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

NASEO Annual Meeting

Regional Collaboration, Cybersecurity, and Risk Assessments: Connecting the Dots
NASEO Energy Security Committee

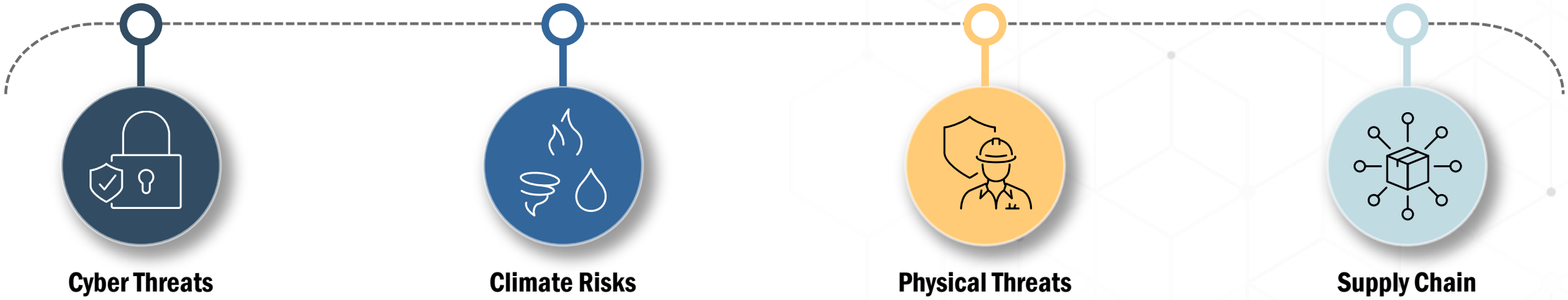
Megan Levy, Project Manager, State, Local, Tribal, and Territorial Program

October 18, 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 Priorities

- Improving security and resilience through **advanced risk analysis**
- Using the energy transition to build cybersecurity and resilience into the energy sector **supply chain**
- Buying down risks through threat-informed **research, development, and demonstration**
- Providing **cybersecurity expertise to all DOE program offices** to ensure energy systems are secure-by-design
- **Building capacity** across industry and state, local, tribal, and territorial (SLTT) partners to ensure they are prepared for the multi-threat environment
- **Strengthening response and restoration capabilities** in light of increased climate, cyber, and physical threats facing the energy sector

Collaboration and Coordination is Essential

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

NASEO National Association of State Energy Officials

National Association of Regulatory Utility Commissioners

American Public Power Association

NCSL

NEMA™

National Governors Association

Energy Government Coordinating Council (EGCC)

Executive Office of the President of the United States

Department of Defense

U.S. Department of Homeland Security

Transportation Security Administration

Department of Energy

Department of Transportation

United States Coast Guard

Office of the Director of National Intelligence

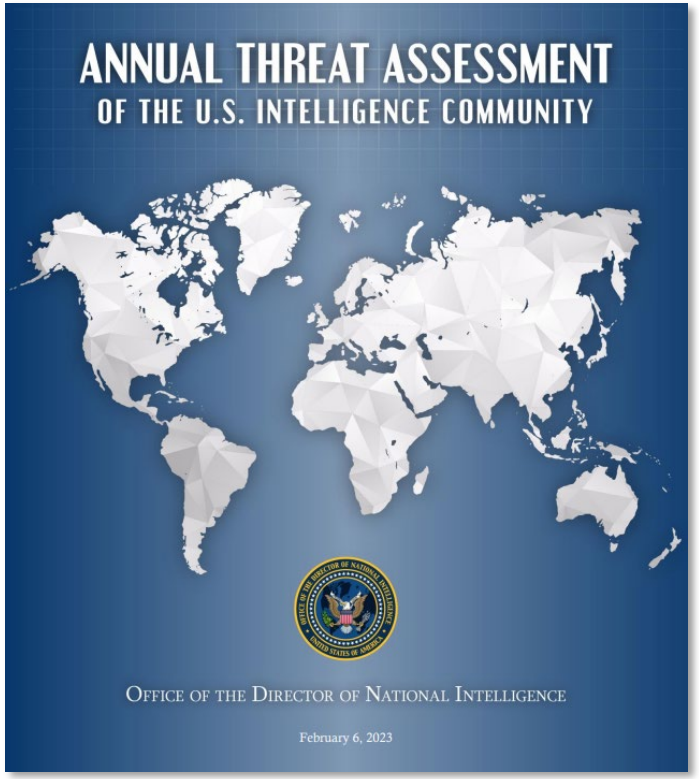
NASEO NARUC NGA

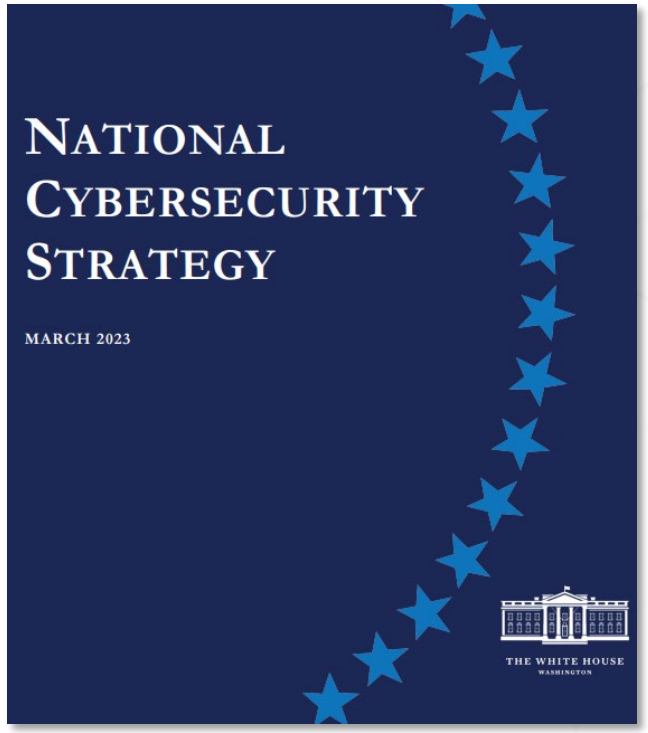
Industry Councils

ESCC Electricity Subsector Coordinating Council

Oil and Natural Gas Subsector Coordinating Council

Cybersecurity Threats





Physical Security Threats

- Rogue actors and domestic violent extremists are targeting critical energy infrastructure
- Of the physical security incidents shared with E-ISAC between 2020-2022, 3% resulted in outages or other grid impacts.
- 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

State Energy Security Plans (SESP) 40108

Purpose

State energy security plans—

1) assess the existing circumstances in the State
2) propose methods to strengthen the ability of the State, in consultation with owners and operators of energy infrastructure in the State to:
   - **secure** the energy infrastructure of the State against all **physical and cybersecurity threats**;
   - **mitigate the risk** of energy supply disruptions to the State; and to **enhance the response** to, and **recovery** from, energy disruptions; and
   - ensure that the State has **reliable, secure,** and **resilient energy infrastructure.**

*Section 40109 provides $500 million in financial assistance for states, contingent upon SESPs meeting Congressional requirements.

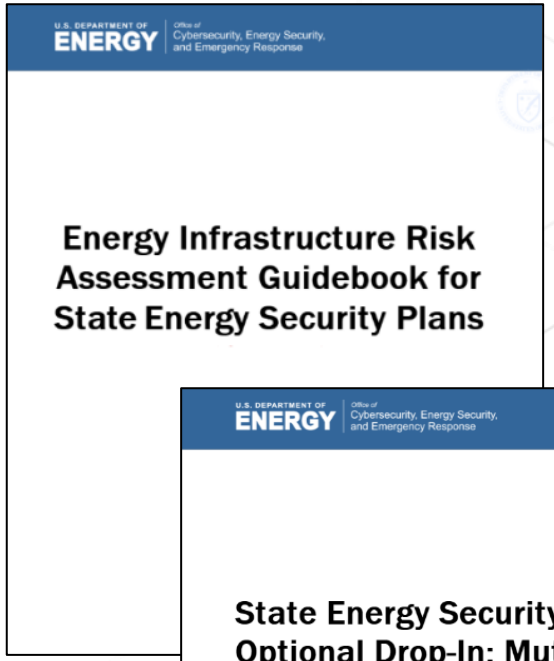
Contents

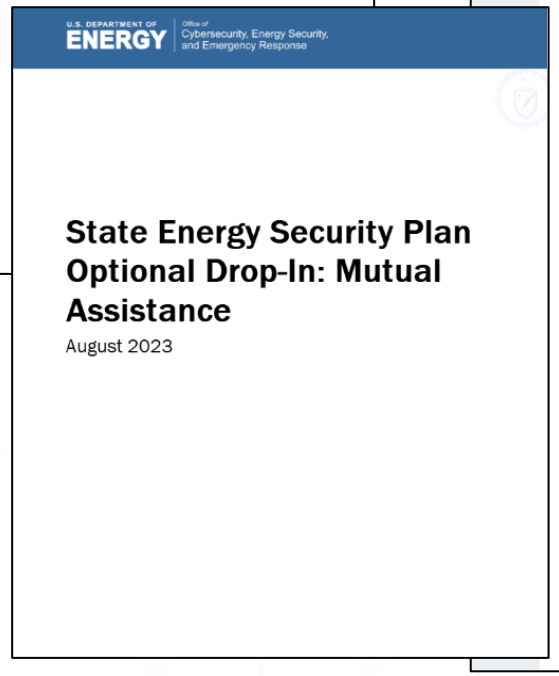
A State energy security plan **shall**—

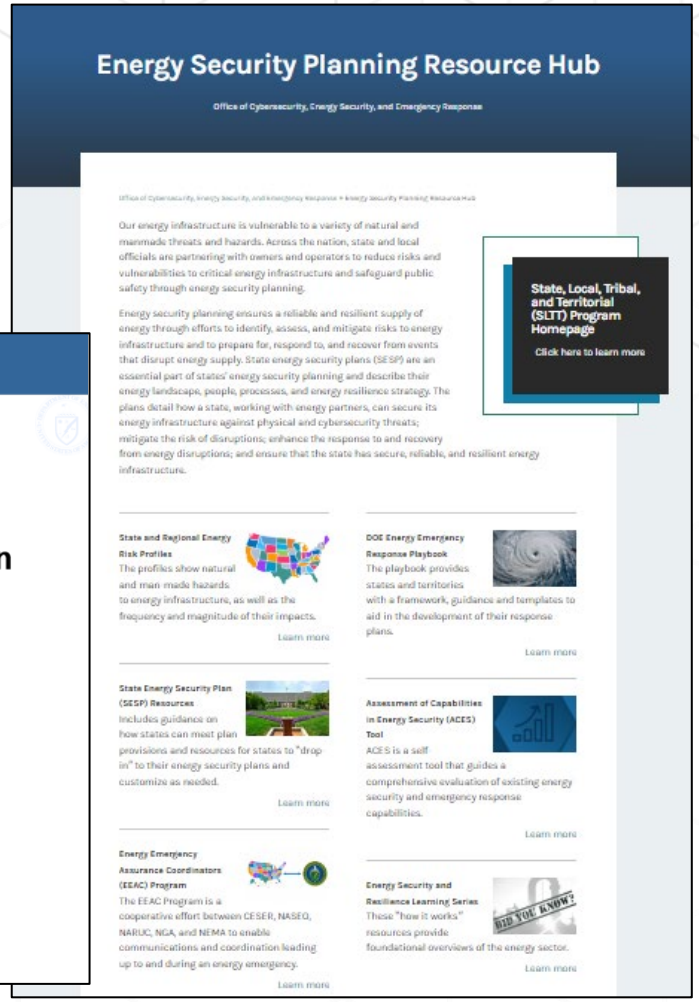
1) address all energy sources and regulated and unregulated energy providers;
2) provide a State energy profile, including an assessment of energy production, transmission, distribution, and end-use;
3) address potential hazards to each energy sector or system, including physical threats and vulnerabilities; and cybersecurity threats and vulnerabilities;
4) provide a risk assessment of energy infrastructure and cross-sector interdependencies;
5) provide a risk mitigation approach to enhance reliability and end-use resilience; and
6) Address
   A. multi-State & regional coordination, planning, and response; and
   B. coordination w/ Indian Tribes w/ respect to planning and response; and
   C. to the extent practicable, encourage mutual assistance in cyber and physical response plans.

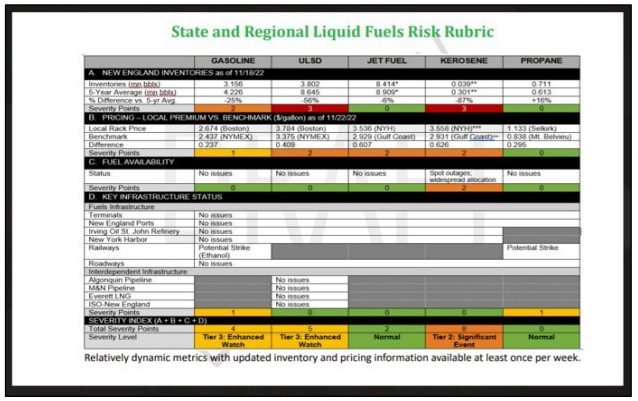
SESP TA . . . Coming Soon

- Mutual Assistance Drop-In
- Risk Assessment Guidebook
- Risk Mitigation Guidebook
- Threat/Hazard Resource
- Launching Cohorts









State and Regional Liquid Fuels Risk Rubric

	GASOLINE	ULSD	JET FUEL	KEROSENE	PROPANE
A. NEW ENGLAND INVENTORIES as of 11/18/22					
Inventories (mp bbls)	3.156	3.802	8.414*	0.039**	0.711
5-Year Average (mp bbls)	4.226	8.645	8.909*	0.301**	0.613
% Difference vs. 5-yr Avg	-25%	-56%	-6%	-87%	+16%
Severity Points	2	3	0	3	0
B. PRICING – LOCAL PREMIUM VS. BENCHMARK ($/gallon) as of 11/22/22					
Local Rack Price	2.674 (Boston)	3.784 (Boston)	3.536 (NYH)	3.558 (NYH)***	1.133 (Selkirk)
Benchmark	2.437 (NYMEX)	3.375 (NYMEX)	2.929 (Gulf Coast)	2.931 (Gulf Coast)**	0.838 (Mt. Belvieu)
Difference	0.237	0.409	0.607	0.626	0.295
Severity Points	1	2	2	2	0
C. FUEL AVAILABILITY					
Status	No issues	No issues	No issues	Spot outages, widespread allocation	No issues
Severity Points	0	0	0	2	0
D. KEY INFRASTRUCTURE STATUS					
Fuels Infrastructure					
Terminals	No issues				
New England Ports	No issues				
Irving Oil St. John Refinery	No issues				
New York Harbor	No issues				
Railways	Potential Strike (Ethanol)				Potential Strike
Roadways	No issues				
Interdependent Infrastructure					
Algonquin Pipeline		No issues			
M&N Pipeline		No issues			
Everett LNG		No issues			
ISO-New England		No issues			
Severity Points	1	0	0	0	1
SEVERITY INDEX (A + B + C + D)					
Total Severity Points	4	5	2	8	0
Severity Level	Tier 3: Enhanced Watch	Tier 3: Enhanced Watch	Normal	Tier 2: Significant Event	Normal

Relatively dynamic metrics with updated inventory and pricing information available at least once per week.

Key Definitions

RISK

The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

THREAT

Anything that can expose a vulnerability and damage, destroy, or disrupt energy systems, including natural, technological, manmade/physical, and cybersecurity hazards.

VULNERABILITY

Weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Vulnerabilities may be specific to the threat, energy type, and infrastructure component.

CONSEQUENCE

Effect of an event, incident, or occurrence, including immediate "direct" impacts and cascading "indirect" impacts

Risk Assessment Formula

=

X

X

RISK

- Risk scores are specific to combinations of specific assets and specific threats

THREAT

- Probability of occurrence on an annual basis, typically on a scale of 0 to 100%
- Specific to location
- Informed by climate data (NOAA, USGS, etc.) and Hazard Mitigation Plan

VULNERABILITY

- May be interpreted as the expected outage duration from exposure to a given threat
- Specific to asset type and region
- Should include inter-dependency considerations
- Informed by subject matter experts and discussions with operators

CONSEQUENCE

- Specific to asset and market
- Direct consequence = lost energy supply
- Indirect consequence = cost to society of lost supply
- Informed by analysis of asset and market data

Risk Assessment Guidebook

Exhibit 28. Example of Semi-Quantitative Risk Matrix

Annual Threat Probability						
	5 (Very Common)	*Medium Risk* L, S, T, U	*High Risk*	*Very High Risk* F		*Extreme Risk*
	4 (Common)	K, X	I, J	A, B	C, D	
	3 (Occasional)		H	G, R	Q	
	2 (Rare)	V, W			P	E, O
	1 (Very Rare)	*Low Risk*				M, N
		1 (Low)	2 (Med-Low)	3 (Medium)	4 (Med-High)	5 (High)
		Impact (Vulnerability x Consequence)				

Exhibit 32: Risk Categorization Matrix

	Threat	Vulnerability	Consequence
Low	Very rare. Less than 1% annual probability of occurrence.	Minor damage. Asset is down or degraded with repairs and restoration taking a few minutes or hours.	If this asset was offline less than 1% of the state would experience a loss of service.
Medium Low	Rare. 1-5% annual probability of occurrence.	Some damage. Asset is down or degraded with repairs and restoration taking less than a day.	If this asset was offline around 2-5% of the state would experience a loss of service
Medium	Occasional. 6-15% annual probability of occurrence.	Moderate damage. Asset is down or degraded with repairs and restoration taking 1-3 days.	If this asset was offline around 6-20% of the state would experience a loss of service
Medium High	Common. 16-30% annual probability of occurrence.	Severe damage. Asset is down or degraded with repairs and restoration taking to 4-7 days.	If this asset was offline around 21-50% of the state would experience a loss of service.
High	Very Common. Greater than 30% annual probability of occurrence.	Very severe damage. Asset is down or degraded with repairs and restoration taking to greater than 7 days.	If this asset was offline greater than 50% of the state would experience a loss of service.

Exhibit 34: Risk Analysis and Rating

Threat						
	High					*Meduim Low Risk*
	Medium High					
	Medium					
	Medium Low					
	Low	*Low Risk*				
Consequence: Low		Low	Medium Low	Medium	Medium High	High
		Vulnerability				

Threat						
	High					*Medium High Risk*
	Medium High					
	Medium			*Medium Risk*		
	Medium Low					
	Low	*Medium Low Risk*				
Consequence: Medium		Low	Medium Low	Medium	Medium High	High
		Vulnerability				

Threat						
	High					*High Risk*
	Medium High					
	Medium					
	Medium Low					
	Low	*Meduim High Risk*				
Consequence:High		Low	Medium Low	Medium	Medium High	High
		Vulnerability				

2023 Capacity-Building Activities

- **Launched Midwest & Southeast Regional Petroleum Collaboratives (NASEO - NEMA)**
  - Advance regional planning, coordination, and recovery activities for petroleum shortage response and help build relationships and processes to facilitate response and restoration efforts.
- **Hosted Energy Security Planning Bootcamp (NASEO)**
  - This event enhanced State officials' ability to better prepare for and respond to energy disruptions and emergencies, and to facilitate intrastate and interstate coordination and planning for energy security.

CESER SLTT Contact Information

Brandi Martin
Asst. Director, Energy Security Policy & Partnerships
Brandi.Martin@hq.doe.gov

Megan Levy
SLTT Project Manager
Megan.levy@hq.doe.gov

Juan Gomez
Energy Sector Specialist
Juan.gomez@hq.doe.gov

Joel Nelson
Energy Industry Specialist
Joel.nelson@hq.doe.gov

Website: energy.gov/ceser

@DOE_CESER

CESER LinkedIn

@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