RESPONSE of PACIFIC NORTHWEST NATIONAL LABORATORY

Additional Questions for the Record

March 23, 2026

Contacts: Tara Robertson, tara.robertson@pnnl.gov

Rebecca O'Neil, rebecca.oneil@pnnl.gov

The Honorable Brett Guthrie (R-KY)

1. DOE is the energy sector authority and must work with other agencies and States. To do this effectively, it must have a culture of constant learning and improvement, which will benefit the whole federal approach to support the energy sector.

a. Would you speak to the importance of a culture of constant learning and constant improvement for the stakeholders you represent?

ANSWER:

- State energy security planning reflects the same culture of constant learning that you describe here. Plans are updated regularly (no more than 5 years) to account for changes in risk dynamics and energy system demand and infrastructure; the goal of a risk assessment is to analyze and learn something new, rather than rely on existing established systems.
- Three ways that the CESER-state energy security program advances constant learning is:
    1. through coordinating across states to learn and share from peers, leveraging partnerships with state energy associations such as NASEO and NARUC;
    2. through technical evaluation, regional risk assessments and analyzing interdependencies at their true scale; and
    3. through national convenings on critical topics such as cybersecurity. This April in Milwaukee, we will host the second CyFERS conference to develop

state proficiency in cybersecurity, after the successful CyFERS conference last year in Salt Lake City.[1]

2. All the bills included in this hearing reflect measures that would support constant learning and improvement, whether through improved leadership, assistance and sharing, or coordination. How would these be useful to strengthen your work to safeguard and respond to threats?

ANSWER:

- Two hallmarks of CESER's mission are that it (1) encompasses all energy systems, not just electricity, and (2) focuses on an objective (security) rather than a technology. As noted, the bills would enhance CESER's roles and authorize continuous improvement cycles in coordination with states, utilities, and other federal agencies in part by leveraging the research and scientific excellence of the National Laboratories. The state energy security program under CESER helps to build a comprehensive and coordinated federal preparedness and response apparatus for energy systems, through supporting excellent planning, leveraging advanced mitigation technologies, and ensuring a baseline of security among all state and territorial partners in a deeply interconnected system.

The Honorable Rick Allen (R-GA)

1. The Savannah River National Lab (SRNL) is adjacent to my district. As I mentioned in the first panel, national labs play a critical role in grid security.

a. How can national labs be leveraged to use their trained cyber operators to enhance security operating technologies?

ANSWER:

- National laboratories can help the energy sector advance-cyber operational technologies by integrating grid model data, OT telemetry, and cyber threat information to deliver operational insights, mitigation, and response options. They

[1] https://www.pnnl.gov/events/cybersecurity-energy-resilience-summit-cyfers-2026

can connect cyber activity to physical and reliability consequences, so owners and operators can make faster, risk-informed decisions and response to incidents. National laboratories are particularly important where private-sector tools may be limited by reduced access to classified or cross-sector information and scale. These strategies directly support CESER's priorities for AI-enabled detection, response, recovery, and operate-through-compromise.

- National laboratories leverage broad expertise in understanding the fundamental operations of physical processes combined with our advanced study of the adversary. Federal investment in this range of capabilities means we can leap-frog common risks and vulnerabilities to our national critical infrastructure. National laboratories can also take on the high-risk high-reward research and development that industry is unable or unwilling to fund. This mix of mission with scientific expertise uniquely positions the laboratories to both lead and inform industry while remaining relevant to government priorities and needs.
- PNNL has in-depth experience in threat hunting, cyber-physical systems phenomenology, supply chain risk management, proactive cyber defenses, and AI-agent-based defensive operations. We are a close collaborator with all of the Department of Energy's national laboratories and would be pleased to convene and explore this question further with our partners at Savannah River NL.

The Honorable Mariannette Miller-Meeks (R-IA)

1. You led the effort to help all 56 states and territories complete their energy security plans. The SECURE Grid Act would add requirements related to supply chain security and threats to local distribution systems. Based on your work with states:

a. **How well are states currently assessing supply chain risks in their energy security plans?**
b. **What challenges do states face in getting visibility into supply chain vulnerabilities, especially for critical components like transformers and inverters?**

c. How would the proposed changes in the SECURE Grid Act improve state planning around supply chain risks?

ANSWER:

- *State analysis of supply chain risks:* Energy system supply chains are global and complex. Energy system supply chain concerns range from the origin of components to digitization of legacy infrastructure.

- Supply chain vulnerabilities for the states can come in many forms – they may come in resource constraint (e.g. fuel), a lack of available components (hardware and software), and concerns about exposure to cyber threats due to overseas manufacturing. In state energy security plans, some of the most robust analyses on supply chains are concerned with access to fuel, especially where the reliance on refined fuel is entirely outside of the state or limited to a few channels.

- Each state and each energy sector have varied challenges when it comes to supply chain vulnerability *mitigation*, or how to respond to supply chain risks. For instance, one state may face difficulties accessing ports for liquified natural gas imports, while another may have bottlenecks associated with the delivery of critical components (e.g., switchgear or pipeline materials) due to limited rail capacity, long lead times, or constrained workforce availability. State mitigation strategies for supply chains included looking to alternative fuels for transportation infrastructure, strategic distributed fuel storage, and additional focused analyses to pinpoint specific vulnerabilities in the state's supply chains.

- States additionally showed awareness that grid components had long lead times and due to their costs, would not make sense to stockpile. State Energy Security Plans have referenced the greatest challenge regarding grid equipment supply chains is that these essential components have little to no manufacturing facilities domestically in the United States.

- *Challenges for state visibility into supply chain vulnerabilities:* States rely on coordinated industry data and reporting to build insights into supply chains. These forms and methods assure uniformity and help states build technical expertise to understand changes and place the information into a risk analysis workflow.

Analyzing fuel availability requires understanding import/export exchanges, multi-modal fuel delivery mechanisms such pipelines and tankers, and distribution channels and available storage capacity. Unfortunately, some of these mechanisms for information collection have been recently discontinued, and known excellent data platforms are only available behind a paywall with a price beyond the reach for most states.

- States are aware that supply chains present cybersecurity vulnerabilities for adversaries to exploit. One method to reduce this risk and improve supply chain resilience is to develop strong stakeholder engagement throughout all nodes of the supply chain. Having strong relationships can better ensure communication and potentially faster mitigation during disruptions. Both the Department of Energy and Department of Homeland Security provide supply chain guidance documents; however, these are now four and seven years old respectively. States could also require hardware and software vendors to provide energy system customers with a "bill of material" so that customers can have adequate transparency into product development features and evaluate risk when new vulnerabilities are exposed. Another method asset owners are implementing to mitigate supply chain risk is to adopt mutual aid agreements that allow for sharing of essential equipment; however, in the event of a disruption transportation logistics may hinder this support.
- *How the SECURE Grid Act would change state planning:* The SECURE Grid Act would amend the requirements for State Energy Security Plans to ensure that states address supply chain risks for electricity system equipment, including generating facilities. As noted above, states already recognize a wide and deep array of supply chain threats, rely on available data and reporting, and compile these insights into a state-specific risk analysis. This new requirement would clarify Congressional direction and emphasize Congressional priorities for state risk analysis. Considerations regarding adding this requirement would be assuring state access to timely data and industry reporting, which is not uniformly available; and clarifying aspects of supply chain risks that are of greatest concern, as the provision directs all components of the electricity system to be addressed.

2. Your research focuses on transmission infrastructure and wildfire hazards. I lead legislation, the Limiting Liability for Critical Infrastructure Manufacturers Act, that provides domestic manufacturers of critical grid components legal certainty so they can invest in American workers rather than hedging against frivolous legal risk. Can you speak to:

a. **How do wildfire risks and associated liability concerns affect utilities' ability to source critical equipment like transformers and switchgear?**
b. **What does this liability risk do to domestic manufacturers when utilities must turn to foreign, potentially Chinese, suppliers who don't face the same liability risk?**
c. **From a research perspective, how important is it to maintain a robust domestic manufacturing base for critical grid components?**

ANSWER:

- *Utility exposure to wildfire liability and connection to the supply chain*: As you note, the threat of wildfire – both withstanding wildfire and avoiding ignition of wildfire – has led electric utilities to invest billions of dollars into hardening distribution and transmission systems.[2] To our knowledge, supply chains for grid equipment explicitly for wildfire mitigation are not a limitation. Pole wraps and other early solutions were a supply chain challenge at one point, but we understand that those challenges are not currently significant. As wildfire hazards move from west to east and become more prevalent across the country, we anticipate continued upward pressure on grid equipment supply chains.

- We also note that liability for electric utilities related to potential wildfire ignitions, typically from conductors interacting with vegetation, has become an acute issue for utility risk management and is an active topic of discussion in state policy. Unlike other causes of widespread devastation such as hurricanes, wildfire is a hazard that can occur naturally, but it can also be caused by people and notably

[2] "Cost Recovery Mechanisms for Utility Wildfire Mitigation." Memorandum to Kansas Corporation Commission, February 2026. Pacific Northwest National Laboratory. https://www.pnnl.gov/sites/default/files/media/file/Final_Cost%20Recovery%20Memo_February%202026.pdf

electric utilities. PNNL research has documented the asymmetrical risk of liability for wildfire ignitions, the ways utilities have invested in mitigation to reduce the potential for wildfire ignition including pre-emptive interruption of power delivery, and how this risk has caused extraordinary changes and costs in utility finance and business models, including the possibility of bankruptcy.[3]

- *Regarding the security benefits of domestic manufacturing*: the lack of available trusted domestic equipment manufacturers hinders the ability to acquire secure critical modern components for energy asset owners. Furthermore, the trusted component of supply chain acquisition cannot be understated, as gaps in supply chain security are pivotal opportunities for attacks from adversaries, particularly with cyber-connected devices. These vulnerabilities can be exploited, causing system or network failures.
- *From a research perspective*, domestic manufacturing is critically important for future investments in the electrical grid and should be addressed. From an in-progress PNNL report, *Securing the US Grid Material Supply Chains*:

"Domestic production of grid equipment (transformers, transmission cables, switchgear) falls short of demand, especially for large transformers—roughly 80% are imported—and even U.S.-assembled equipment depends heavily on foreign parts. Upgrading the grid requires accelerating production capacity of grid equipment in the country, which in turn requires secure supply chains for engineered components (electric steel laminates, copper bars, permanent magnet pucks, and aluminum rod), and the critical material feedstocks (electric steel, copper, aluminum, iron, manganese, silicon, and rare-earths) and equipment available to manufacture them. Lead times for critical equipment have increased exponentially in recent times.

"Sensing demand, several equipment manufacturers are increasing domestic grid equipment manufacturing capacity through federal programs which collectively provide

[3] Coleman A., et al. (2026). *Current Best Practices on Wildfire Risk Reduction for Electric Transmission and Distribution Systems*. Richland, WA: Pacific Northwest National Laboratory. PNNL-38528. https://www.pnnl.gov/projects/wildfire-risk-resilience/best-practices. DOI: https://doi.org/10.2172/3016062
Barlow, J., et al. (2025). *Wildfire Risk: Review of Utility Industry Trends*. Richland, WA: Pacific Northwest National Laboratory. PNNL-SA-211619. https://www.pnnl.gov/projects/wildfire-risk-resilience/changing-utility-business-models

demand signals, financial support, and policy frameworks encouraging private sector capacity expansion. However, decades of offshoring and underinvestment have weakened domestic material, component and manufacturing equipment supply chains, slowing grid modernization efforts. Primary material production is dwindling in the country, and recycling remains underutilized due to technical, economic, and infrastructural obstacles. Much scrap is exported or lost, and few recycling systems exist for high-value applications, particularly for rare earths. Shortfalls in one material affect the entire grid upgrade process, causing delays and higher costs amid global demand and regulatory pressures. Manufacturing expansion is further hampered by a lack of robust heavy equipment and tooling base, which is mostly produced abroad. This secondary dependency further restricts domestic production growth and prolongs grid modernization timelines.

“To alleviate this situation, to expand grid capacity by facilitating increased production of grid equipment in the near-term and reduce foreign dependence, a multi-pronged approach is required, organized around complementary strategies:

- Improving engineered product volumes through AI-driven process optimization, autonomous manufacturing systems, digital twins, predictive maintenance, and advanced manufacturing techniques including thin-strip casting, friction extrusion, additive manufacturing, and atmospheric pressure chemical vapor deposition.
- Developing secure local material supply chains through both enhanced recycling—employing automated disassembly, advanced sorting, improved insulation removal, and melt-free recycling technologies—and development of high-performance drop-in replacement materials including advanced soft magnets, next-generation conductors with nanoscale additives, advanced dielectrics, and rare-earth-free permanent magnets.
- Securing equipment and tooling supply chains through modular equipment design, advanced fabrication including large-scale additive manufacturing, digital twin-enabled development, advanced tooling materials, and federal financing and procurement incentives.

“Current efforts in grid material and component supply chains development exhibit significant gaps. GOES-specific manufacturing[4] and recycling R&D receives disproportionately little attention relative to its supply chain criticality compared to permanent magnets. Most advanced manufacturing research concludes without translation to commercial deployment. Insufficient coordination exists between upstream materials R&D and downstream grid equipment manufacturing needs. University programs in electrical steel metallurgy have declined, creating workforce concerns. Research on grid-relevant structural steels and high-temperature insulation systems for grid and data center applications is emerging currently.

“Securing the U.S. grid's supply chain is a critical infrastructure challenge, spanning material extraction, recovery, manufacturing, assembly, and equipment needs. These interdependent layers require coordinated solutions, as fixing one bottleneck alone isn’t enough. Domestic production cannot keep up with rising demand for grid materials and equipment, creating heavy import reliance and vulnerability to geopolitical and trade disruptions. Expanding capacity takes years, but the need for grid modernization is urgent. Promising short-term approaches include high-performance materials and advanced recycling, which can boost grid capacity using existing infrastructure and reduce import dependence. Accelerated commercialization of these technologies is needed. Equipment and tooling also require strategic focus; without them, domestic manufacturing can't expand. Reviving industrial machinery through modern design, partnerships, and incentives should be prioritized.”

- PNNL would be pleased to follow up with a complete copy of this paper or technical consultation if desired.

3. Iowa State University is leading CyDERMS, a regional cybersecurity center focused on securing Distributed Energy Resources. As we integrate millions of new devices we're dramatically expanding the attack surface of our grid. At the same time, we're deploying AI and machine learning tools to detect attacks and manage these distributed systems. This creates a paradox: we're using high-tech AI solutions to

[4] GOES stands for grain-oriented electric steel, the magnet laminates that are used in transformers. The reason that new transformers have a 2-3 year lead time is the supply chain for GOES.

secure increasingly complex systems, but that technology itself could be a vulnerability.

a. **How do you think about this balance?**
b. **Are there certain applications where simpler, lower-tech approaches might actually be more secure?**
c. **How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?**

ANSWER:

- *Balancing cyber-protections with AI*: As you note, while AI can help us manage DER-scale or grid-edge device complexity, AI also becomes part of the critical attack surface. A recent international event involving distributed energy resources highlights the risk: when there are many remotely managed devices, attackers do not need to breach a utility control center to create an electricity system impact. And, if there are common vulnerabilities across all assets, the attack is easily replicable. If DERs are compromised, a loss of integrity could damage the distribution system, grid-edge connected devices, and if coordinated over a large footprint, the bulk power system. DOE's Cyber Informed Engineering strategy, along with modern approaches to cybersecurity (e.g., software-defined networking, zero trust) can help reduce the attack surface while enabling the benefits of widespread connectivity.

- *On the question of low-tech simpler solutions:* flexibility in software can be a great strength when it comes to general purpose computing, but this flexibility is a weakness when it comes to critical infrastructure cyber-protection. In contrast, analog or electromechanical devices operate according to the laws of physics. Their behavior is deterministic. Given specific inputs, their output is guaranteed. In situations where the consequence of failure is physically irreversible or catastrophic (e.g., loss of life), protection logic can be implemented using analog or electromechanical devices. Purpose-built, these devices only do one thing but are proven to be safe and secure. Programmable digital devices (i.e. software) can contain undiscovered vulnerabilities and can be modified through numerous methods, from well-meaning customers to compromised supply chains.

- There are plenty of tried-and-true low-tech cybersecurity practices that are more secure than complex AI solutions, such as strong authentication, least privilege, network segmentation, and patching updates.
- One challenge for the DER industry and distribution utilities is a consistent standard for adoption: many of these controls are not consistently implemented at the device or owner-operator level. As a result, DER cybersecurity practices can be voluntary or uneven. As many DER owners and small operators do not have dedicated IT/OT staff, basic security hygiene can be hard to sustain, which leaves gaps that attackers can exploit.
- *Ensuring secure AI*: In the current environment, human-AI partnerships are necessary, leveraging the strengths of both to quickly detect incidents, rapidly respond to incidents to decrease adversary effectiveness, and recover more quickly from incidents.
- We already trust computers to take the appropriate action at "line speed" –in the millisecond timeframes—much faster than a human can reason or act. Explainable AI will be crucial to building trust in AI systems. When critical life safety decisions must be made, ideally there should be a human-in-the-decision-loop. At the same time, there may not be time to alert a human and wait for a decision. Strict requirements and requirement traceability throughout the software lifecycle (similar to how the Nuclear Regulatory Commission approves designs[5]) should be used to evaluate AI. Due diligence should be in line with impact of an incident.
- Standards, best practices, and patterns for explainable and trustworthy AI are needed to ensure consistency in the implementation of artificial intelligence systems. For example, digital communications and controls standards for DER usage can be standardized, rather than multiple tools with inconsistent coverage by multiple vendors. Knowledge that does not change can be marked as immutable (i.e. permanent). Knowledge the changes over time should have an "expiration date" to avoid being slowly changed over time, but remembered forever (i.e. poisoned by an adversary).

[5] https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/new-nuc-plant-des-bg

- Decentralization within the power system, with more extensive communications and controls, enables more functionality and responsive capabilities to disruptions. At the same time, through vast deployment of interconnected devices with various control platforms, new vulnerabilities to cyber threats are created. Operators want transparency and visibility into the system but also new observational strategies to manage this level of complexity. Physics-based ML/ AI offers an improvement over traditional methods for observing power system conditions. As noted in a PNNL-authored IEEE conference paper, "[I]ncreased dependency on communication networks exposes [smart grid] infrastructure to cyber-physical security threats, such as false data injection (FDI) attacks. Currently, real-time monitoring of power systems is done through State Estimation (SE). SE has error processing capabilities; however, it is limited to steady-state assumptions and lacks compatibility to the rapidly evolving demands of cyber-physical security in smart grids. In contrast, machine learning solutions consider temporal and spatial information to validate data and learn the normal state of a properly functioning grid to detect anomalies introduced in field measurements. Together, physics-based and data-driven methods can complement one another to provide a promising outlook for cyber-physical security in smart grids."[6]

- Using physics-based data to analyze the behavior of operational technology (OT) systems is an active area of research at PNNL and a promising direction that goes beyond today's "physics-informed" methods. Traditional physics-informed approaches mainly compare measurements from the physical process to what the cyber layer (e.g., an HMI) reports, and they are primarily effective at mitigating one class of threats: false data injection attacks (FDIA).

- In contrast, side-channel techniques—physics-based modalities long used to extract sensitive information from computing systems—are now being adapted for defense. By collecting physics-based sensor data from multiple components across OT and power systems (not only the primary physical process), defenders can correlate and corroborate cyber/logical data with independent physical

[6] Vega-Martinez V., et al. 2022.*Hybrid Data-Driven Physics-Based Model Framework Implementation: Towards a Secure Cyber-Physical Operation of the Smart Grid***.** Piscataway, New Jersey:IEEE.PNNL-SA-171685.doi:10.1109/EEEIC/ICPSEurope54979.2022.9854693

evidence. Combined with machine learning methods that fuse signals and cluster behavioral states, these richer datasets can characterize system behavior more completely, reduce false positives, and improve detection of novel attacks and other anomalies.

- In conclusion, there are strategies that can meaningfully reduce risk, but there is no one-size-fits-all approach and no “ultimate” solution—rather the strategy is a range of controls that one can combine based on the system and the consequences. AI, just like any cybersecurity ecosystem, needs its own set of rules and a system.