



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Cybersecurity, Energy Security,  
and Emergency Response

# NASEO Annual Meeting

Andrew Wills, Chief of Staff and Senior Advisor

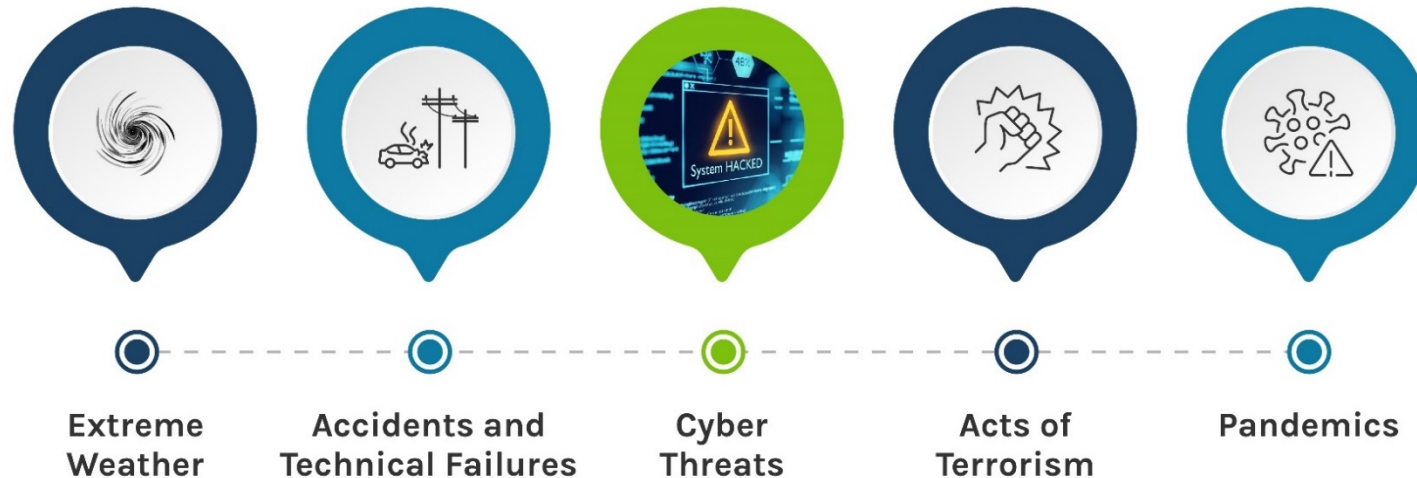
October 12, 2022



# CESER Mission & Energy Threat Landscape

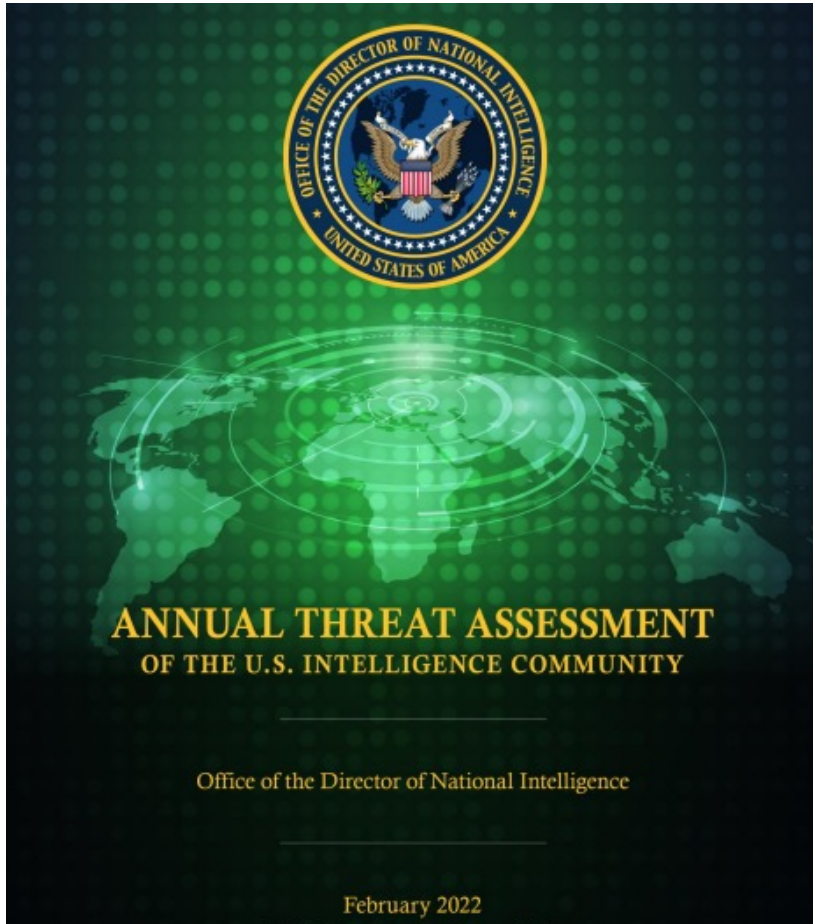
To enhance the security of U.S. critical energy infrastructure to all hazards, mitigate the impacts of disruptive events and risk to the sector overall through preparedness and innovation, and respond to and facilitate recovery from energy disruptions in collaboration with other Federal agencies, the private sector, and State, local, tribal, and territory governments.

## Evolving Threats to Critical Infrastructure





# Why Cybersecurity?



 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 5500 miles of pipeline after being hit by a ransomware attack.

1 month ago




 Wall Street Journal

## The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw

The Log4j flaw allows attackers to execute code remotely on a target computer, which could let them steal data, install malware or take control.



 Bloomberg.com

## Russian Hackers Tried Damaging Power Equipment, Ukraine

...

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



# CESER's Cybersecurity Resources

## Tools and Technology

Partners in Situational Awareness



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



Pacific Northwest  
NATIONAL LABORATORY




**CyTRICS**  
Cyber Testing for Resilient  
Industrial Control Systems




**C2M2**  
Cybersecurity  
Capability  
Maturity Model

## Capacity Building



**NARUC**  
National Association of Regulatory  
Utility Commissioners

Cybersecurity Tabletop Exercise Guide



Lynn P. Costantini  
Ashton Raffety  
September 2020



U.S. DEPARTMENT OF ENERGY'S  
**CYBERFORCE**  
PROGRAM


A CYBERSECURITY WORKFORCE DEVELOPMENT PROGRAM



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

**National Cyber-Informed  
Engineering Strategy**  
from the U.S. Department of Energy

JUNE 2022



2022 National  
Summit On State  
Cybersecurity



**NATIONAL GOVERNORS**  
ASSOCIATION

## Ongoing Efforts

### ICS Plan



### IIJA Cyber Provisions 40121, 40124, 40125, & 40126

Department of Energy

**DOE Announces \$45 Million for Next-  
Generation Cyber Tools to Protect the  
Power Grid**

AUGUST 17, 2022

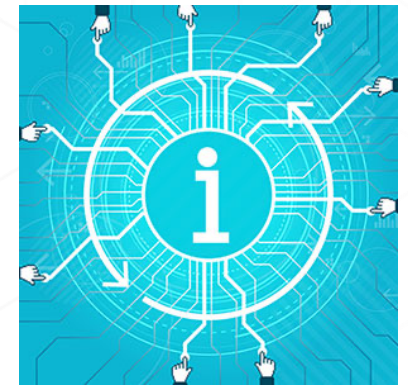
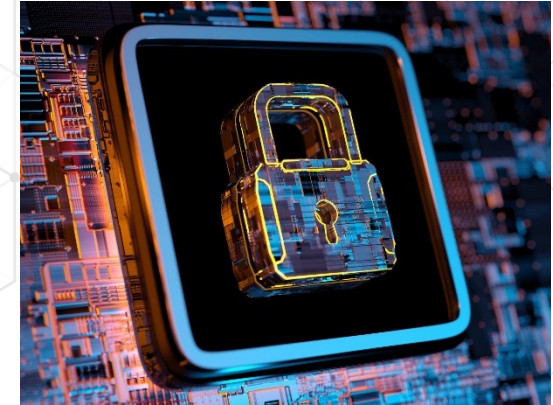


# 40124: Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program

**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.



# 40124: RMUC

**Funding:** via grants, technical assistance, cooperative agreements

**Eligibility:**

- Rural electric cooperatives
- Municipal electric utilities
- Not-for-profits in partnership with rural or municipal electric utilities
- Investor-owned electric utilities that sell < 4,000,000 MWh/year

**RMUC Listening Sessions:**

- CESER-led [listening sessions](#) with rural, municipal, and small investor-owned utilities that have limited cybersecurity resources



# State Energy Security Plan (SESP) Resources

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

## State Energy Security Plan Optional Drop-In: IT/OT and Cyber Threat Overview

May 2022

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

Argonne NATIONAL LABORATORY

## Understanding Your State's Cyber Landscape Questions To Ask Other State Officials

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

**Graphic 1. Cyber Threat Actors**

### CYBER THREAT ACTORS

A participant in an action or process that is characterized by malicious use of computers, devices, systems, or networks.

<b>CYBERCRIMINALS</b> Largely profit-driven and represent a long-term, global, and common threat.			<b>INSIDERS</b> Current or former employees, contractors, or other partners who have access to an organization's networks, systems, or data.
<b>NATION-STATE</b> Actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.			<b>HACKTIVISTS</b> Politically, socially, or ideologically motivated and target victims for publicity or to effect change, which can result in high-profile operations.
 <b>TERRORIST ORGANIZATIONS</b> Their limited offensive cyber activity is typically disruptive or harassing in nature.			

The energy sector is uniquely critical because all of the other critical infrastructure sectors depend on power and fuel to operate. Unfortunately, this makes the Nation's energy infrastructure an attractive target for cyber-attacks. Table 2 lists known cyber-attacks that have impacted energy systems. States are encouraged to add examples to this Table. All energy systems have vulnerabilities to cyber threats, 100% security is not possible. But many steps can be taken to harden OT systems to mitigate these threats.

### Questions to Ask PUCs

*Goal: Understand the cybersecurity maturity and preparation level and identify possible gaps where SEO's convening ability may be beneficial*

1. What level of cybersecurity protections or plans are in place with the utilities you regulate? Have any completed and shared a cybersecurity maturity assessment? Do all of the utilities have a cyber incident response plan? What gaps or concerns do you have?
  - Review the current status of cyber preparedness, planning and investments.
2. Are there areas you think the State Energy Office may act as a convener to host some of these cyber discussions with state and energy partners?



# Cybersecurity Reports



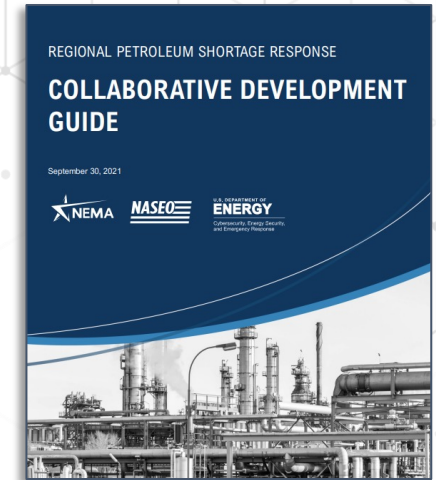
## Congressional Report In-Progress

- CESER is working with NREL on a Report to Congress authorized in IIJA Section 40121.
- The report will assess the priorities, policies, procedures and actions needed to take to enhance the cybersecurity of the electrical distribution system.
- Last week, CESER and NREL convened a stakeholder information sharing session that included input and participation from federal agencies, state regulators, and industry stakeholders.



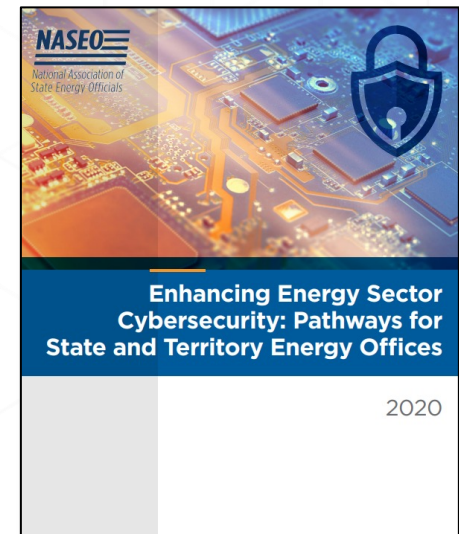
# Upcoming NASEO Activities

- **Regional Petroleum Shortage Response Collaborative**
  - Midwest and Southwest collaboratives
- **State Energy Security Planning Bootcamp**
- **Cybersecurity for Electric Vehicle Charging Infrastructure Guidance**



# Cybersecurity Call to Action

- Consider cybersecurity in all-hazard energy security planning
- Collaborate with your State: Information Security Officer, Homeland Security Advisor and Public Utility Commissioners
- Train staff to be aware of cyber threats, specifically avoiding “social engineering” cyberattacks
- Attend NARUC’s Cybersecurity Training
- Institute regular cyber threat briefings for energy stakeholders and state officials
- Build well-defined, trusted information-sharing processes and implement exchange mechanisms that meet the needs of federal, state, and private sector partners.
- Exercise information sharing protocols and channels.





# CESER Contact Information



**Andrew Wills**

Chief of Staff and Senior Advisor

[Andrew.wills@hq.doe.gov](mailto:Andrew.wills@hq.doe.gov)

202-586-4081



Website: [energy.gov/ceser](https://energy.gov/ceser)



[@DOE\\_CESER](https://twitter.com/DOE_CESER)



[CESER LinkedIn](#)



**Brandi Martin**

SLTT Program Manager

[Brandi.Martin@hq.doe.gov](mailto:Brandi.Martin@hq.doe.gov)

202-586-7983



**Megan Levy**

SLTT Project Manager

[Megan.levy@hq.doe.gov](mailto:Megan.levy@hq.doe.gov)





@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