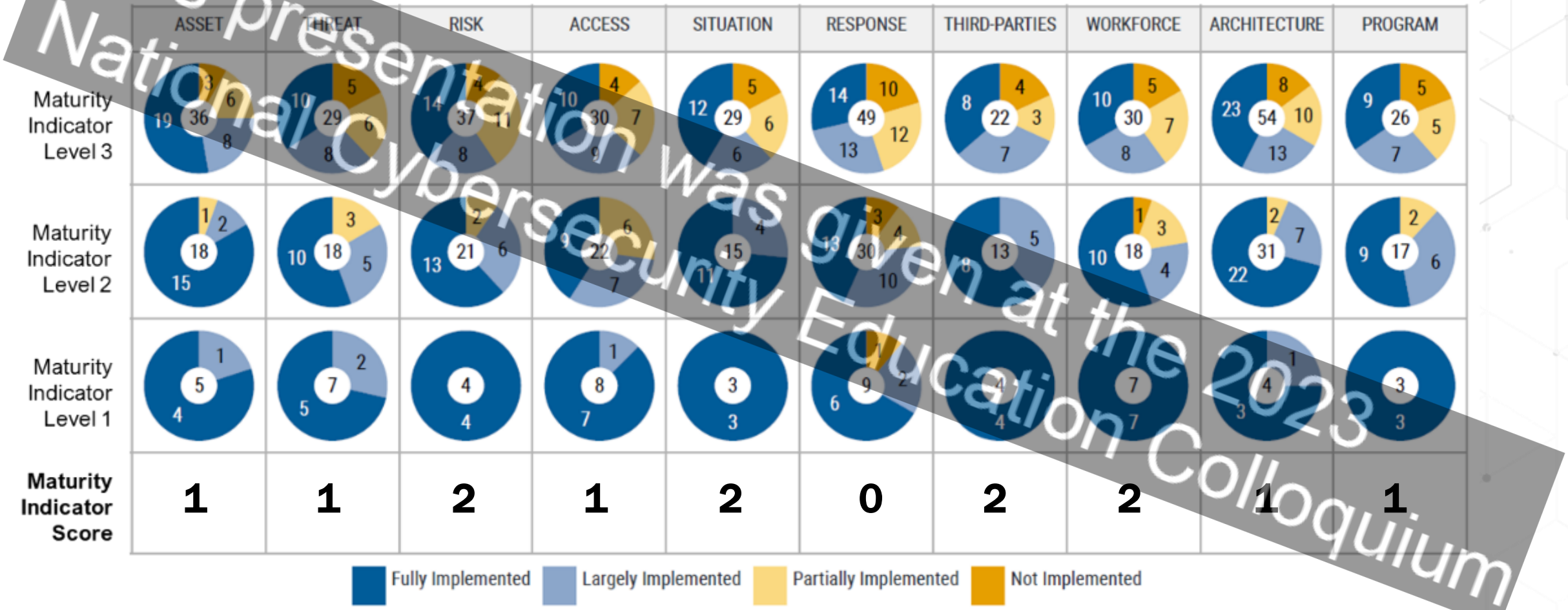
1. Asset, Change, and Configuration Management (ASSET)
2. Threat and Vulnerability Management (THREAT)
3. Risk Management (RISK)
4. Identify and Access Management (ACCESS)
5. Situational Awareness (SITUATION)
6. Event and Incident Response, Continuity of Operations (RESPONSE)
7. Third-Party Risk Management (THIRD-PARTIES)
8. Workforce Management (WORKFORCE)
9. Cybersecurity Architecture (ARCHITECTURE)
10. Cybersecurity Program Management (PROGRAM)

# C2M2 Maturity Indicator Levels (MIL)

| Level | Characteristics |
|---|---|
| MIL0 | • Practices are not performed |
| MIL1 | • Initial practices are performed but may be ad hoc |
| MIL2 | Management characteristics:<br>• Practices are documented<br>• Adequate resources are provided to support the process<br>Approach characteristic:<br>• Practices are more complete or advanced than at MIL1 |
| MIL3 | Management characteristics:<br>• Activities are guided by policies (or other organizational directives)<br>• Responsibility, accountability, and authority for performing the practices are assigned<br>• Personnel performing the practices have adequate skills and knowledge<br>• The effectiveness of activities is evaluated and tracked<br>Approach characteristic:<br>• Practices are more complete or advanced than at MIL2 |

# C2M2 Results





# CESER as the SRMA



Energy was identified as one of the 16 critical functions in Presidential Policy Directive-21 (PPD-21). Each critical function has an associated Sector Risk Management Agency (SRMA). The Department of Energy is the SRMA for energy. CESER is tasked to carry out this function as a core part of its mission.

The SRMA is responsible for:

- Representing sector-specific interests in the national cybersecurity strategy
- Leading sector incident management response
- Providing technical and logistics support for the energy sector to identify risks and vulnerabilities
- Supporting the Department of Homeland Security Cybersecurity & Infrastructure Security Agency's (CISA) role as national cyber response coordinator

# Response and Restoration



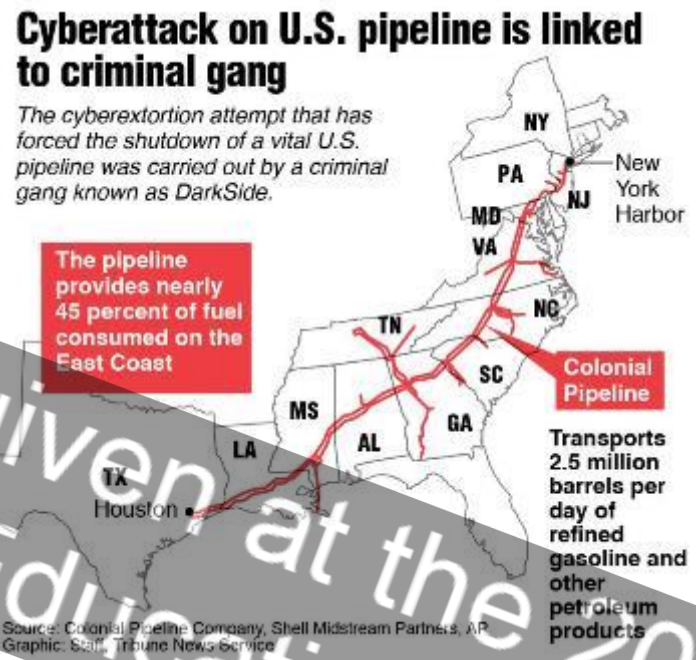
**Facilitating the restoration of disrupted or damaged energy systems**

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

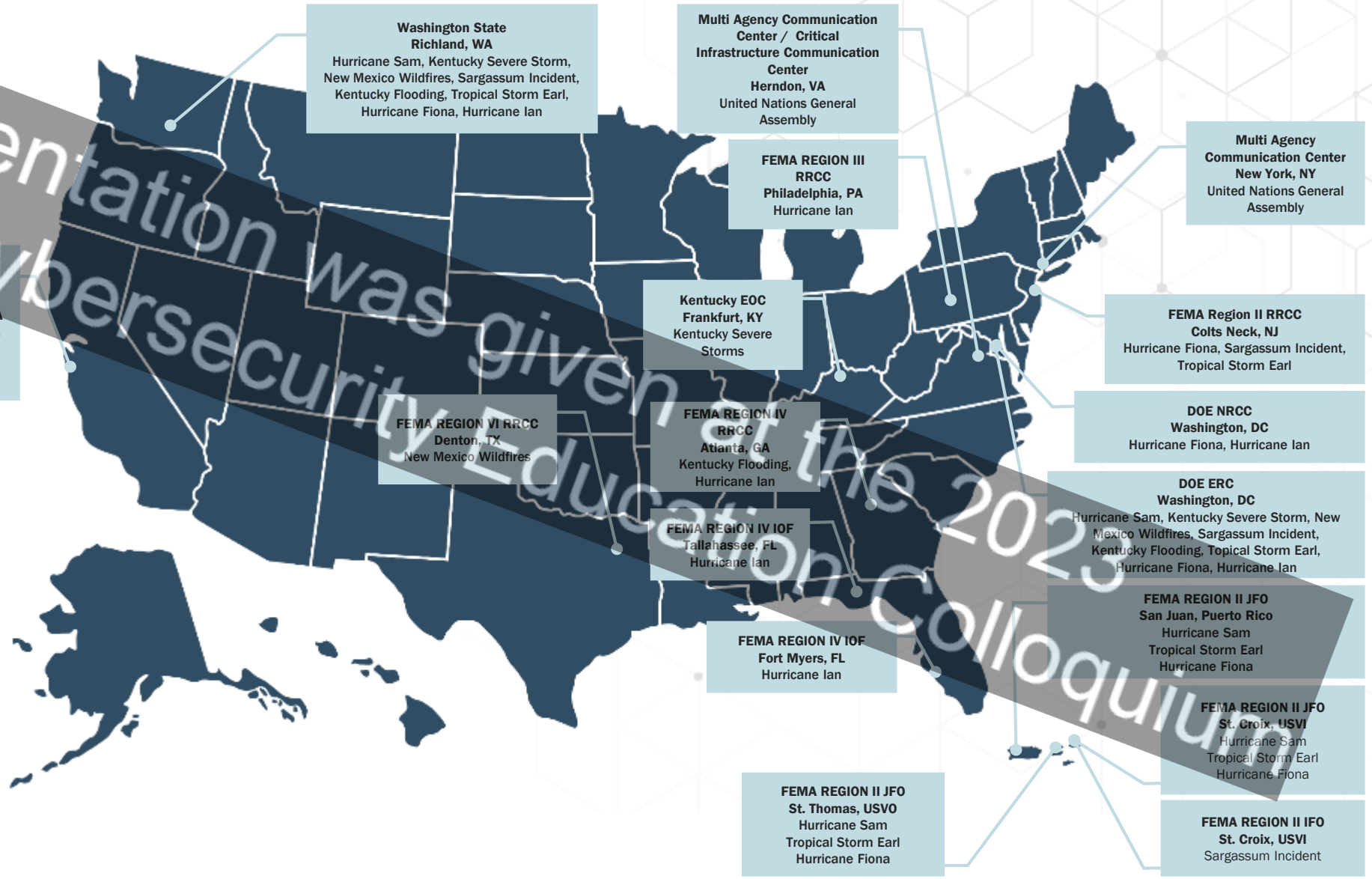



# 2022 Response Summary

**169** Days Activated

**38** Responders Deployed

- Three Hurricanes
- One Tropical Storm
- Severe Winter Weather
- Flooding
- Wildfires
- Sargassum Seaweed Overgrowth
- Four National Special Security Events



# Collaboration and Coordination is Essential



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

Industry Trade Assoc.

Industry Councils

Energy Government Coordinating Council (EGCC)

NASEO
National Association of State Energy Officials

NCSL

NATIONAL GOVERNORS ASSOCIATION

NEMA™

EEI
Edison Electric Institute

NRECA
America's Electric Cooperatives

AMERICAN PUBLIC POWER ASSOCIATION

ESCC
Electricity Subsector Coordinating Council

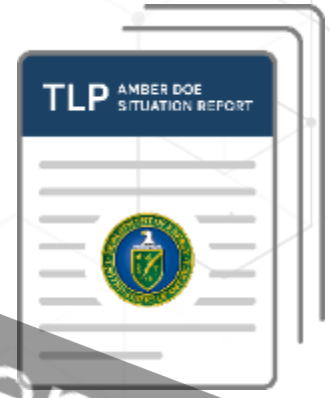
OIL AND NATURAL GAS SUBSECTOR COORDINATING COUNCIL

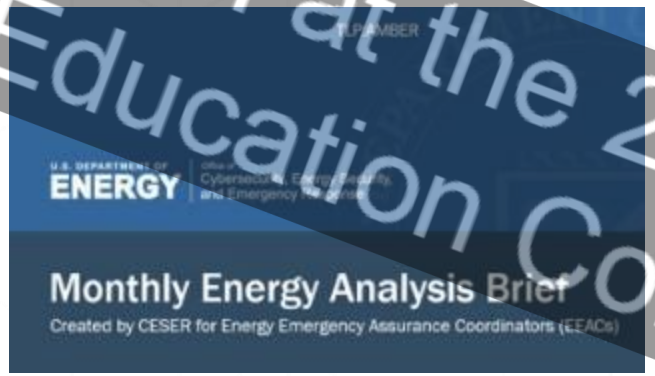
NASEO NARUC NGA

# Energy Emergency Assurance Coordinators (EEACs)



- The **EEAC Program** is a cooperative effort between CESER, NASEO, NARUC, NGA and NEMA to enable information sharing leading up to and during an energy disruption or emergency
- States designate primary and secondary contacts to share information with DOE and other states during events
- Provides credible, accurate, and timely source of information and updates on actions taken.
- Goal is to improve information-sharing and communication and lower response times.
- To provide ongoing situational awareness, the SLTT Program distributes Monthly Energy Analysis briefs that analyze the impact and significance of energy disruptions.

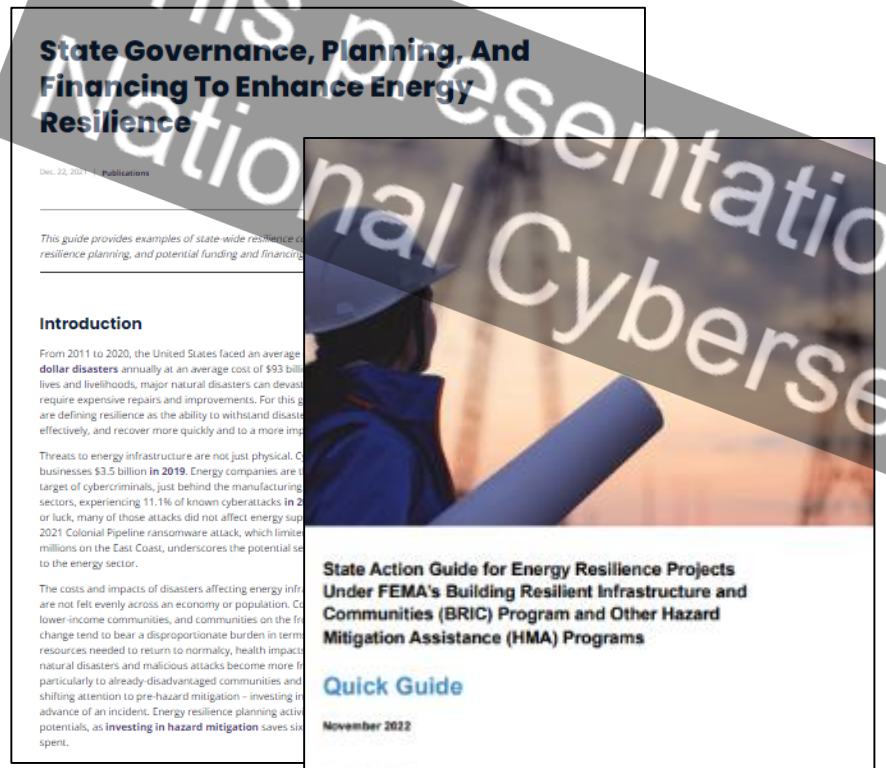



[Energy Emergency Assurance Coordinators (EEAC) Program]

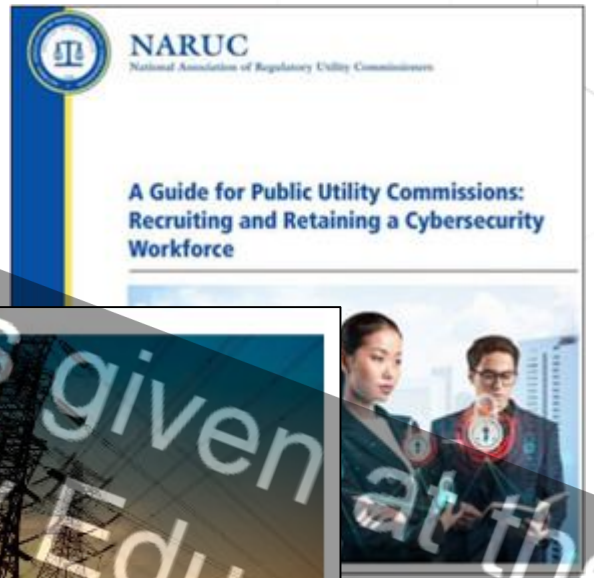
# SLTT Capacity Building

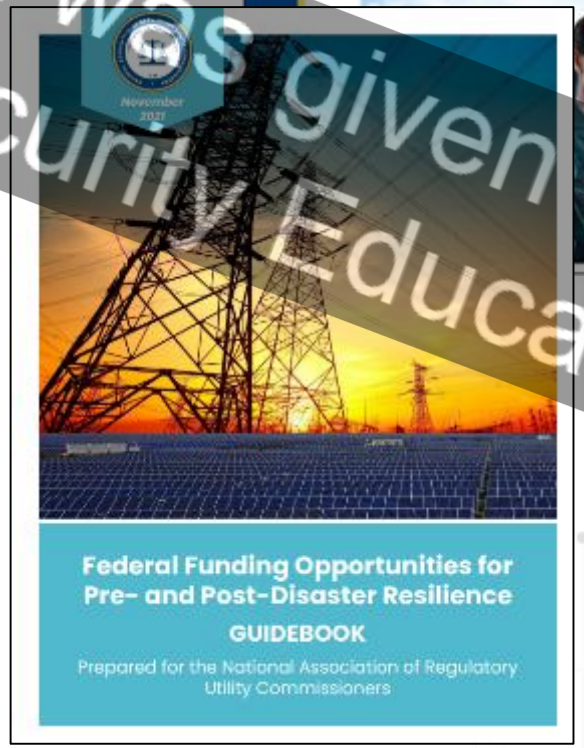


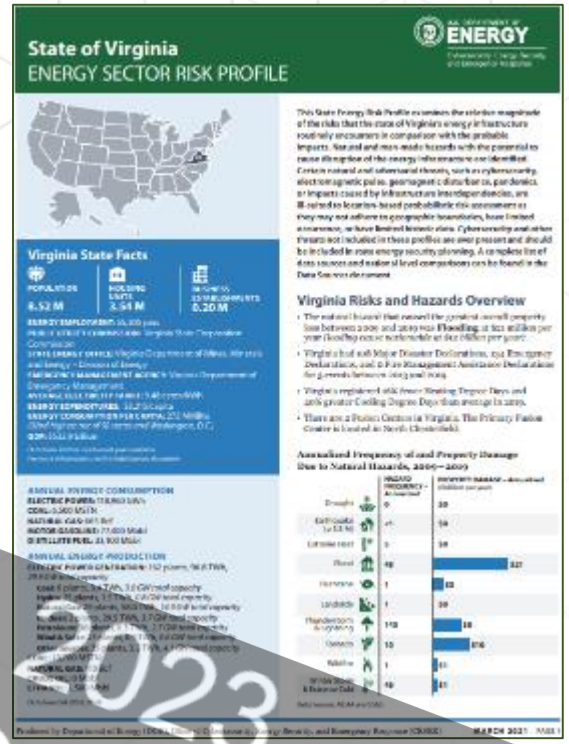


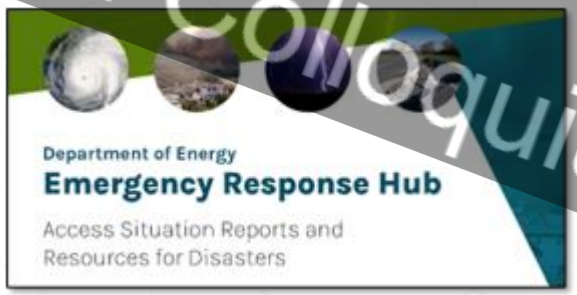






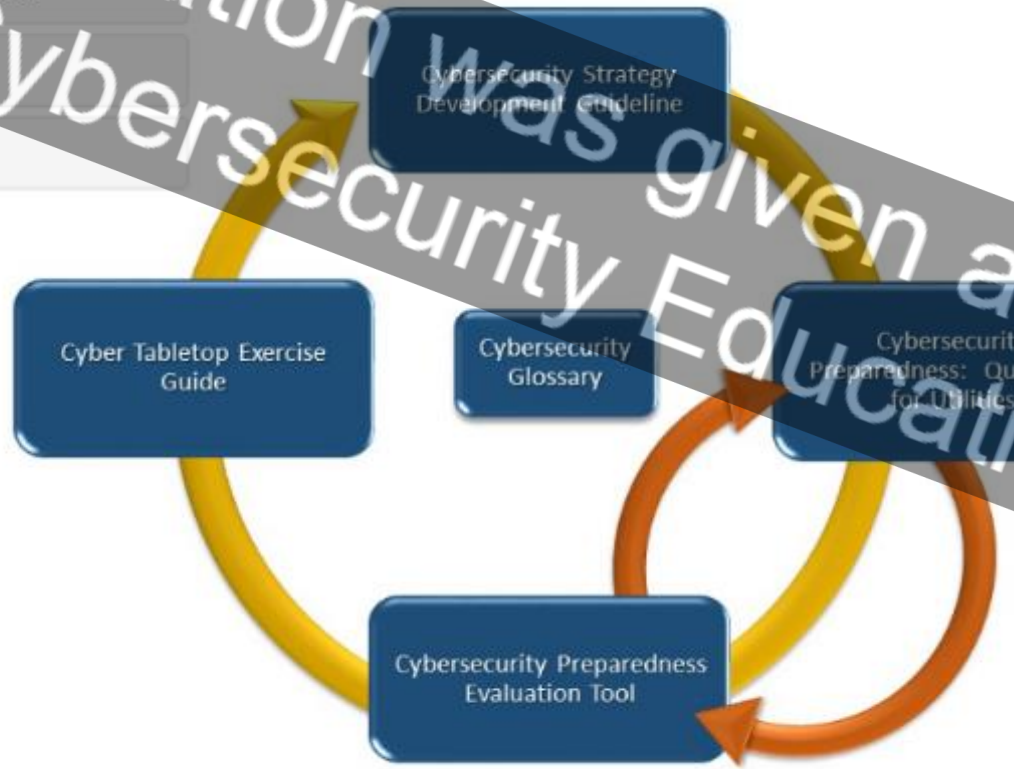



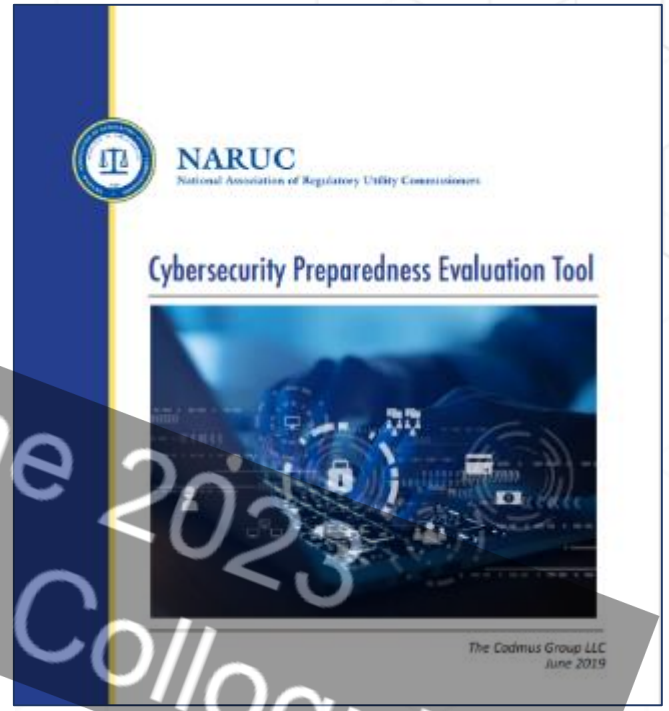




[SLTT Program Resource Library]

# NARUC Cybersecurity Manual

- Cybersecurity Strategy Development Guide
- Cybersecurity Preparedness: Questions for Utilities
- Cybersecurity Preparedness Evaluation Tool
- Cybersecurity Tabletop Exercise Guide
- Cybersecurity Glossary



# President Biden's Letter to Governors


March 18, 2022

## Letter Urging States to put mandatory Cybersecurity Protections in Place

Questions in the Letter:

- "Do you have the authority to set and enforce cybersecurity baselines standards for the utilities in your state, and if so, have you done it?
- Have the Public Utility Commissions or others in your state set minimum cybersecurity standards for your critical infrastructure? If not, ask them to do so.
- Do you or your Public Utility Commissions have the ability to require critical infrastructure to take emergency cybersecurity measures? If so, have you or they required utilities to step up their security in light of the current conflict?
- Have you and your emergency management team considered how you would respond to a cyber attack that has physical consequences, including impact to the operations of your critical infrastructure?"

# Exercises



## Clear Path

Annual all-hazards energy security and resilience exercise.

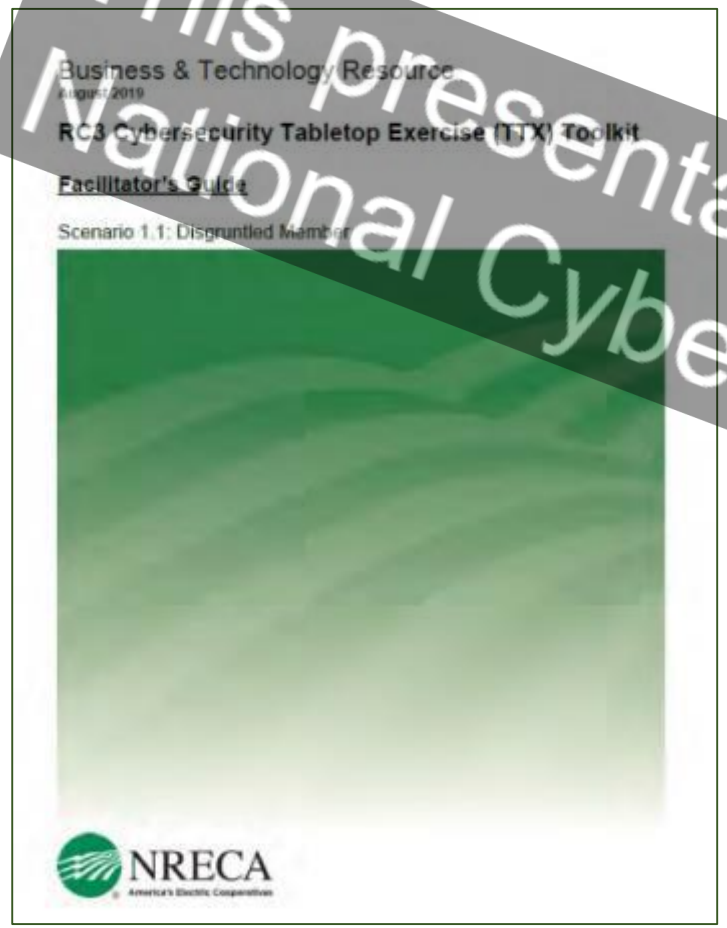
DOE has engaged over 1,400 energy sector and cross-infrastructure sector partners

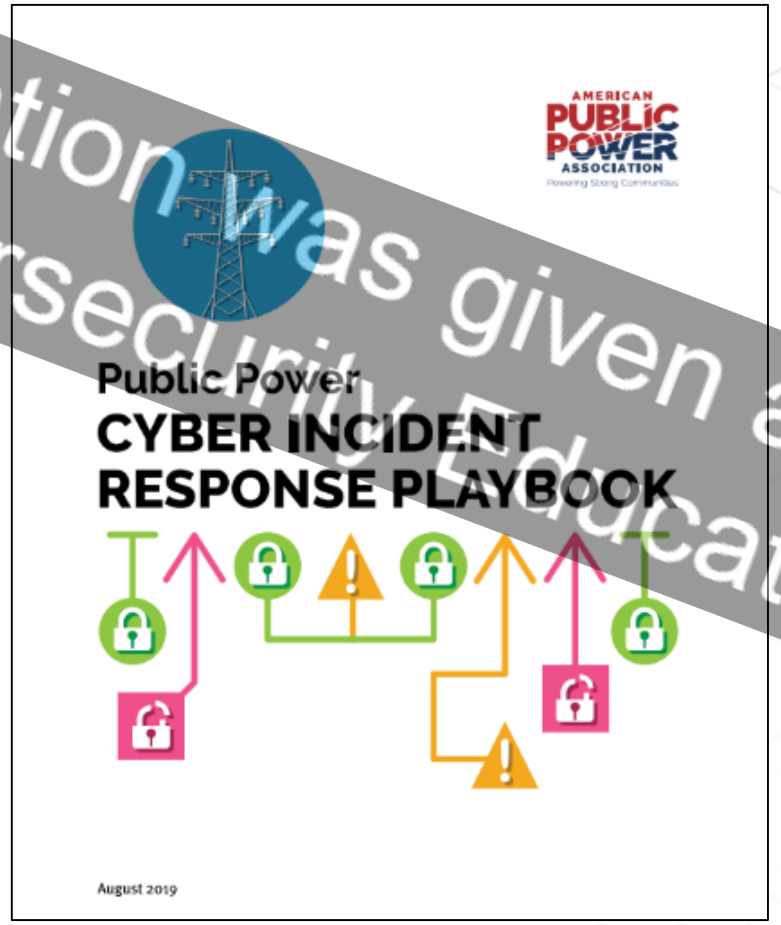

## Liberty Eclipse

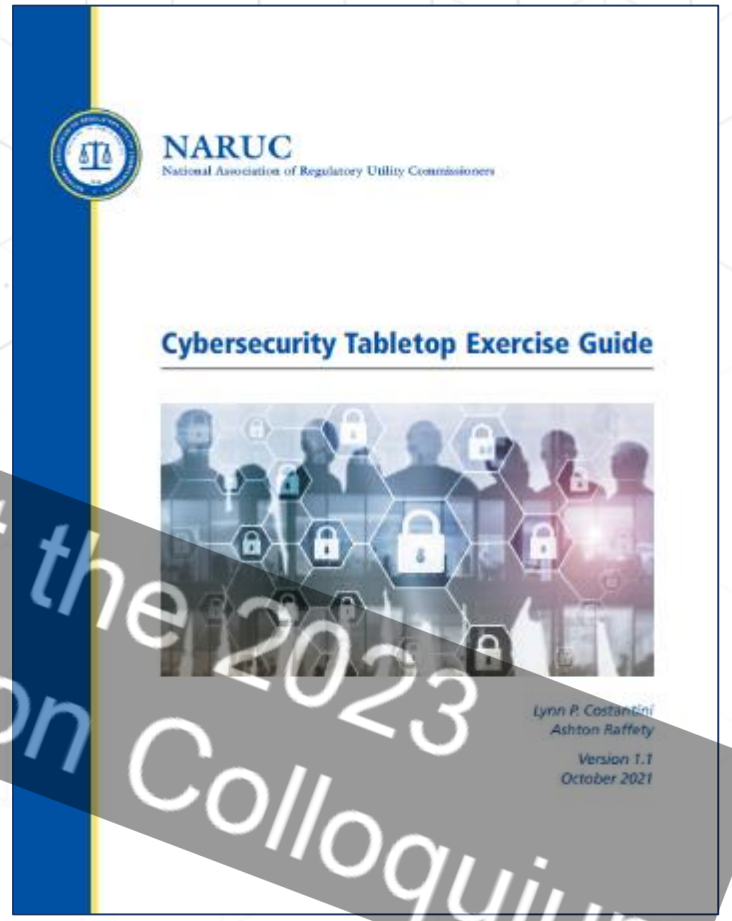
ICS-focused energy cybersecurity exercise

# Exercises





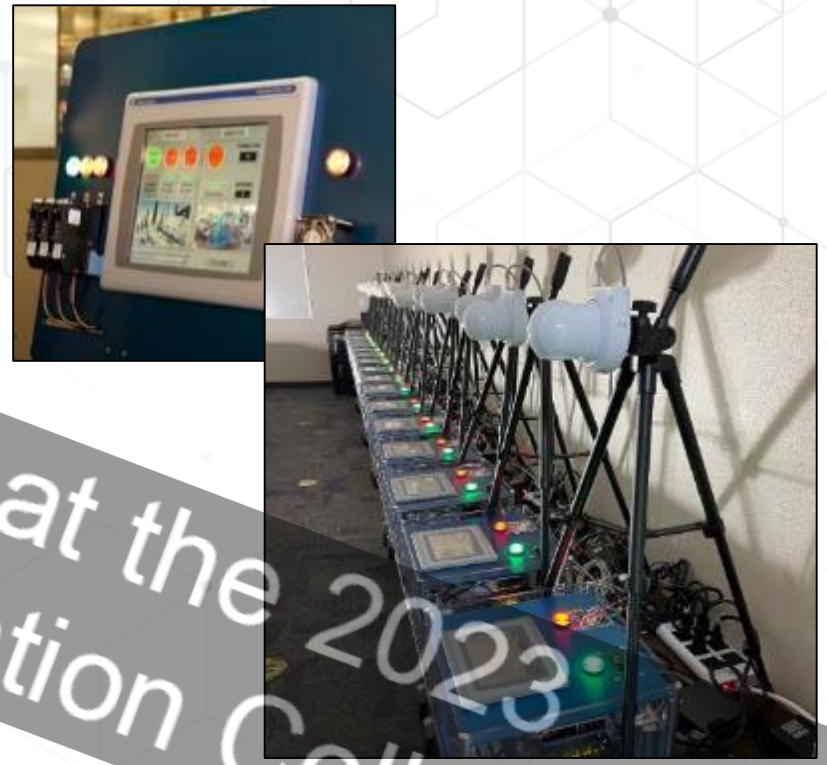




[Cybersecurity Tabletop Exercise]

# Training and Workforce Development



- 82 training sessions
- Trained approximately 3,700 personnel

CyberStrike Training - INL

# Training and Workforce Development

- 3rd Cohort
- 21 Alumni




OTDefender: Operational Technical Defender Fellowship (inl.gov)

# Training and Workforce Development



- 3rd Cohort
- 21 Alumni

4th Cohort Applications now being accepted

DUE: September 30, 2023


OTDefender: Operational Technical Defender Fellowship (inl.gov)

# 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.

https://cyberforce.energy.gov

# Training and Workforce Development




### 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




### 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.

Registration is open to students through September 29th for the November 4, 2023, CyberForce Competition

https://cyberforce.energy.gov

# Bipartisan Infrastructure Law (BIL) Key Opportunities



The IIJA includes over $62B for the U.S. Department of Energy to deliver a more equitable clean energy future.

**Cybersecurity Workforce Provisions :**

- Cybersecurity for electric utilities: **40124**
- Cybersecurity curriculum: **40125(b)**

DOE BIL Homepage
BIL Programs at Department of Energy
NGA IIJA Implementation Resources

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



**Funding:**

$250 million over 5 years (FY22-26) via grants, technical assistance, and cooperative agreements

**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**.

# RMUC Program Eligibility and Priorities



**Eligibility:**

- Rural electric cooperatives (~900)
- Municipal electric 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)
- Municipal electric 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 Eligibility and Priorities

# RMUC Eligibility



| Cooperative | Municipal | Investor-Owned (IOU) |
| --- | --- | --- |

# RMUC Eligibility



| Cooperative | Municipal | IOU |
| --- | --- | --- |

# RMUC Priorities



| Cooperative | Municipal | IOU |
| --- | --- | --- |
| Utilities with limited cybersecurity resources | | |

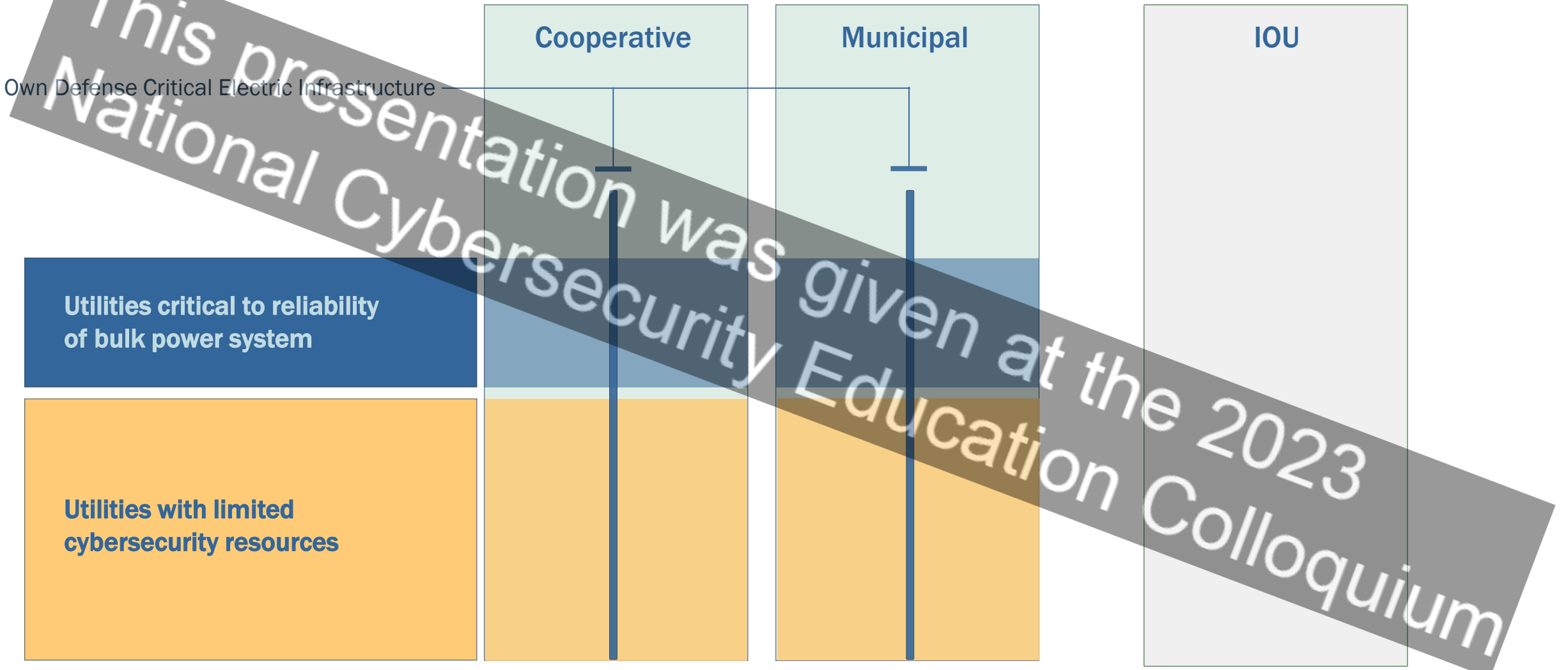
# RMUC Priorities



| | Cooperative | Municipal | IOU |
|---|---|---|---|
| Utilities critical to reliability of bulk power system | | | |
| Utilities with limited cybersecurity resources | | | |

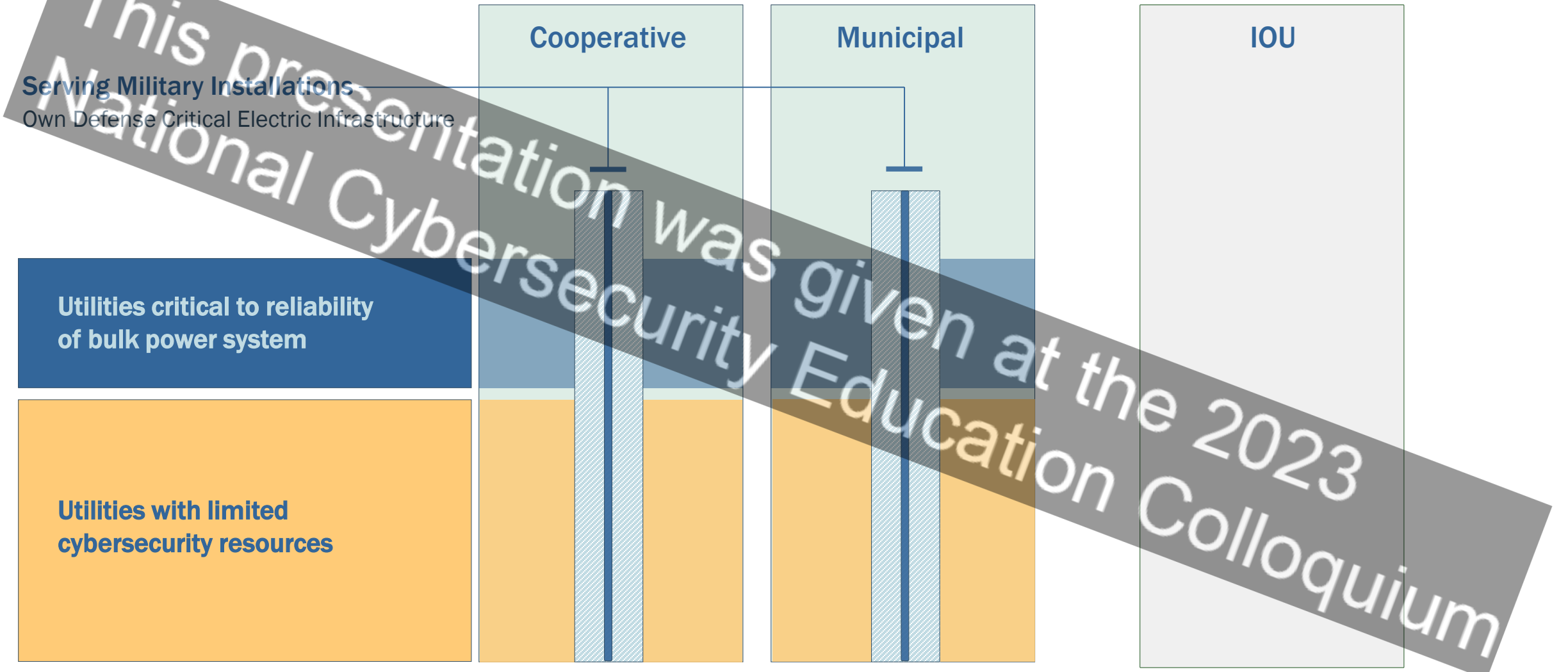
# RMUC Priorities





# RMUC Priorities

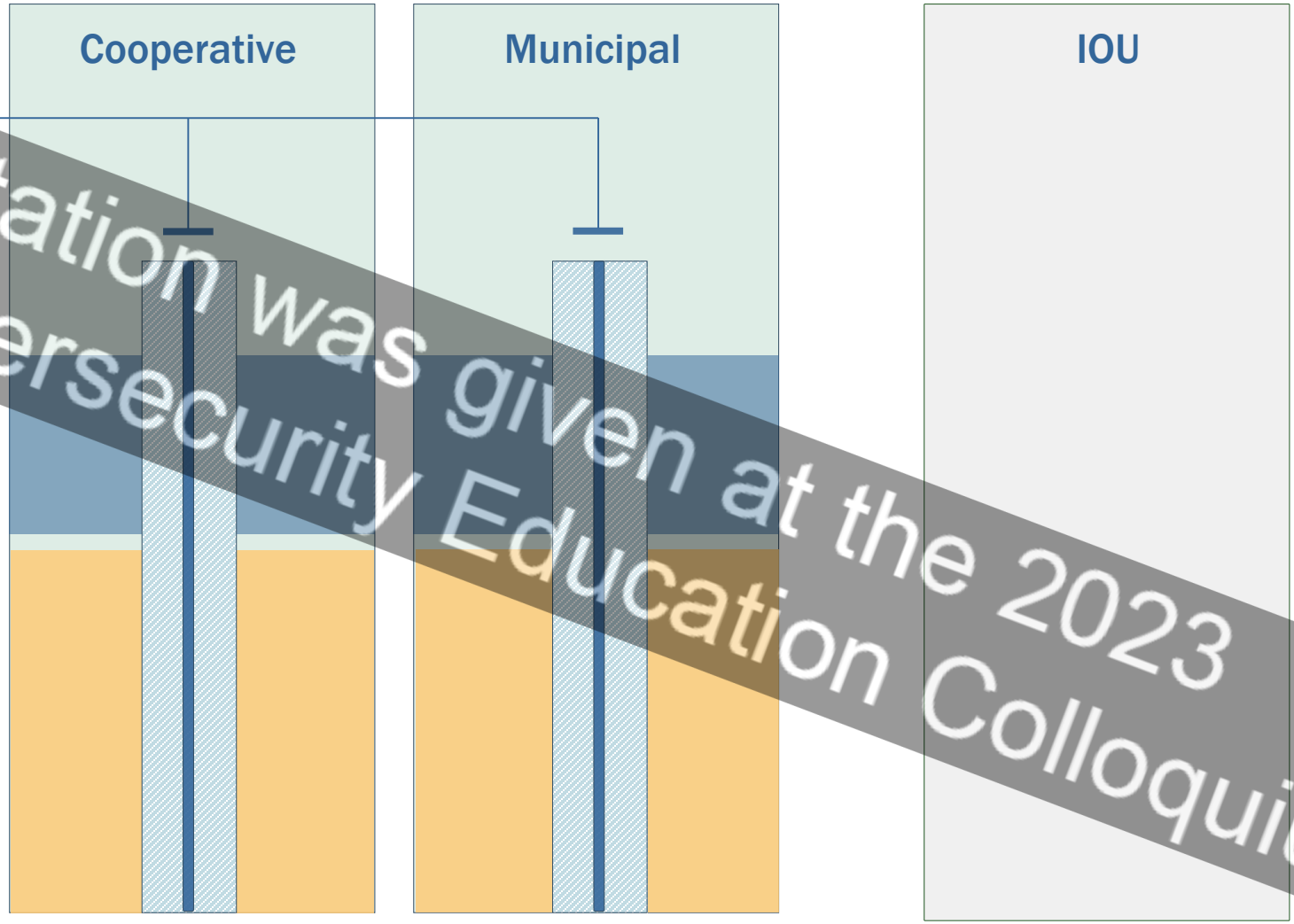




# RMUC Eligibility

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



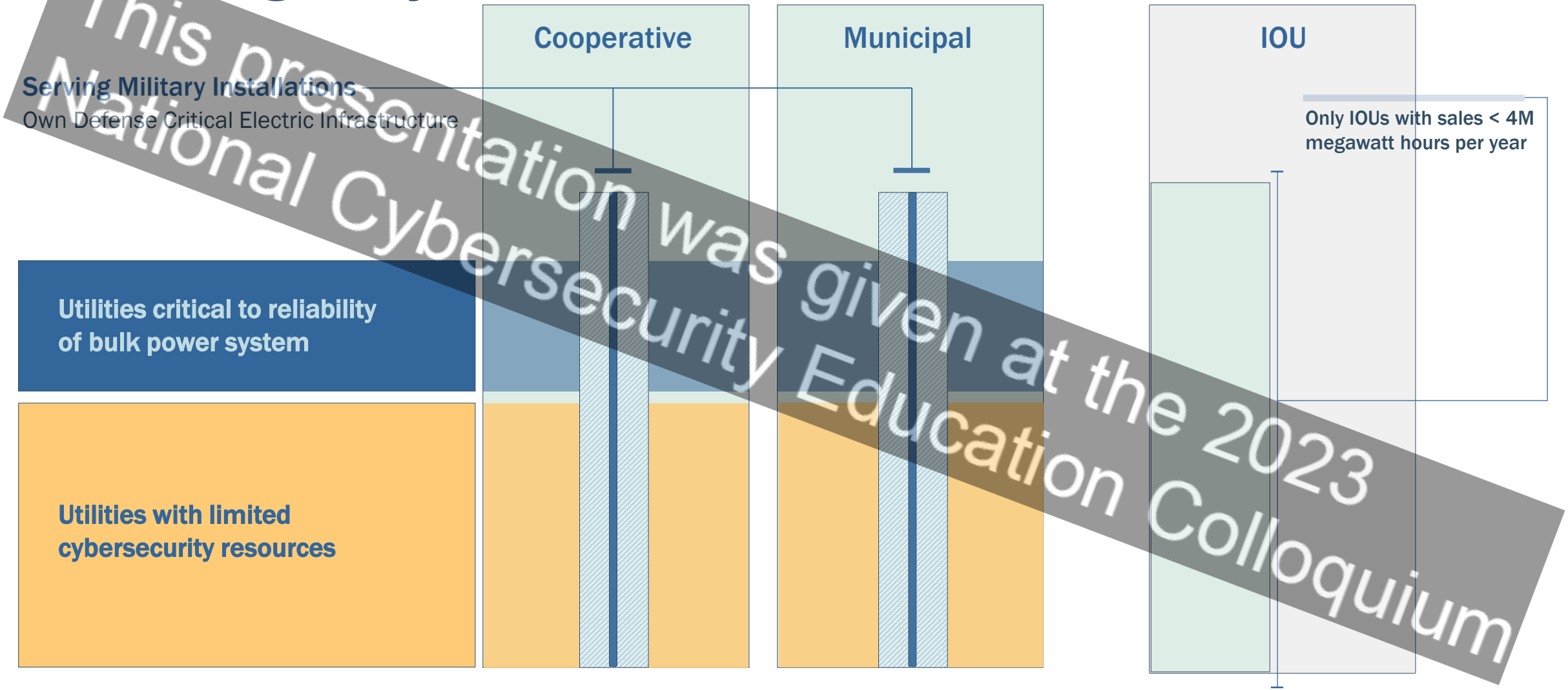

**Utilities critical to reliability of bulk power system**

**Utilities with limited cybersecurity resources**

# RMUC Eligibility

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

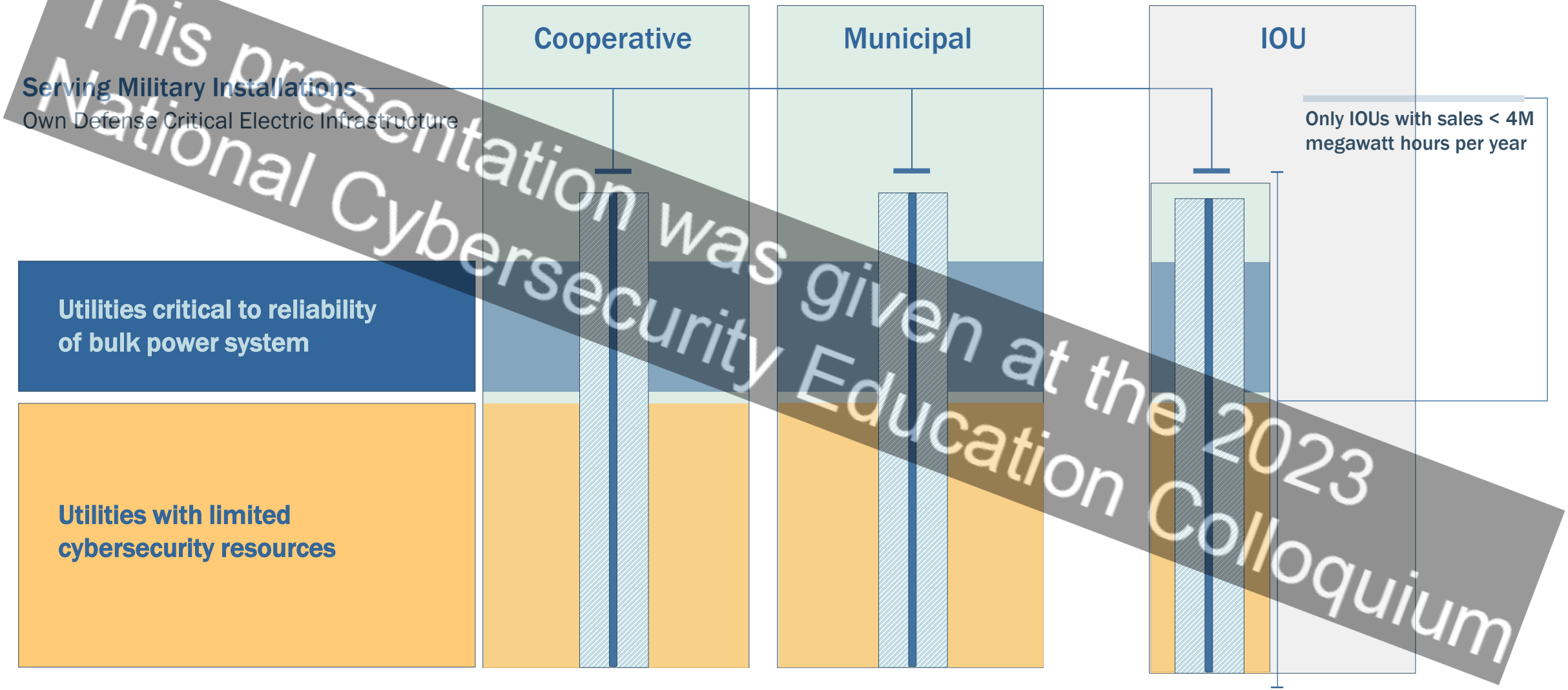
**Serving Military Installations -**
Own Defense Critical Electric Infrastructure



# 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



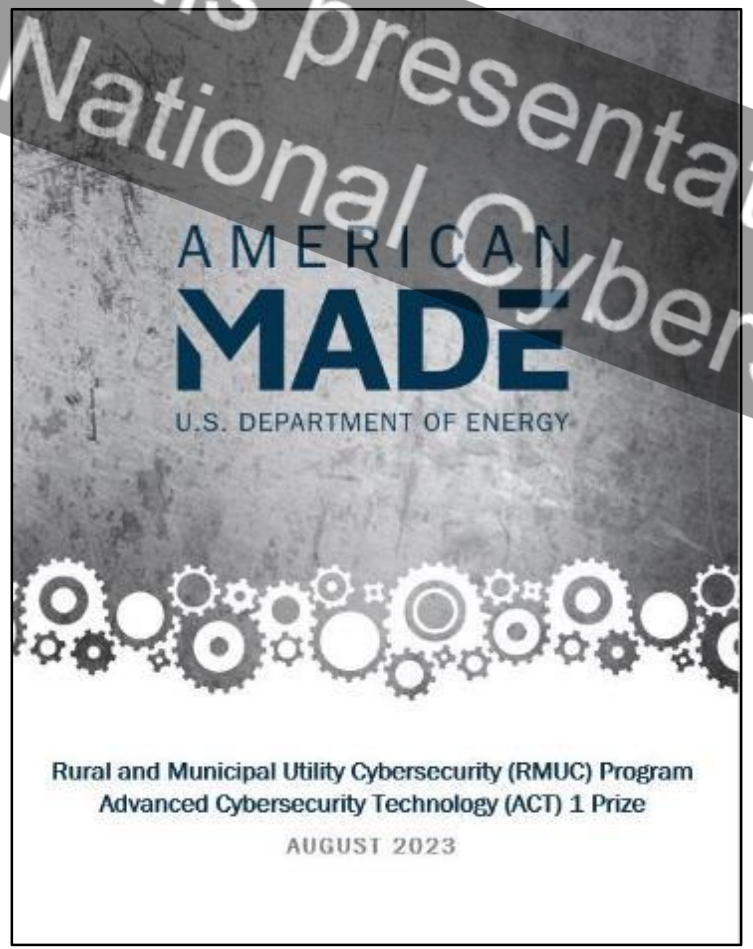
# RMUC Program:
# Advanced Cybersecurity Technology (ACT) 1 Prize




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




- Minimal administrative burden.
- $8.96 Million:
  - $7.25 in cash awards
  - $1.71 in technical assistance vouchers
- Up to 55 utilities will win an ACT 1 Prize
- Priority:
  - Utilities with limited cybersecurity resources
  - Utilities service military installations
- ACT 1 is the first in the ACT Prize Program series

# ACT 1 Prize Structure



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 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 technical assistance providers to make progress toward completing their implementation roadmap.

# ACT 1 Prizes



| Prize Phase | LIMITED CYBERSECURITY RESOURCES Track | MILITARY Track |
|---|---|---|
| Commitment | • $50,000<br>• Up to 60 hours of TA<br>• Up to 50 winners | • $50,000<br>• Up to 120 hours of TA<br>• Up to 5 winners |

# ACT 1 Prizes



| Prize Phase | LIMITED CYBERSECURITY RESOURCES Track | MILITARY Track |
|---|---|---|
| Commitment | • $50,000<br>• Up to 60 hours of TA<br>• Up to 50 winners | • $50,000<br>• Up to 120 hours of TA<br>• Up to 5 winners |
| Planning | • $50,000<br>• Up to 60 hours of TA<br>• Up to 25 winners | • $50,000<br>• Up to 120 hours of TA<br>• Up to 5 winners |

# ACT 1 Prizes

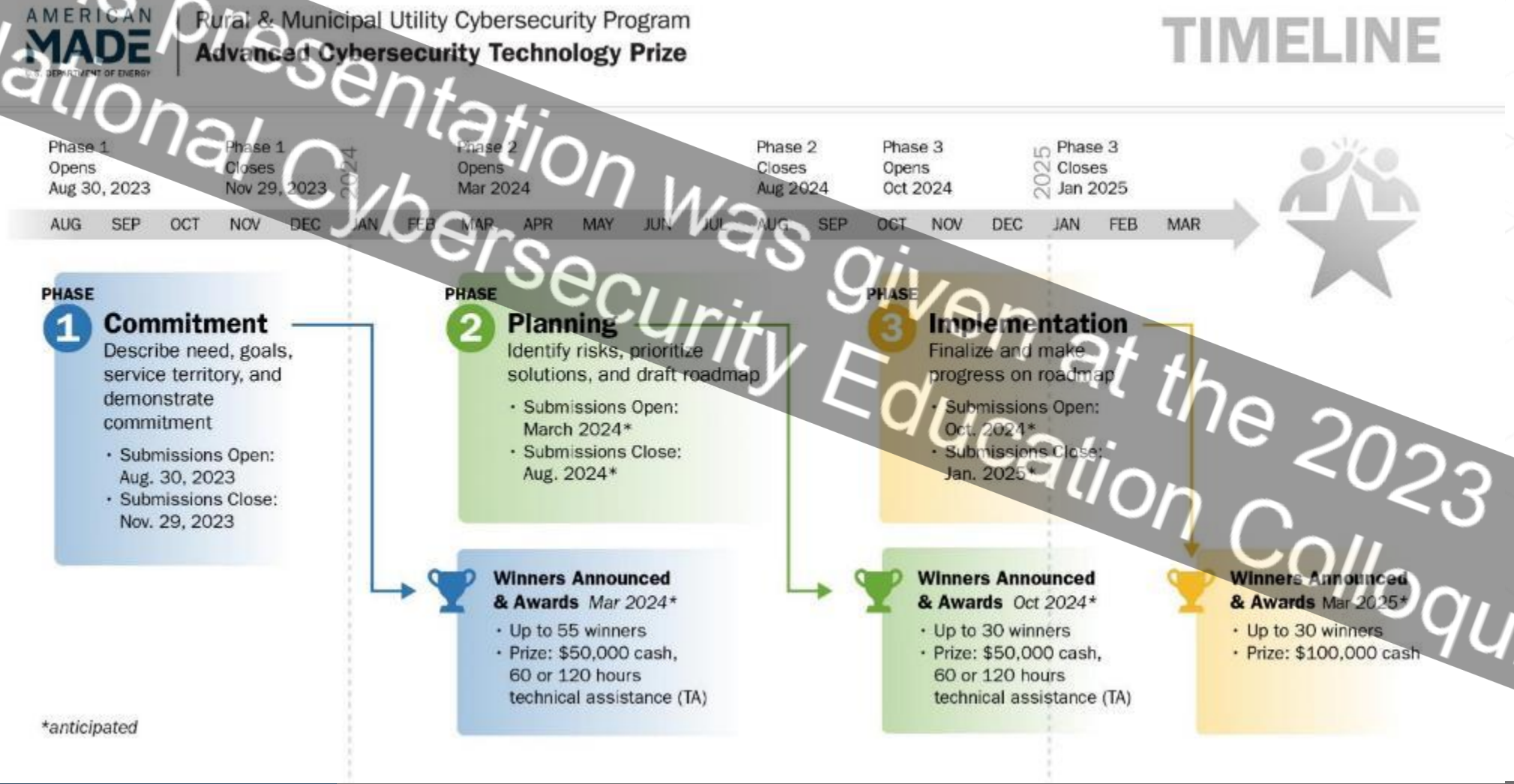


| Prize Phase | LIMITED CYBERSECURITY RESOURCES Track | MILITARY Track |
|---|---|---|
| Commitment | • $50,000<br>• Up to 60 hours of TA<br>• Up to 50 winners | • $50,000<br>• Up to 120 hours of TA<br>• Up to 5 winners |
| Planning | • $50,000<br>• Up to 60 hours of TA<br>• Up to 25 winners | • $50,000<br>• Up to 120 hours of TA<br>• Up to 5 winners |
| Implementation | • $100,000<br>• Up to 25 winners | • $100,000<br>• Up to 5 winners |
| **Total potential cumulative award*** | **• $200,000<br>• 120 hours of TA** | **• $200,000<br>• 240 hours of TA** |

* If utility wins all three phases

# ACT 1 Prize Timeline





# RMUC Program ACT 1 Prize



Applications Due:
November 29, 2023


https://www.herox.com/ACT1Prize

# RMUC Program: ICS Cybersecurity Training



**Industrial Control Systems Cybersecurity Training**

- Tuesday-Thursday, October 31-November 2, 2023: Columbus, OH
- Tuesday-Thursday, November 28-30, 2023: Orlando, FL
- Tuesday-Thursday, December 5-7, 2023: Kansas City, MO
- Wednesday-Friday, January 17-19, 2024: San Diego, CA
- Tuesday-Thursday, January 23-25, 2024: Dallas, TX
- Tuesday-Thursday, April 23-25, 2024: Buffalo, NY

# RMUC Program: ICS Cybersecurity Training



## Advanced Cybersecurity Technology (ACT)

## Funding Opportunity Announcement

# 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

# Section 40125(b) Cybersecurity for the Energy Sector Research, Development, and Demonstration Program



40125(b)

(1) (D) to develop workforce development curricula for energy sector-related cybersecurity

# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?
- Not training the right audience(s)
- Recruitment issue
  - Potential candidates not interested
  - Human resources infrastructure

# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?
- Not training the right audience(s)
- Recruitment issue
  - Potential candidates not interested
  - Human resources infrastructure

# Pipeline

Where do energy asset owners and operators go to recruit cybersecurity subject matter experts that understand ICS/OT cybersecurity?

# Closing the SA gap in KSAs

- Internship
- Engineering Co-op
- Legal Clinic
- Apprenticeship
- Medical Rotation
- Certification
- Boot Camp
- Competitions

# Engineering Co-op Model: SOC



Norwich University Applied Research Institutes (NUARI) Security Operations Center

- Dr. Sharon Hamilton, Vice President of Strategic Partnerships at Norwich University
- Initial qualification training (IQT), mission qualification training (MQT), “sit crew” – work with the SOC team on missions, receiving alerts, investigating those alerts, determining whether things are false positives or not, and writing up reports.
- playbook for all staffing, onboarding, operations, technical evaluation/acquisition, and overall program evaluation
- Certification, 70 students
- Apprenticeship

# Legal Clinic Model



## Consortium of Cybersecurity Clinics

- International network of university-based cybersecurity clinics and allies working to advance cybersecurity education.
- "Cybersecurity clinics promote hands-on learning by matching students with real clients and giving them the work experience they need to land their first job in cybersecurity." (https://cybersecurityclinics.org/blog/cyber-clinics-and-the-national-cybersecurity-workforce-strategy/)
- Students provide *pro bono* essential cybersecurity services in their local communities. (https://cybersecurityclinics.org/)
- Google committed $20 M to support the creation and expansion of cybersecurity clinics at 20 higher education institutions across the U.S. (https://blog.google/inside-google/message-ceo/commitment-cybersecurity-workforce/)

# Apprenticeship Model



## Building Apprenticeship Systems in Cybersecurity (BASIC) project

- Funded by the Closing the Skill Gap grant by the Department of Labor.
- EnergySec (https://www.energysec.org/basic/)

## Cybersecurity & Industrial Infrastructure Security Apprenticeship Program (CIISAp)

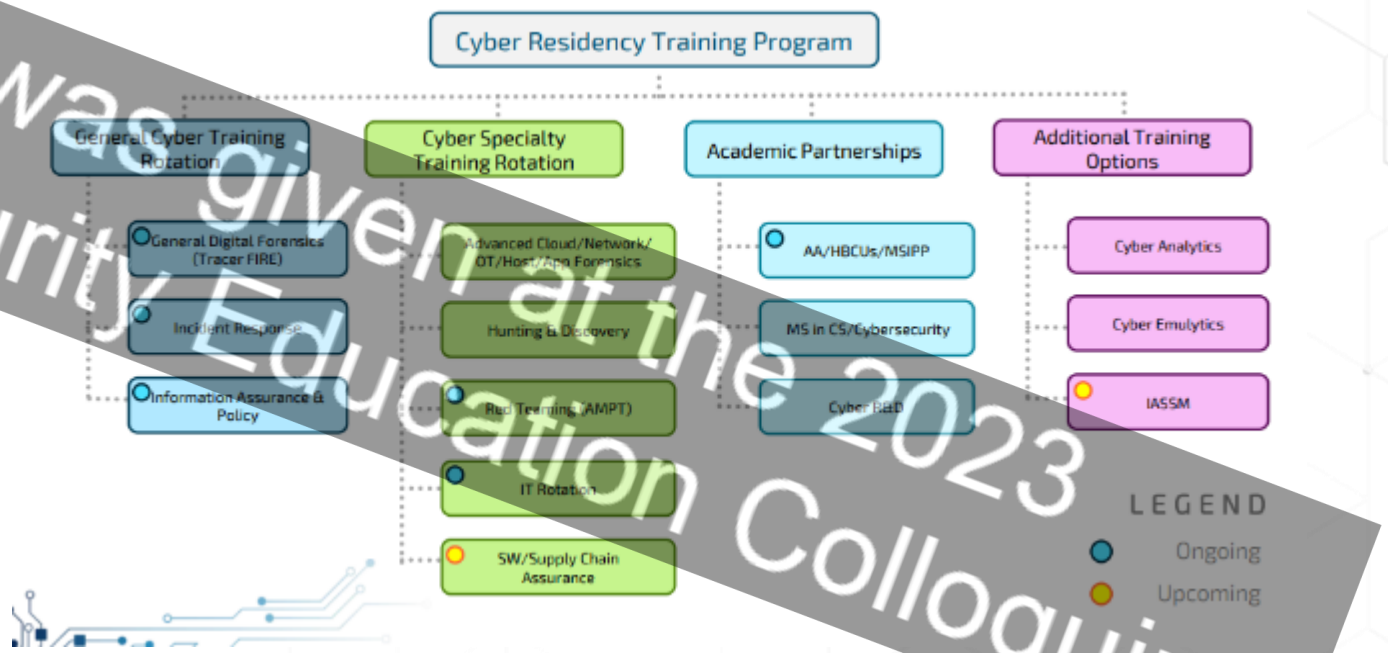
- Announced December 2021
- The founding members of CIISAp:
  - Capitol Technology University
  - ICS Village, Inc.
  - Idaho State University (ISU)
  - MISI Academy
  - Regional Economic Development for Eastern Idaho (REDI)
  - SANS Institute
  - Siemens Energy

# Medical Rotation Model



## Sandia Cyber Residency Rotational Program

Attract, retain, and develop Sandia cybersecurity practitioners and researchers with the necessary knowledge and skills for defending and securing Sandia and the nation from emerging and evolving cybersecurity threats.

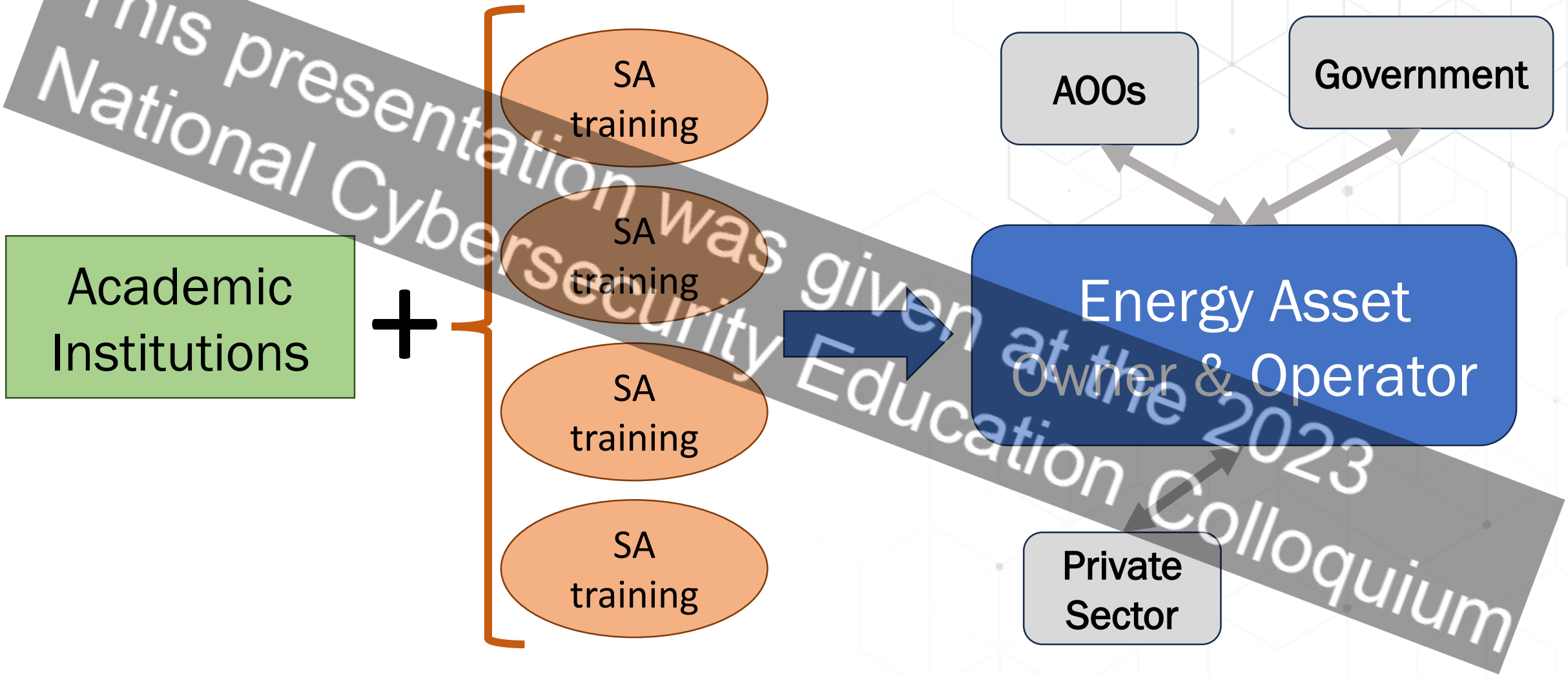


# Medical Rotation Model

New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)

- Michael Geraghty, NJ Chief Information Security Officer (CISO) and Director of NJCCIC
- A component organization within the New Jersey Office of Homeland Security and Preparedness that is a combined cyber fusion and security operations center.

# Pipeline: Role of Academic Institutions?



# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?

- Not training the right audience(s)
  - Recruitment issue
  - Potential candidates not interested
  - Human resources infrastructure

# Who is included in the cybersecurity workforce?

- Information technology cybersecurity
- ICS/OT cybersecurity
- Engineering
- Operations

# ~ 3,000 Electric Cooperative & Municipal Utilities

- Limited economic and cybersecurity resources
- Institutional challenges
- Subject matter experts unwilling to relocate

# Who is included in the cybersecurity workforce?

- Information technology cybersecurity
- ICS/OT cybersecurity
- Engineering
- Operations
- Legal
- Human Resources
- Procurement
- Finance

# Who is included in the cybersecurity workforce?

- Information technology cybersecurity
- ICS/OT cybersecurity
- Engineering
- Operations
- Legal
- Human Resources
- Procurement
- Finance
- CEO, General Manager, Senior Leadership Team
- Board of Directors, elected officials

# Who is included in the cybersecurity workforce?

- Information technology cybersecurity
- ICS/OT cybersecurity
- Engineering
- Operations
- Legal
- Human Resources
- Procurement
- Finance
- CEO, General Manager, Senior Leadership Team
- Board of Directors, elected officials

- Renewable energy
- IoT and IIoT
- Engineering
- Systems design
- Product manufacturing
- Software
- Digital hardware and firmware
- Energy markets
- Etc., etc.

# What problem(s) are we trying to solve?

- Not enough training?
- Not the right training?
  - Effective training methods? Delivery?
  - The right content? What does the market need?
- Limited access to training?
- Not training the right audience(s)
- Recruitment issue
  - Potential candidates not interested
  - Human resources infrastructure

# Challenges in hiring

- Occupational job codes for ICS/OT (no National Center for Education Statistics Classification of Instructional Program (CIP) codes, or DOL O*NET codes)
- Unclear job roles and responsibilities in ICS/OT cybersecurity
- Historical cultural expectations
  - Automated resume reviews
  - Length of employment
  - Requirements for certifications/degrees
  - Expecting unicorns

# BLUF



## Cybersecurity Workforce Strategy for CESER

Current premise:

Energy asset owners and operators need the resources and staff
with the knowledge, skills, and abilities
to successfully adapt and respond
to a constantly changing cybersecurity threat landscape.

Thursday at 10:15:  Is it time for a professional degree in cybersecurity?

# Lifelong Learning

# Lifelong Learning

## Imposture syndrome is part of the job

Lifelong Learning

Imposture syndrome is part of the job

Diversity of thought is essential

# We're Hiring!



## Upcoming Opportunities

- Cyber Security Specialists
- R&D Technology Managers
- Regional Preparedness and Response Experts
- Energy Policy Experts
- Risk Analysts
- Supervisory Program Managers
- Management and Program Analysts
- Engineers
- Budget and Finance Analysts
- Operations Support Resource Managers
- External Affairs Specialists

**Learn more and access postings at:**
energy.gov/ceser/join-our-team

**For more information reach out to CESER-HC@hq.doe.gov**

# CESER Contact Information



**Dr. Cynthia Hsu**
Cybersecurity Program Manager, Rural and Municipal Utilities
Cynthia.hsu@hq.doe.gov
202-209-3817


CESER.RMUC@hq.doe.gov

This presentation was given at the 2023 National Cybersecurity Education Colloquium

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

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