U.S. DEPARTMENT OF
ENERGY

Cybersecurity, Energy Security, & Emergency Response

NGA Cybersecurity Roundtable on State, Federal, and Utility Energy Cybersecurity Coordination and Information Sharing

Kate Marks, State and Industry Engagement

Office of Cybersecurity, Energy Security and Emergency Response (CESER)

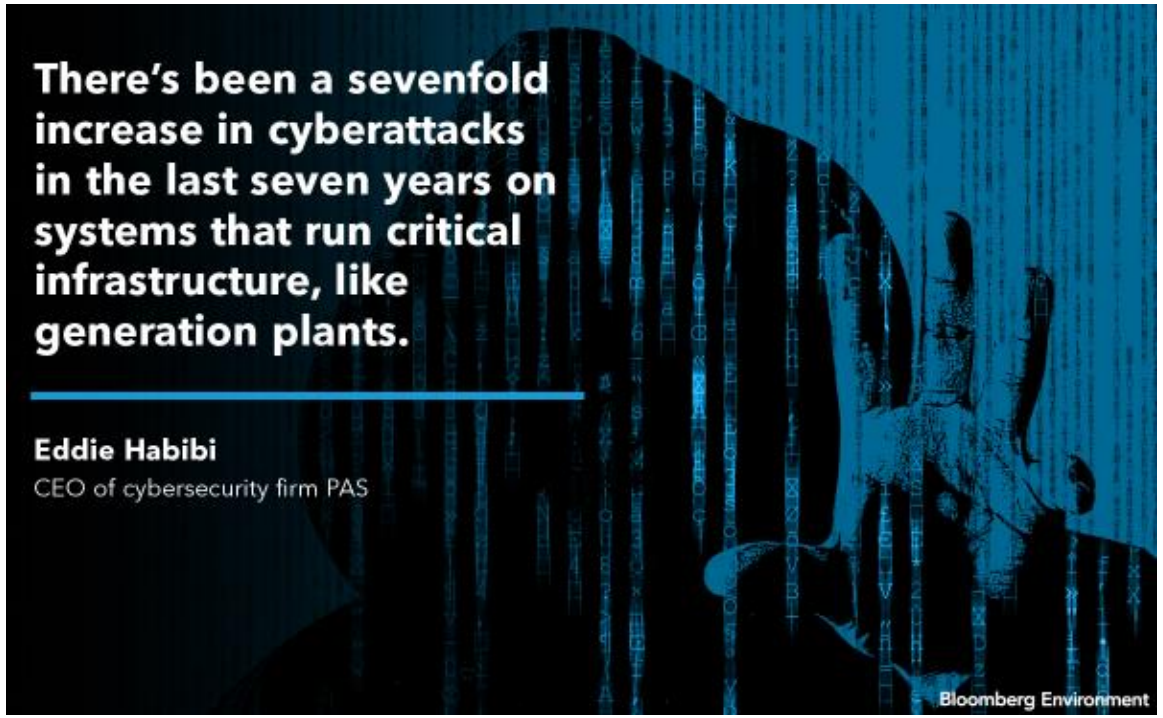
U.S. Department of Energy

August 15, 2019

Presentation Overview

1. Significance of Cybersecurity in the Energy Sector
2. Review of the DOE CESER Office Programs and Projects
3. Vital Cooperation Between DOE and the States

Cybersecurity and the Energy Sector



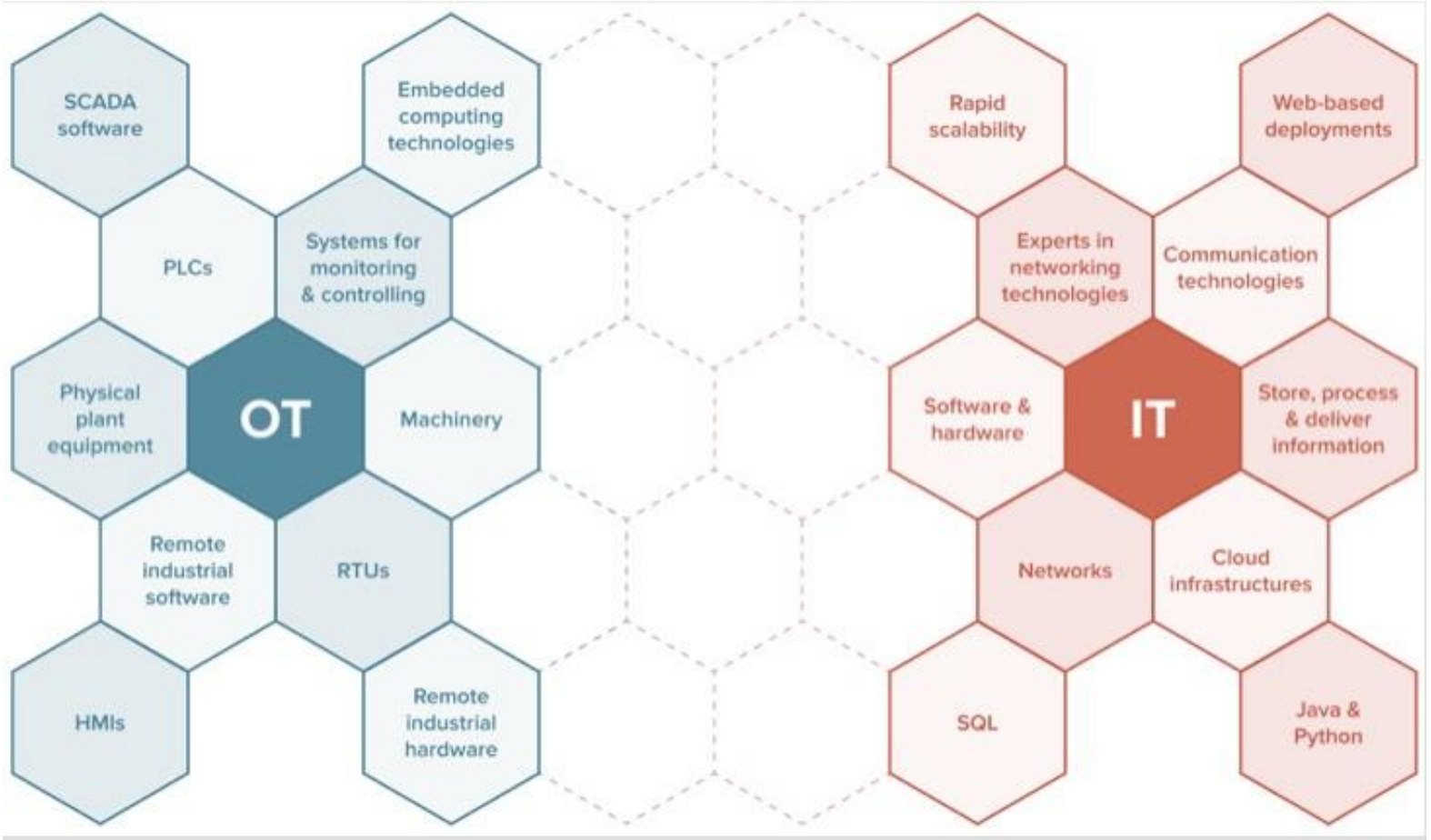
Duke Energy, one of the largest power companies in the nation serving 7.6 million customers reported more than 650 million attempted cyberattacks in 2017

"In an average day, WAPA's firewalls are pinged nearly 200,000 times by suspicious or potentially damaging events," Mark Gabriel, administrator and CEO of Western Area Power Administration (WAPA)

Cyber Landscape in Energy Sector

Operational Technology Network

Information Technology Network

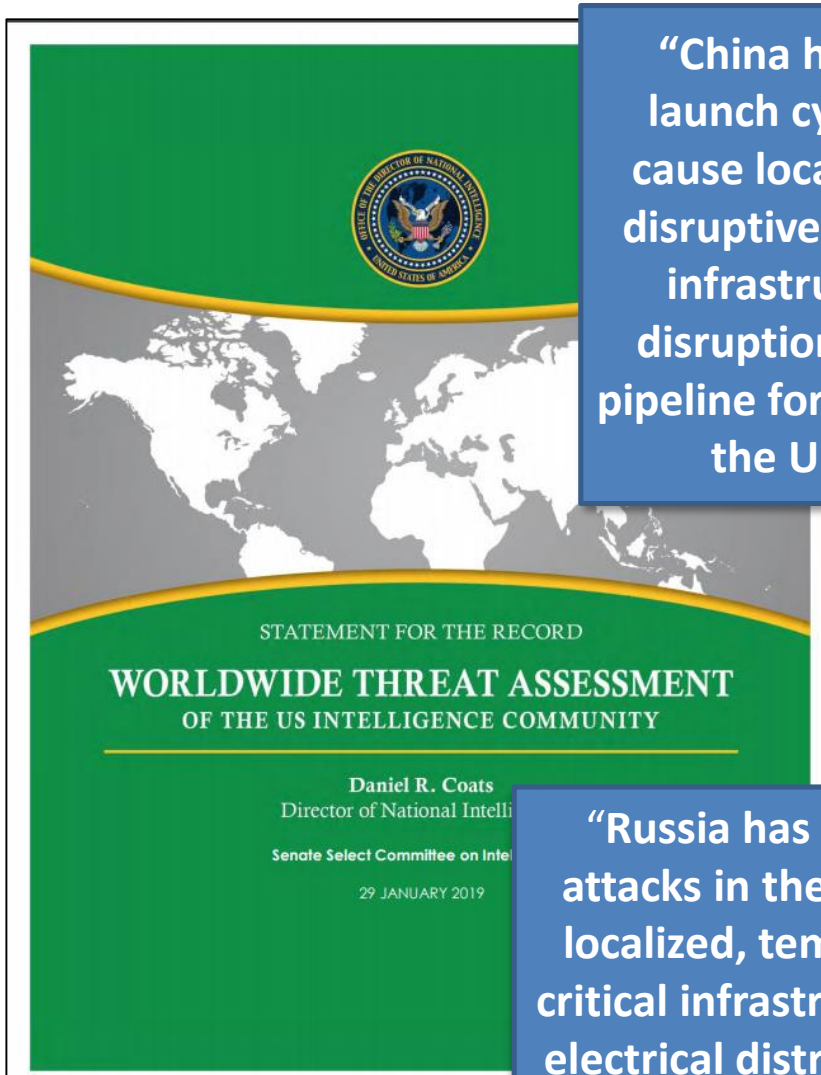


Source: IEB Media Industrial Ethernet Book

CESER's Mission

Cybersecurity, Energy Security, and Emergency Response (CESER) leads the Department's efforts to secure U.S. energy infrastructure against all threats and hazards, reduce the risks of and impacts from disruptive events, and facilitates restoration activities.

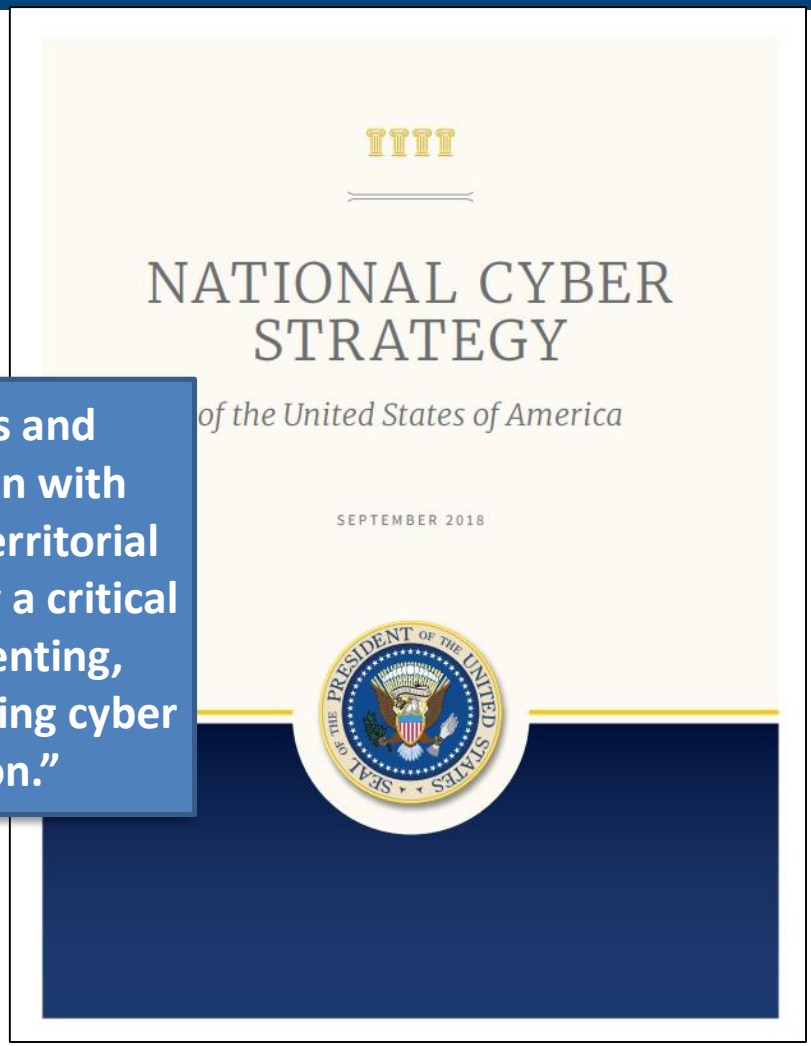
Cyber Threats and National Cyber Strategy



"China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."

"Federal departments and agencies, in cooperation with state, local, tribal, and territorial government entities, play a critical role in detecting, preventing, disrupting, and investigating cyber threats to our Nation."

"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—similar to those demonstrated in Ukraine in 2015 and 2016."



Recent Executive Orders Focused on Cyber

America's Cybersecurity Workforce (May 2019)

America's cybersecurity workforce is a strategic asset

The US Government must:

- Enhance the workforce mobility to improve America's national cybersecurity
- Support the development of cybersecurity skills so that America can maintain its competitive edge
- Create organization and technological tools to maximize the cybersecurity talents of American workers

Securing the Information and Communications Technology and Services Supply Chain (May 2019)

- Foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology (ICTs) and services
- Unrestricted acquisition or use of ICTs allows foreign adversaries to exploit vulnerabilities

<u>Executive Order PROHIBITS transactions that:</u>

- Involve info and communications technology services designed or developed by foreign adversaries
- Pose an undue risk of sabotage or subversion of design, production and distribution of technology
- Pose an undue risk of catastrophic effects on the security or resiliency of US critical infrastructure or the digital economy
- Pose an unacceptable risk to US national security and safety of citizens

DOE's Sector Specific Agency (SSA) Authorities

FAST Act (2015)

Codified DOE's SSA Role

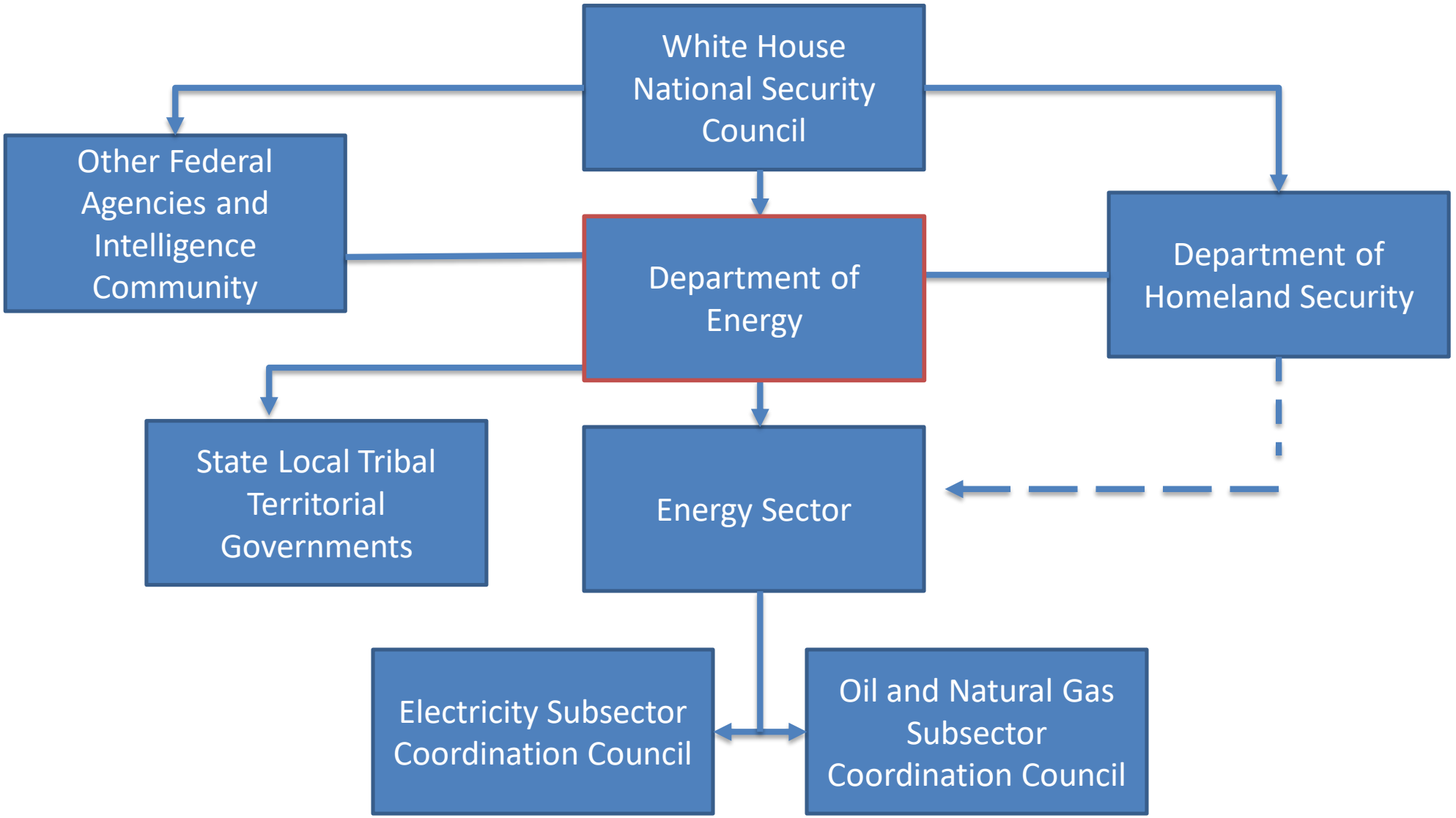
Presidential Policy Directives (PPD)

- **PPD-21 –** Establishes a shared responsibility among the Federal government, **State**, local, tribes and territorial governments, and public and private owners and operators for critical infrastructure security and resilience.
- **PPD-41 –** Federal Government's response to any cyber incident involving government or private sector entities.

U.S. Department of Energy (DOE) Office of CESER

State, Local, Tribal, and Territorial Governments (SLTT)	Oil and Natural Gas Subsector Coordinating Council (ONG SCC)	Electricity Subsector Coordinating Council (ESCC)	Energy Government Coordinating Council (EGCC)	Emergency Support Function (ESF) #12 – Energy

Energy Sector Government Organizational Structure



CESER Collaboration Across the Energy Sector

State, Local, Tribal and Territorial (SLTT) Program

NASEO
National Association of State Energy Officials

AMERICAN PUBLIC POWER ASSOCIATION

NCSL

NGA
NATIONAL GOVERNORS ASSOCIATION

NEMA™

ESCC
Electricity Subsector Coordinating Council

Who	• Electricity trade associations and their members
Purpose	• Coordinate efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure.
Working Groups	• Vision and Planning • Threat Information Sharing • Industry-Government Coordination • Research & Development • Cross-Sector Liaisons

OIL AND NATURAL GAS SECTOR COORDINATING COUNCIL

Who	• Oil & natural gas trade associations and their members
Purpose	• Provide a forum to coordinate security strategies, activities, policy and communications across the sector to support the nation's security mission
Working Groups	• Cyber • Information Sharing • Regulatory Engagement • Emergency Management • Law Enforcement Engagement • Pipeline

State Energy Security Preparedness and Response

- Energy Emergency Assurance Coordinators (EEAC) Outreach
- Incident Calls
- Situational Awareness (EAGLE-I)
- DOE Situation Reports

- Cyber Manual Toolkit (NARUC)
- Guidance on Petroleum Shortage Response Planning (NASEO)
- *Hardening the Grid* Report (NCSL)
- Cybersecurity Cost-Recovery (LBNL)

State Energy Security Planning and Strategies
Energy Security Accelerator (NASEO)
Energy Security Online Training

- Regional Cybersecurity Training
- Viking Shadow Workshop 2018
- Petroleum Shortage Workshop 2019
- USVI Preparedness Workshop

DOE Workforce Initiatives

U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE™ COMPETITION
DEFENDING U.S. ENERGY INFRASTRUCTURE

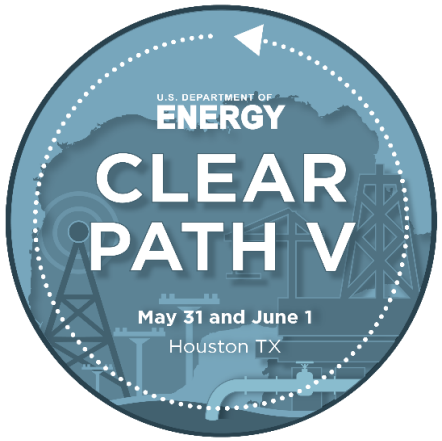
- DOE's annual collegiate cyber defense competition
- Student teams defend simulated cyber-physical infrastructure against professional red-team attackers
- Hosted in collaboration with DOE's National Laboratories



CYBER STRIKE
Sponsored by the U.S. Department of Energy

- Hands on training for energy sector owners and operators
- Focused on preparing for and responding to a cyber incident impacting ICS (Ukraine example)
- Hosted with industry; workshops held periodically and by request


Exercises and Trainings



GridEx V

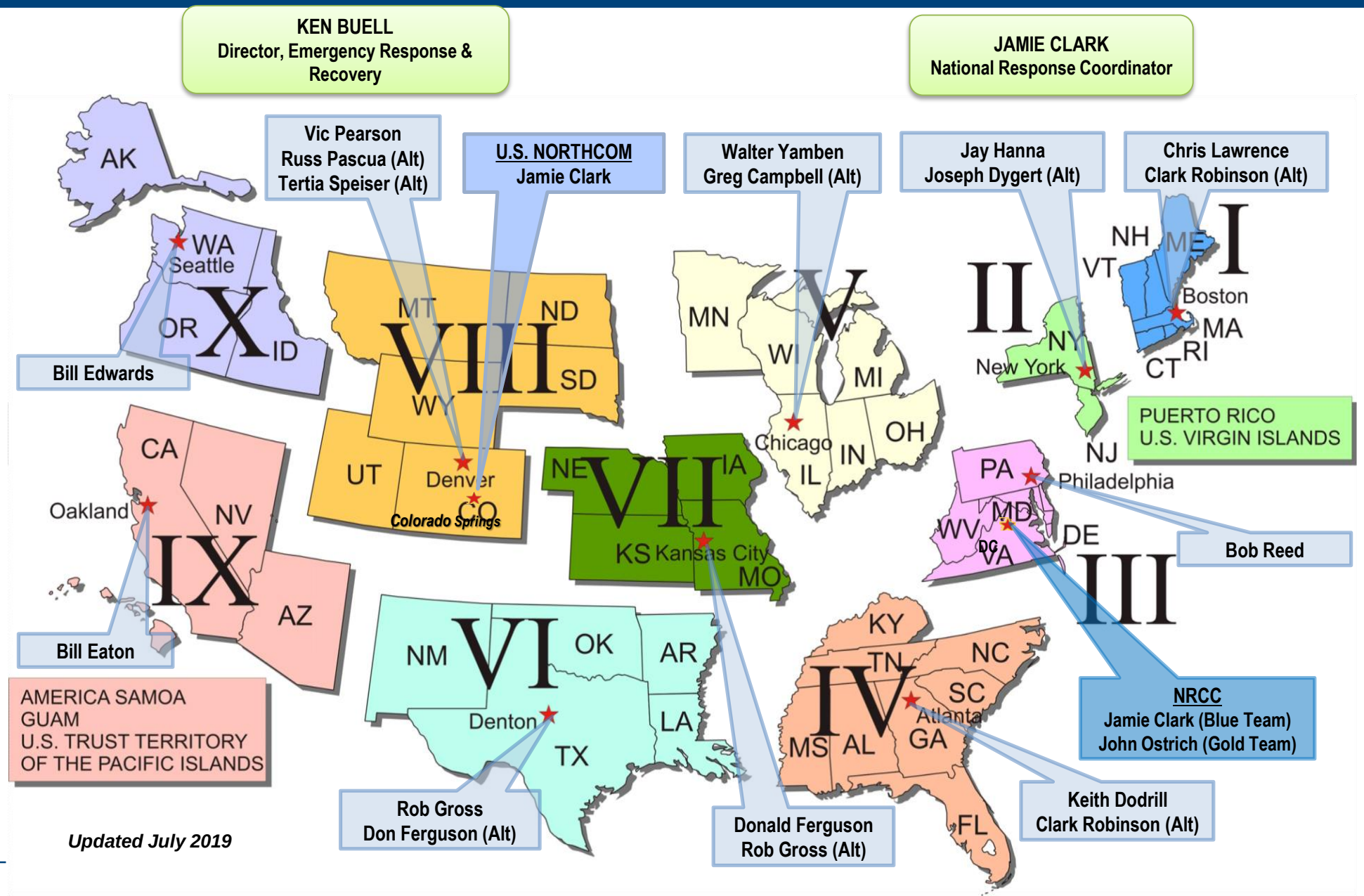
GRID SECURITY EXERCISE 2019

Energy Sector All-Hazards Response

Activities

- Situational Awareness
- Damage Assessments
- Restoration Priorities
- Regulatory Relief Assistance
- Unity of Message
- Mutual Aid Support
- Interdependency Analysis
- Cascading Impact Analysis

DOE Regional Coordinators



Updated July 2019

Cybersecurity for Energy Delivery Systems

Cybersecurity Research, Development, and Demonstration

P PREVENT CYBER INCIDENTS by decreasing the attack surface or blocking unauthorized access or use of EDS components.

M MITIGATE CYBER INCIDENTS by distinguishing malicious activity from other operational issues or anomalies, and automatically respond by isolating or eliminating the threats.

D DETECT CYBER INCIDENTS by rapidly identifying anomalous or suspicious behaviors and functions that could potentially damage equipment or destabilize the grid.

S RE-DESIGN ENERGY DELIVERY SYSTEMS TO SURVIVE CYBER INCIDENTS by restricting systems from performing functions that cause grid instability and allowing systems to continue operating in the face of an attack.

CESER R&D Delivers

NETWORK ARCHITECTURES

Tools and technologies that design or reconfigure the way devices interconnect or communicate to enhance cybersecurity capabilities. This includes software-defined networking, wireless configurations, and altering the way information flows between EDS components.

ACCESS CONTROL

Tools and technologies that use encryption, authentication, or authorization to make information and devices indecipherable or inaccessible to unauthorized users.

ATTACK IDENTIFICATION AND RESPONSE

Tools and technologies that identify and respond to cyber attacks or intrusions to mitigate potential damage. This includes detecting and mitigating the effects of malicious software, anomalous behavior, abnormal communication, and physical tampering

SITUATIONAL AWARENESS AND OPERATOR SUPPORT

Tools and technologies that assist human operators by providing real-time information on the status of their operational networks to inform decision-making.

GUIDANCE AND PRACTICES

Guides, best practices, or reports that inform owners, operators, regulators, and/or end users of policies or practices that can improve cybersecurity. This includes identifying requirements, challenges, misconceptions, and recommendations for future action.

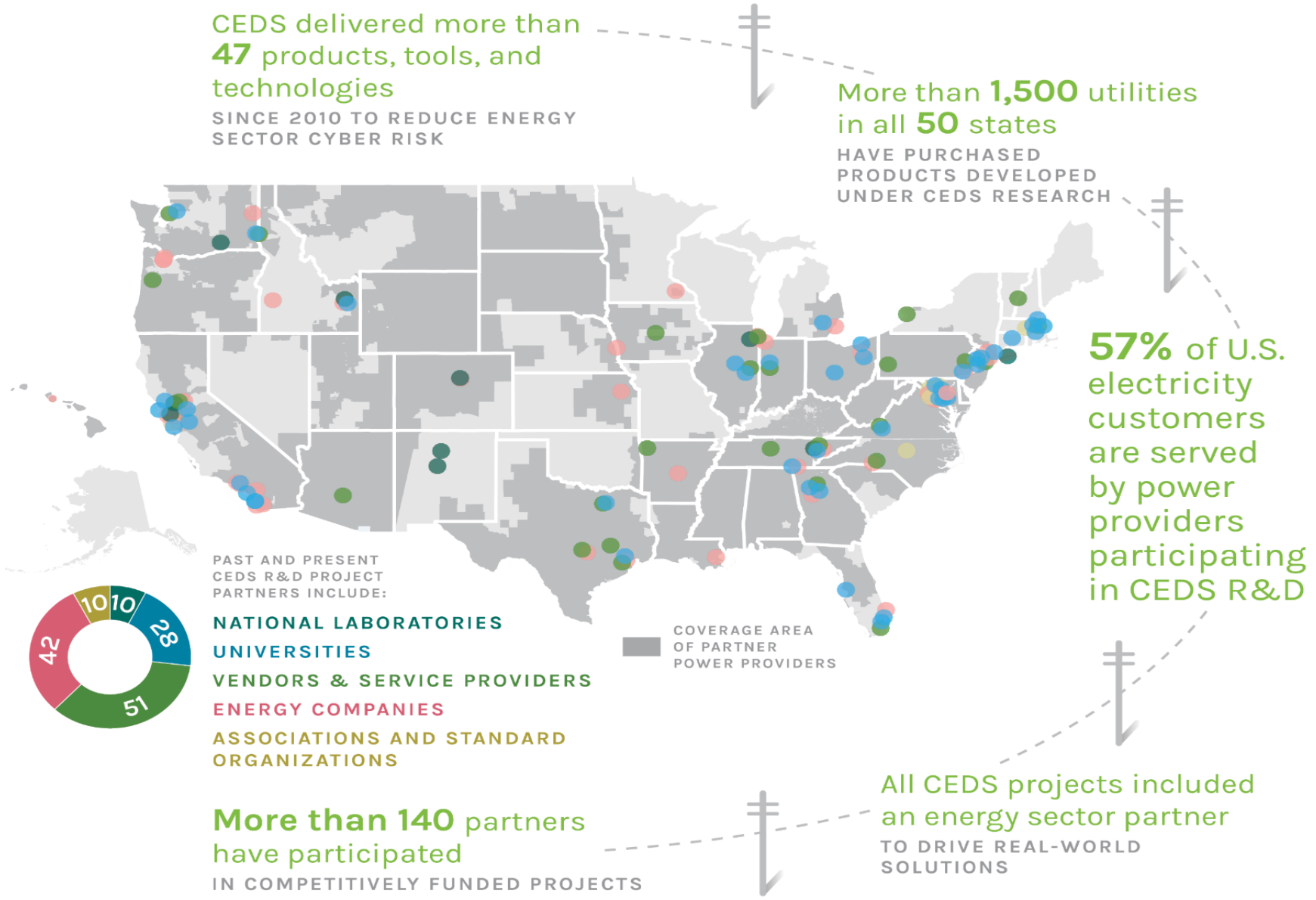
REDUCED EXPOSURE

Tools and technologies that preemptively identify and assess system risks and potential attack vectors to enhance cybersecurity.

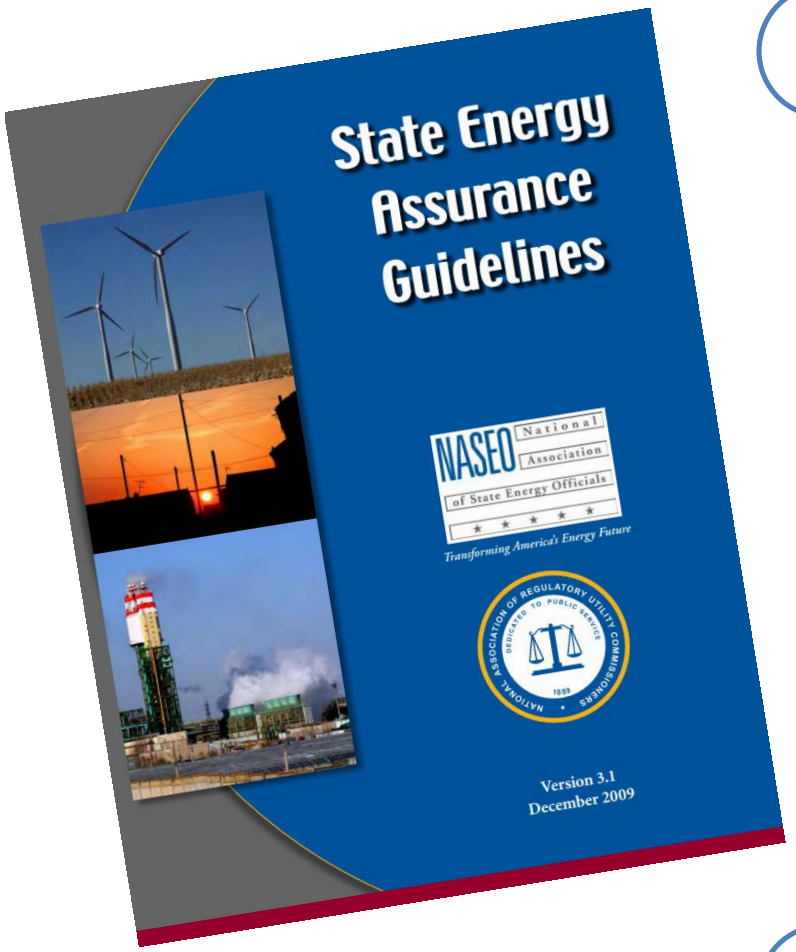
CESER R&D Reach and Impact

- **Funds earlier, high-risk/high-reward R&D** in areas critical for national security where a business case cannot readily be established by a private-sector company

- **Builds R&D pipeline through partnerships** with energy sector utilities, vendors and service providers, universities, and national laboratories



State Energy Assurance Plans



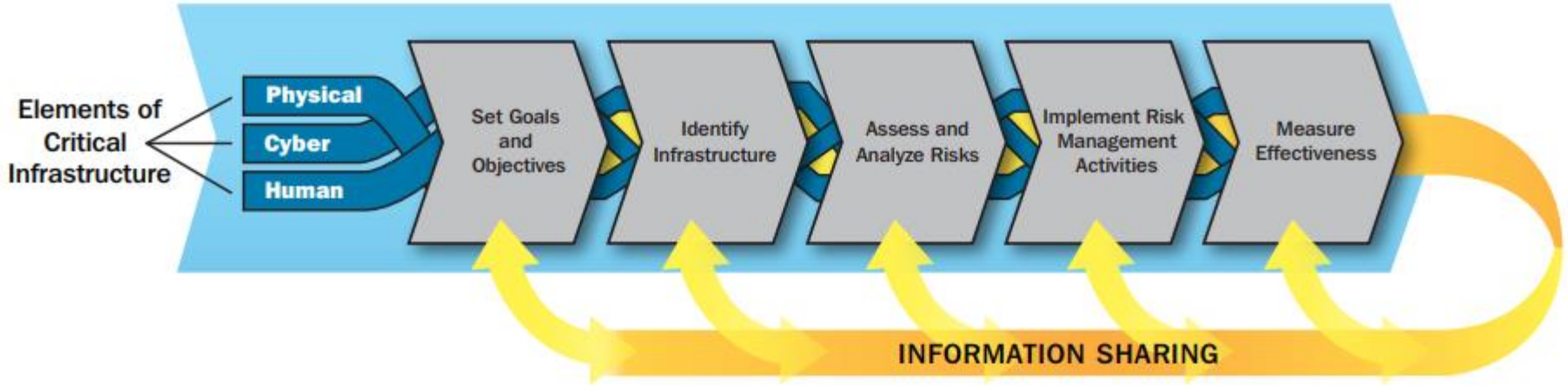
- Energy profile
- Historical events and actions taken
- Roles of energy assurance / response agencies
- Interrelationship of large energy producers, consumers, associations to state/local
- Methods of assessing severity and consequences of energy disruptions and tracking rate of recovery
- Emergency communications protocols
- Management decision processes

EAP Resources:
https://www.naseo.org/energyassurance

Cybersecurity Guidance for States

- **Consider cybersecurity in all-hazard energy security planning**

Critical Infrastructure Risk Management Framework



Source: DHS NIPP CI Risk Management Framework

Cybersecurity Guidance for States

- **Clarify state agency roles and responsibilities for cybersecurity**
  - Incorporate Cybersecurity roles and responsibilities into Energy Assurance Plans
- **Collaborate with your:**
  - State Information Security Officer
  - State Homeland Security Advisor
  - Public Utility Commissioners
- **Participate in cyber response exercises**
  - Indiana started Critical Exercise series to test SCADA penetration for utilities
- **Leverage the National Guard - Cyber Units**
  - Michigan, Delaware, Massachusetts, Maryland, Missouri, Rhode Island and Utah

CESER State Engagement Contacts

Kate Marks
Sector Engagement Lead
Kate.Marks@hq.doe.gov
202-586-9842

Brandi Martin
Sector Engagement
Brandi.Martin@hq.doe.gov
202-586-7983

Cyber Response

Department of Energy (DOE) Consolidated Emergency Operations Center	(202) 586-8100	doehqeoc@oem.doe.gov
FBI National Cyber Investigative Joint Task Force (NCIJTF) CyWatch	(855) 292-3937	cywatch@fbi.gov
DHS National Cybersecurity and Communications Integration Center (NCCIC)	(888) 282-0870	NCCICCustomerService@us-cert.gov