Experts Roundtable on Energy Cybersecurity Coordination and Information Sharing among State, Federal, and Utility Officials

Thursday, August 15, 2019

Hall of the States, 444 North Capitol Street NW, Room 333, Washington, DC

BACKGROUND

Establishing and maintaining a secure and reliable energy sector is a top priority for governors, state regulators, and officials, as it is for the electricity sector, the oil and gas sectors, and the federal government. Through collective actions, these players have established productive working relationships and reduced risks to the energy sector posed by natural phenomena, and manmade physical and cyber threats.

However, there are a variety of coordination and information sharing gaps that risk slowing additional progress and may challenge response to future incidents. These include:

- Questions surrounding the roles and responsibilities of private industry and government in cybersecurity;
- Challenges sharing sensitive cybersecurity threat information and coordinating response and recovery between states and the energy sectors during a cyber incident; and
- Information silos that may undermine unity of messaging and emergency communications during energy emergencies and cyberattacks.
- Coordination issues that complicate the process for granting state and federal waivers/permits to facilitate mutual aid;

This roundtable discussion will convene experts from state government, federal agencies, and the energy sector to identify best practices and solutions to mitigate future cybersecurity threats and respond and recover from cyber-attacks more effectively, particularly focused on coordination and information sharing.

OBJECTIVES AND GROUND RULES

This one-day experts roundtable, hosted by the National Governors Association with support from the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER), will examine policies and actions to improve coordination and information sharing between the states, energy sectors, and the federal government in preparation and response to future cybersecurity threats and emergencies. The discussions will inform the preparation of a whitepaper to be released later in 2019.

This is an invitation only meeting, closed to the press, to encourage open dialog. Discussions will not be directed at consensus and remarks will not be cited for attribution. While some sessions will feature brief introductory presentations, the primary goal is to foster engaged discussion among all participants throughout the day.

PRELIMINARY DISCUSSION GUIDE

8:30 a.m. – 9:00 a.m. **Registration and Breakfast**

9:00 a.m. – 9:45 a.m. **Welcome, Discussion of Objectives and Introductions**
NGA staff will open the meeting, welcome participants, facilitate introductions, and discuss the objectives of the meeting.

- **Sue Gander**, Division Director, NGA Center: Energy, Infrastructure & Environment
- **Lauren Stienstra**, Program Director, NGA Center: Homeland Security and Public Safety

9:45 a.m. – 10:30 a.m. ***Breakout Discussion:*** **Perspectives on Roles and Responsibilities**
To establish a baseline for discussion throughout the day and begin identifying opportunities for improved coordination, participants will break out into respective groups of state, federal, and industry representatives to discuss how they work with partner organizations to prepare, respond, and recover from cybersecurity energy emergencies. Each group will designate one person to report out at the end of this session.

Questions to answer:
Please answer the following for your sector.

- What are your sector's responsibilities prior to a cybersecurity incident in the energy sector?
- What are your sector's responsibilities during or after a cybersecurity incident in the energy sector?
- What information does your sector need from other stakeholders to better meet those responsibilities?

10:30 a.m. – 12:00 p.m. ***Roundtable Discussion:*** **Defining Roles and Responsibilities Before, During and After a Cybersecurity Energy Incident**
Based on the preceding breakout discussion, participants in this session will evaluate the outcomes of the breakout session and discuss which actors should have which roles and respective responsibilities to improve information sharing and coordination.

Moderator: Dan Lauf, Program Director, NGA Center: Energy, Infrastructure & Environment

Discussion Questions:

- Who are the state, federal, and private sector actors that need to be involved in the planning for, response to, and recovery from an energy cybersecurity incident?
- What challenges exist for you and your respective organization/state that inhibit coordination with other sectors?

- What expectations does your organization have when engaging with the state on a response related to an energy cybersecurity incident? What expectations do states carry for private sector engagement?
- When and how should states be notified and involved in planning and response for a cyber-attack?
- How can states, the federal government, and the energy industry cooperate to ensure the continuity of critical business services to the public during a cyber-attack and/or energy incident?

12:00 p.m. – 1:00 p.m. **Lunch & Keynote**

Introduction: Sue Gander, NGA Center

Update on Federal Resources

- **Kate Marks**, Director for State, Local, and Tribal Policy Analysis, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

1:00 p.m. – 2:00 p.m. **PRE-BOOM**

Roundtable Discussion: **Joint Threat Information Sharing and Coordination for Prevention and Protection before a Cyber Incident**

In this session, participants will discuss what threat and vulnerability information needs to be shared with state and utility partners and how threat information sharing should be handled pre-cyber incident.

Moderator: Reza Zommorodian, Policy Analyst, NGA Center: Homeland Security and Public Safety

Discussion Questions:

- What energy cybersecurity threat information is currently shared between the public and private sectors, including the states?
- What do you see as the biggest challenge to robust threat information sharing, externally and from within your organization?
- What is your biggest reservation or concern with sharing relevant energy threat or vulnerability information with other organizations or sectors? What cybersecurity protections and risk management practices need to be implemented?
- Is there a role for more declassified briefings? How can those be facilitated?
- How can governors/state government improve information sharing and facilitate improved coordination between the states, industry, and federal partners?

2:00 p.m. – 3:00 p.m.

POST-BOOM

Roundtable Discussion: **Information Sharing and Coordination During and After an Energy Cybersecurity Incident**

In this session, participants will identify what information gaps exist that may hinder response and recovery to cybersecurity energy emergencies and their biggest reservations or challenges to sharing additional information during an incident.

Moderator: **Alyse Taylor-Anyikire, PhD,** Senior Policy Analyst, NGA Center: Energy, Infrastructure & Environment

Discussion Questions:

- Once you know there is a cybersecurity incident, who do you contact, when and why?
- What information do you need from other partners during a cybersecurity incident that is not currently or adequately shared?
- At what point should states be notified about cybersecurity incidents or threats? What information is important to share with state partners?
- How can governors/state government improve information sharing and facilitate improved coordination between the states, private, and federal partners during an event?
- When or should a governor declare an emergency related to an energy cybersecurity event?

3:00 p.m. –3:30 p.m. *Break*

3:30 p.m. –4:30 p.m.

Roundtable Discussion: **Getting the Word Out**

Concise, coordinated, and timely messaging is critical during energy emergencies, whether real or perceived. People today expect information to be shared near-real time, especially during an energy disruption. This challenge is compounded by social media, where misinformation can lead to additional challenges. Inconsistent or conflicting information from states, the federal government and the sector can create confusion, public distrust, and more severe threats to health and safety. In this session, participants will discuss strategies and best practices for keeping the public informed during an energy cybersecurity incident and ensuring unity of messaging with all parties involved, including the states.

Moderator: Lauren Stienstra, Program Director, NGA Center: Homeland Security and Public Safety

Discussion Questions:

- How should governors, the federal government, and the energy industry collaborate in advance of an incident to ensure emergency communications protocols are aligned, systems are interoperable, and information is shared in a timely manner?
- What information is appropriate to disclose to the public if an incident is triggered by a cyber-attack? At what point should the energy sector or state government make a public announcement?
- What types of messages should be shared and what are the triggering points for those messages?
- Who should disclose that information to the public and how should other partners remain informed and coordinated? When should that information be shared?
- Who should be coordinating communication efforts during the recovery phase after a cyber-attack?

4:30 p.m. – 5:00 p.m.

Closing Remarks and Wrap-Up

During this last session, the group will identify major themes from the discussion. NGA will highlight takeaways and begin mapping steps for future action.

Dan Lauf, NGA Center