NASEO Energy Security Committee Cyber and Physical Security Strategy Session: Protecting Against Manmade Threats

Prepared by: Matt Kelly

02/08/2023

8,000+
Employees
75 global / 45 U.S. locations
Reston, VA HQ

2,000+
Energy and grants management Professionals

50+
years of energy work

State energy security plan support for **7 states**

Climate and clean energy plans in **10 states**

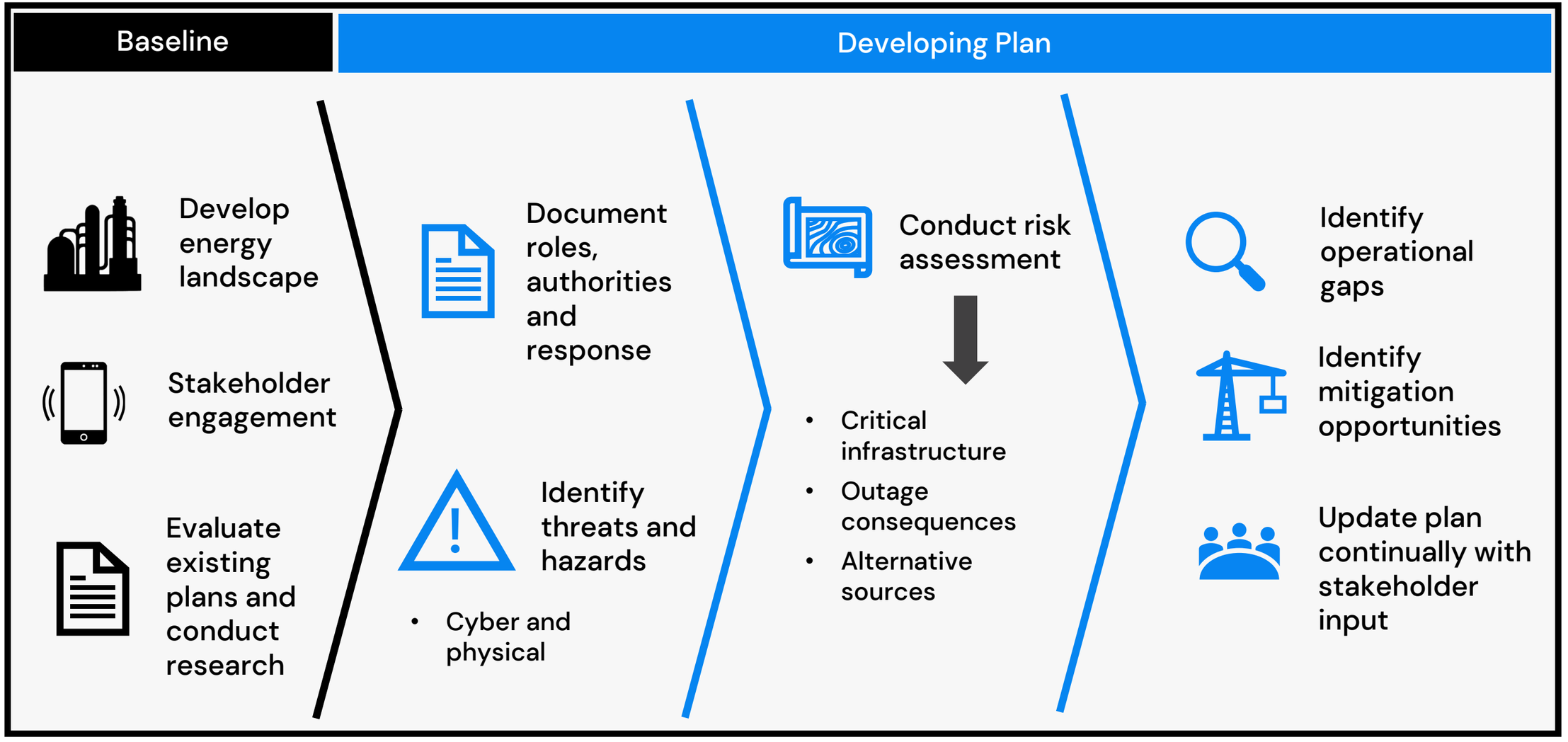
Services include:

- Energy assurance planning
- Stakeholder engagement/ outreach
- Climate action and clean energy planning
- GHG inventories and energy assessments
- Economic, health, and equity analysis
- Energy and GHG modeling
- Climate risk assessments

AMERICA'S BEST MANAGEMENT CONSULTING FIRMS | Forbes 2022 POWERED BY STATISTA

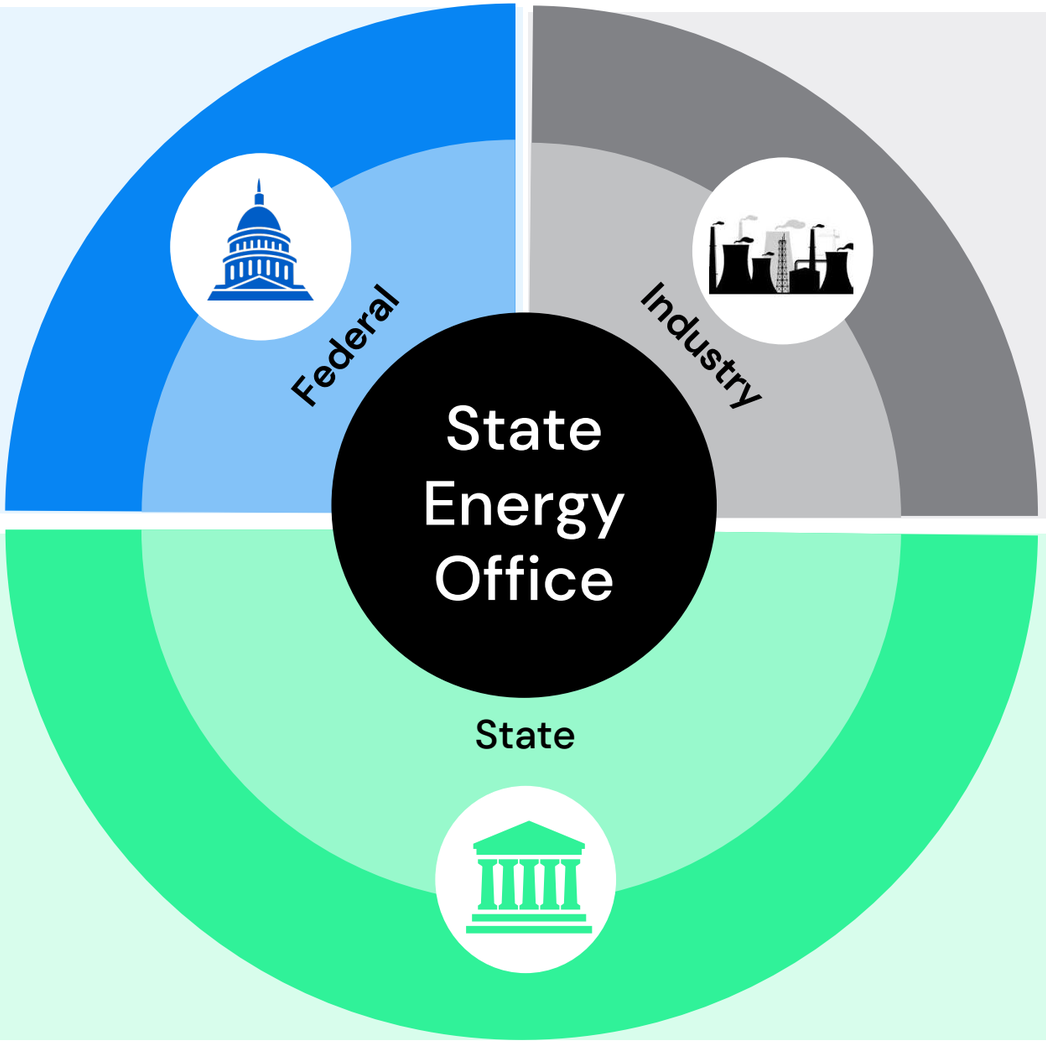
THE BEST EMPLOYERS FOR DIVERSITY | Forbes 2022 POWERED BY STATISTA

ICF's approach to developing state energy security plans



Stakeholders

- Department of Energy
- FBI
- CISA
- TSA
- PHMSA
- National Guard
- ISACs



- Electric Utilities
- Natural Gas Utilities
- Petroleum Terminals
- Pipeline Operators
- Refiners

- State Emergency Management Agency
- Public Utilities Commission
- DOT, DOH, DEP

- Governor's Office, especially if there is a Cybersecurity point of contact
- State fusion center
- State Police

Stakeholder questions

Threats/Hazards

- What are the key threats and hazards impacting energy systems in the state?
- Are there any specific infrastructure that are uniquely vulnerable in the state?
- Are any regions or communities of the state that are uniquely vulnerable?
- Understand timelines for repair and replacement activities. (Crew shortage, transformer supply issues, etc.)
- Understanding energy asset ability to continue operations if OT/IT offline?

Communication/ Coordination

- Discuss your emergency response plan. Are different stakeholders engaged if it is a cyber or physical event?
- Do you participate in regional planning or response? (Other states, utility mutual aid)
- What formal event reporting requirements, if any, are you subject to at the state level?

Response

- What resources do you have available to deploy during events? What resources can you request from other stakeholders?
- What regulatory waivers can you grant (or request)? (HOS waivers, RVP, etc.)

Mitigation

- What mitigation activities do you have underway (or identified as next steps) for critical energy infrastructure?

Cyber and physical impacts come in many forms

FBI Thwarts Targeted Plot To Attack Maryland's Electrical Substations

Four substations attacked in Washington state, leaving thousands without power

FBI investigating damage to substation for Keystone Pipeline

U.S. regulator releases report blaming Freeport LNG blast on inadequate processes

Hackers stole data from multiple electric utilities in recent ransomware attack

North Carolina power outages could last days after shooting attacks on substations

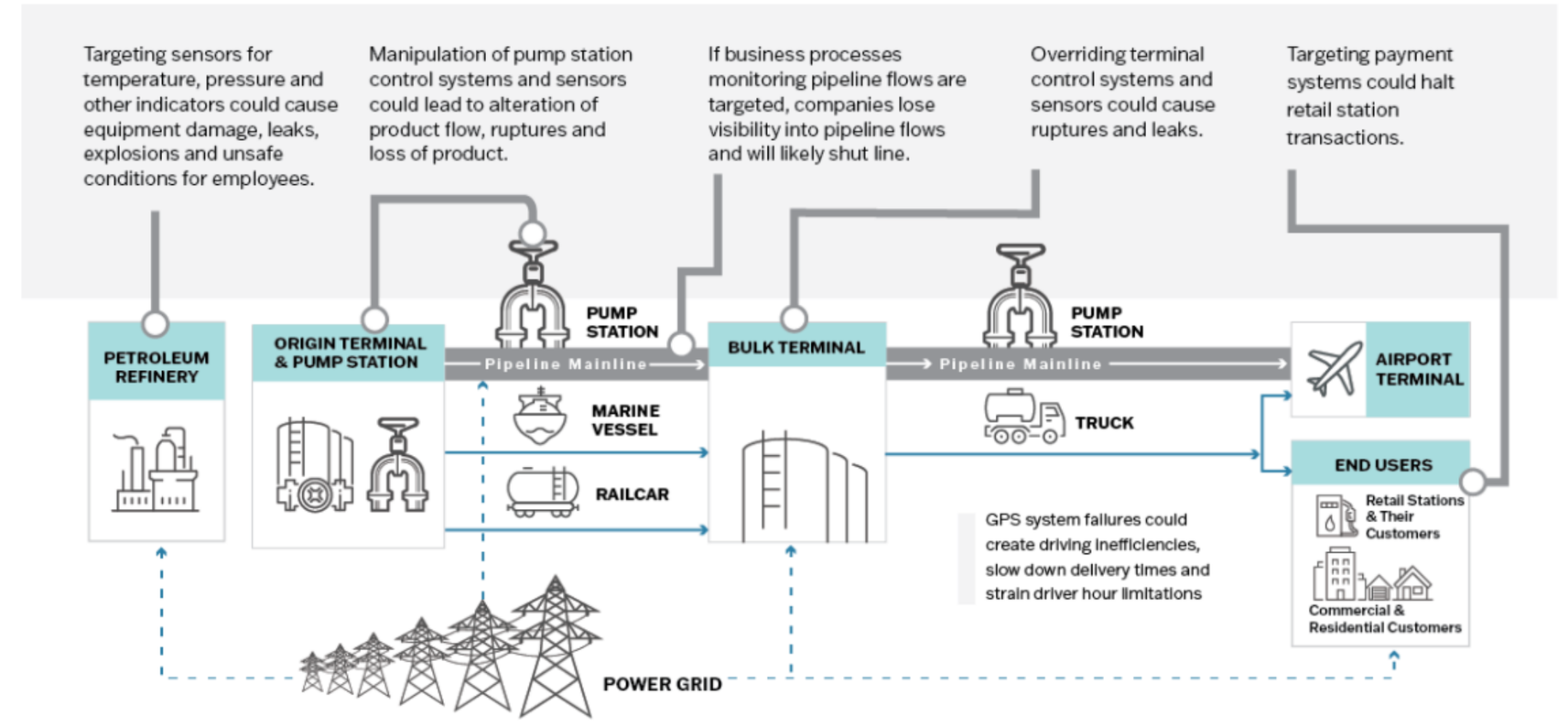
Hackers Breached Colonial Pipeline Using Compromised Password

Car hits pole, takes down power lines during early morning crash in Northeast Philadelphia

Enbridge briefly shut Line 5 after protesters tampered with pipeline

Cybersecurity threats and impact

Exhibit 7: Examples of Cyber Threats to the Liquid Fuel Supply Chain



A **cyberattack** resulting in widespread power outages could disrupt operations for refineries, pipelines, terminals and end users. For example, a power outage at a refinery that disrupts cooling water or steam generation could damage equipment, shut down processes and create unsafe conditions. Manipulation of power plant sensors or other generation infrastructure could damage equipment and cause a power plant to go offline.

A **ransomware** or other IT attack on company headquarters or data servers could limit ability to access and/or keep private company data, complete financial transactions, access internal company software or maintain a public-facing website. Attacks on IT infrastructure may result in the company proactively shutting down physical infrastructure.

Maryland Energy Administration

[Maryland liquid fuel plan]

7

Risk assessment

Threat exposure

- Likelihood of event occurring
- Location

Vulnerability

- Factor to account for potential event impact

Consequence

- Asset importance
- Alternative supply

8

Mitigation options to consider and/or fund

State

- Requiring utilities to submit cyber resilience plans to the PSC or PUC (E.g., Maryland)
- Increasing penalties for physical attacks on energy infrastructure: North Carolina, South Carolina, Arizona
- Conducting cyber and physical exercises
- Sharing best practices

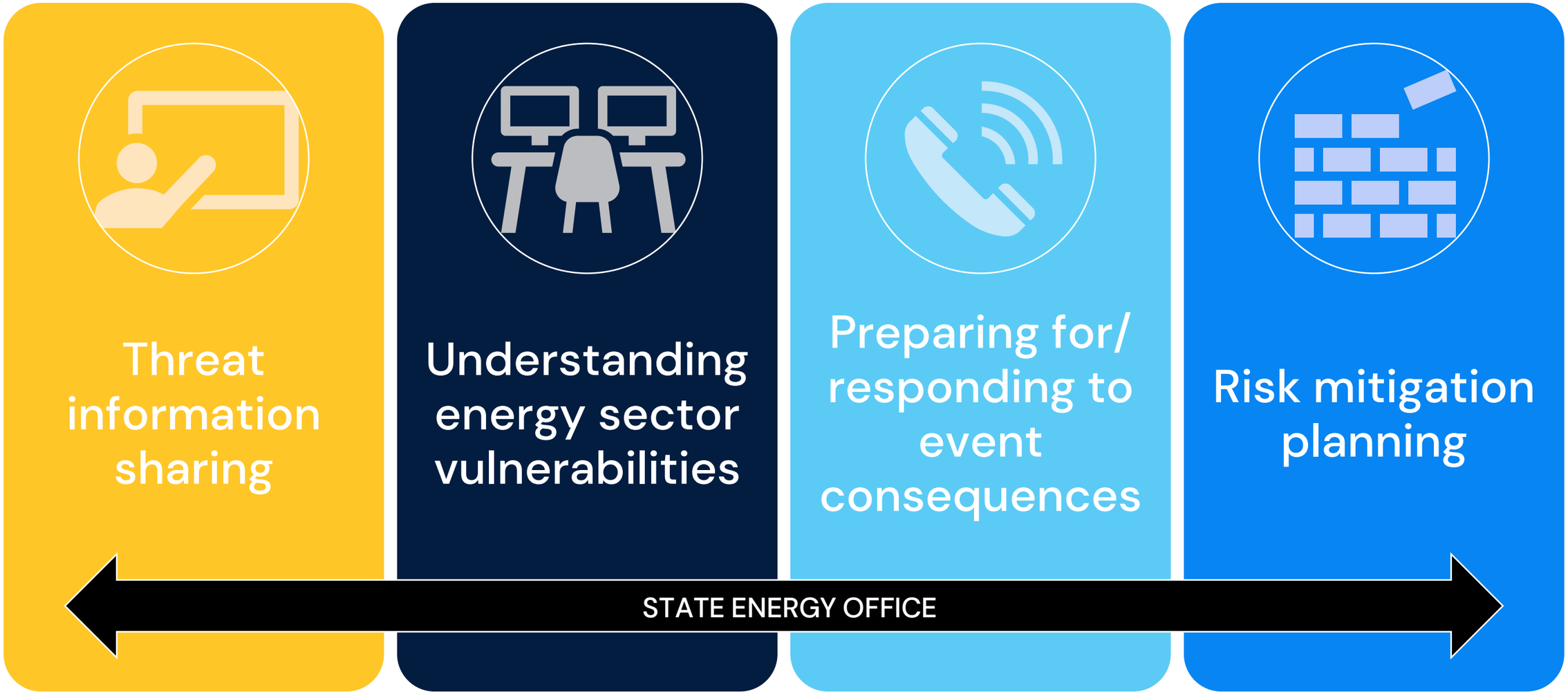
Industry

- Increasing redundancy of electricity systems
- Coordinating with other utilities for mutual assistance and agreements to share transformers, etc., if needed
- Contracting private companies to increase cyber security/evaluate cyber resilience
- Collaborating with other utilities on cyber resilience and sharing best practices
- Applying for grants for mitigation funding
- Conducting exercises
- Upgrading security operations centers
- Hardening transmission infrastructure, including perimeter fencing, electronic monitoring equipment, and improved access control
- Testing new equipment to assess potential and cost-to-benefit tradeoff

Federal

- Funding opportunities
- Establishing standards and regulatory requirement (TSA cybersecurity requirements for pipelines; NERC CIP-014 for physical security and multiple CIPs for cybersecurity)
- Facilitating information sharing between private sector and/or states on threats
- Assisting with threat assessment

Summary: SEO's Role in Energy Sector Cyber and Physical Security



Questions?

Get in touch:

Matt Kelly

Director, Energy Markets, ICF
Matt.Kelly@icf.com

icf.com

linkedin.com/company/icf-international/

twitter.com/icf

https://www.facebook.com/ThisIsICF/

About ICF

ICF (NASDAQ:ICFI) is a global consulting and digital services company with over 8,000 full- and part-time employees, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future.