Day 1: Tuesday, April 28, 2026

9:00 - 10:00 am	Registration
9:45 - 10:45 am	**Black Start Escape Room hosted by INL** (optional, registration required)
	Lunch on Your Own
11:00 - 12:30 pm	Registration
12:10 - 12:25 pm	**Welcome from Wisconsin**
12:25 - 12:45 pm	**Keynote: Alex Fitzsimmons, Director of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at DOE**
12:45 - 2:00 pm	**The Cyber Threat Landscape** A comprehensive review of the current cybersecurity threat landscape. This briefing will discuss emerging threats and trends with a focus on threats to the US electricity and oil & natural gas (ONG) sectors, including a discussion of the particular threats to local energy assets in the distribution network.
2:00 - 3:15 pm	**Day in the Life – Utility Cybersecurity** This session will provide boots on the ground perspective of day-to-day battling cybersecurity threats. Discussion will feature different perspectives from power market administration, electric and natural gas utilities on how they monitor and address cyber-attacks.
3:15 - 3:30 pm	**Networking Break**
3:30 - 4:45 pm	**What to Expect When You Get Cyber Hacked** This panel will have real-world case studies. Based on recent cyber incidents they have experienced and proximity to threats outlined in the mornings' briefing, panel will outline procedures to take after being hacked. Who should you call? Who do you have to call? Attendees will gain practical insights into the strategic and operational aspects of CISO's role.
4:45 - 5:00 pm	**Wrap-Up, Preview Day 2**
5:15 - 6:15 pm	**Black Start Escape Room hosted by INL** (optional, registration required)

Day 2: Wednesday, April 29, 2026

7:30 - 8:30 am	**Registration**		
8:30 - 9:00 am	**Welcome Keynote + Opening Activity**		
9:00 - 10:00 am	**Oil and Natural Gas Cybersecurity** This session will outline partnerships and sub-industries. It will cover key ONG cybersecurity standards, reporting requirements, and operational realities for oil and natural gas pipelines, storage, and related facilities. It will highlight the interfaces between federal requirements and state authorities, and discuss where state officials can support planning, exercises, and incident coordination with operators.		
10:00 - 10:15 am	**Networking Break**		
10:15 - 11:15 am	**Cyber Workforce Development** This panel examines workforce pipeline models for state agencies and industry, strategies for placing cybersecurity experts in smaller utilities, partnerships with academia, and initiatives like CyberForce that are building the next generation of cyber talent.		
11:15 -12:15 pm	**Supply Chain and Procurement** Participants will leave with example template language and checklists they can adapt for solicitations, subgrants, and cooperative agreements. Discussion will cover model contract clauses, how to coordinate with state procurement officers, and the use of whitelists, blacklists, Cyber-informed Engineering (CIE), and SBOM analysis to reduce risk.		
12:15 - 1:15 pm	**Working Lunch:** **Andy Bochman, Resilience Strategy Lead, West Yost**		
1:15 - 2:15 pm	**Cybersecurity for New Generation Technology** Panel will outline cybersecurity considerations for new generation technology including small modular reactors, geothermal, hydrogen and other more digitally connected generation sources.	**Supply Chain and Procurement: "Fix the RFP" Mad Libs**	**Black Start Escape Room hosted by INL**
2:15 - 3:15 pm	**Cyber Insurance and Quantification of Risk** Session will cover how utilities and energy producers insure themselves. Discussion will also include guidance on how to package and present salient information on risks to leadership to ensure organizational buy-in and investment.	***Brainstorming*: Human-AI Collaboration to Attack Difficult Problems**	**Black Start Escape Room hosted by INL**
3:15 - 3:30 pm	**Break**		

3:30 - 4:45 pm	**Review of New NASEO Cyber Resources & Cy-Phy Working Group Outcomes** Walkthrough NASEO Cyber Toolkit. Topics will include incident coordination, ONG, and fundamentals chapters, plus case studies and checklists. Discussion of Cyber-Physical Working Group findings, resources, and outputs.
4:45 - 5:00 pm	**Wrap-Up, Preview Day 3**

Day 3: Thursday, April 30, 2026

8:30 - 8:45 am	**Welcome**
8:45 - 9:30 am	**Cyber Stories from the Field** Case studies of actual cyber incidents.
9:30 – 9:45 am	**Networking Break**
9:45 - 10:45 am	**Standards and Legislation** Baseline session to help states understand key cybersecurity standards and frameworks including when and where they apply, and why they matter for state policy and programs. The discussion will distinguish between mandatory standards, such as NERC CIP for certain electric assets, and voluntary frameworks, such as the NIST Cybersecurity Framework and relevant IEEE standards. Topics for this session will include AI, critical energy infrastructure Information protections. Perspectives from Industry will be included in this discussion.
10:45 - 11:45 am	**Information Sharing and Cross-sector Interdependencies** Session will focus on state roles in improving cybersecurity and integrating efforts with the private sector and multiple state agencies across the entire energy sector. Topics will include how to process threat intel, what do you do? Learn your role; how to build trust and practical info-sharing avenues with industry by ensuring information is protected. Discussion will explore common barriers such as liability, regulatory exposure, and reputational risk, as well as practical solutions such as anonymization, aggregation, and use of trusted intermediaries.
11:45 - 12:00 pm	**Closing Remarks and Prizes**