House Energy & Commerce Committee
Subcommittee on Energy
"Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid."
December 2, 2025

Zach Tudor
Associate Labe Director, National & Homeland Security
Idaho National Laboratory
Responses

The Honorable Robert Latta (R-OH)

Q1. What is the Idaho National Lab doing to help ensure people are well trained and focused on the most important cybersecurity and physical threat risks?

Answer: Since 2007, the Idaho National Laboratory has been addressing a critical workforce gap in cybersecurity and physical security training for critical infrastructure — a gap that traditional industry training programs and university curricula haven't been able to fill. While workforce training isn't traditionally the purview of national laboratories, INL stepped into this role because operational technology (OT) and industrial control systems (ICS) security require highly specialized, hands-on expertise that wasn't available elsewhere.

What distinguishes INL's training approach is our deep bench of experts, across all mission areas, who are conducting cutting-edge research and development. Our instructors aren't just teaching established curricula — they're researchers and engineers working at the forefront of cybersecurity threats, vulnerability analysis and defense technologies. This enables us to use training and knowledge transfer as a direct mechanism for deploying and disseminating the latest solutions. Our programs reflect updated approaches that are directly applicable to real-world problems, delivered as close to real time as possible as threats evolve.

Our training programs provide immersive, practical experience that goes far beyond classroom instruction. In February alone, we conducted our Accelerate training program, hosted an ICS Detect the Attacker threat hunting course, hosted an ICS 301 course, and hosted members of the U.S. Army Cyber Command for specialized training. We also delivered a CyberStrike training workshop in Los Angeles focused on coordinated cyberattack defense in the lead-up to the 2028 Olympic Games and sponsored an interactive ICS Escape Room at the DISTRIBUTECH Conference in San Diego for power grid professionals. Many of these training programs draw on lessons learned from actual cyber events that have impacted global critical infrastructure.

These efforts build on nearly two decades of program development. Working closely with the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, we've developed training courses specifically for securing ICS. That includes ICS 300/301, Fundamentals of Industrial Control Systems, and specialized nuclear cybersecurity training for advanced reactor technology. Programs like Liberty Eclipse prepare utilities with

practical tactics, techniques and procedures to restore the grid following a cyber event, while the Operational Technology Defender Fellowship develops the next generation of OT cybersecurity leaders.

We also leverage partnerships with academic institutions — including the University of Texas at San Antonio, University of South Florida and University of Utah — as well as organizations like Cyber Florida at USF and the Forge Institute to strengthen cybersecurity talent pipelines. Through internships, fellowships and cooperative education programs, we provide hands-on experience that transforms theoretical knowledge into operational capability.

In fiscal year 2025, INL reached over 40,000 external trainees through 605 in-person and virtual engagements, totaling 215,164 person hours and awarding 12,249 continuing education units. These engagements spanned mission areas such as cybersecurity, control systems, defense, critical infrastructure protection, wireless communications and nuclear nonproliferation.

Q2. What specific risks do Chinese-manufactured inverters — found in solar, battery and other energy technologies — pose to the security and reliability of the U.S. electric grid?

Answer: The security and reliability risks associated with inverters and power electronics in distributed energy resources stem from both technical vulnerabilities and supply chain considerations, regardless of country of origin. However, the concentration of manufacturing in the People's Republic of China (PRC) presents specific challenges for the U.S. energy sector.

Supply chain concentration

Current market analysis indicates that PRC-based manufacturers produce approximately 70% of power electronics, inverters, control components, sensors and related devices used in U.S. energy systems. Over 90% of these technologies contain at least one critical component sourced from PRC manufacturers. This concentration has developed over approximately two decades through strategic investments in intellectual property acquisition, manufacturing capacity expansion and competitive market pricing.

At present, there is no completely domestically sourced solution for many of these technologies. Products that meet "Buy America" requirements typically do so through final assembly performed in the United States, while the underlying hardware and firmware — which represent the primary sources of technical risk — are manufactured offshore.

Technical security considerations

Several technical factors contribute to cybersecurity risk in inverters and power electronics:

- Undocumented communication protocols: Some devices contain communication capabilities that are not fully documented in technical specifications, which can complicate security monitoring and network segmentation efforts.
- Authentication weaknesses: Weak credential management or insufficient authentication mechanisms can create pathways for unauthorized access or manipulation.

- Configuration vulnerabilities: Both foreign- and domestically sourced equipment can pose risks if improperly configured during installation or operation.
- Remote access capabilities: Connectivity features, while often necessary for operational management, introduce potential attack surfaces that require careful security controls.

Inspection and transparency challenges

Contractual agreements with some manufacturers have limited the ability of U.S. companies and utilities to conduct thorough security inspections of systems and components. Original equipment manufacturer agreements sometimes restrict deep technical analysis under intellectual property protection provisions. Greater transparency and inspection rights would enable more comprehensive security assessments and risk mitigation.

Potential consequences

The potential impact of compromised inverters or power electronics varies based on several factors:

- Local impacts: Compromise of a single inverter or site would most likely result in localized effects rather than systemwide disruption. The physical and electrical characteristics of individual installations limit the scope of impact.
- Larger impacts: Systemwide consequences from a single compromised device are unlikely due to existing protective relays, safety systems and the physical limitations of individual units.
- Coordinated scenarios: While coordinated manipulation across multiple sites could theoretically produce larger effects, executing such an attack would be technically challenging due to variability in equipment configurations, network architectures, site-specific protective systems and physical safeguards.

Broader context

It is important to note that cybersecurity vulnerabilities exist across the equipment supply chain and are not exclusive to any single manufacturer or country of origin. Recent vulnerability disclosures through the Common Vulnerabilities and Exposures process have identified security weaknesses in various inverter and power electronics products. Common issues include hard-coded vendor passwords; reliance on complex, open-source software components without adequate security review; and maintenance supply chain pathways that could introduce vulnerabilities after initial installation.

Addressing these risks requires a comprehensive approach that includes technical security controls, supply chain transparency, inspection capabilities and ongoing vulnerability management — regardless of equipment origin.

Q3. What short-term and long-term strategies should the U.S. government take to mitigate the threat created by having Chinese-manufactured inverters on the electric grid?

Answer: A comprehensive mitigation strategy requires coordinated action across multiple timeframes, addressing both the existing, installed base and future procurement decisions. The following recommendations draw from recent CESER analysis and align with established cybersecurity frameworks.

Short-term technical recommendations (existing installed base)
We can implement several immediate risk-reduction measures for equipment already deployed on the grid:

- **Strategic component replacement**: In locations where consequences of compromise would be most significant — such as substations serving critical facilities, large population centers or defense installations — prioritize replacement of high-risk control components with alternatives that offer greater supply chain transparency and security assurance.

- **Threat hunting and monitoring**: Deploy both commercial OT monitoring solutions and open-source network analysis tools to identify potential adversary activity or anomalous behavior in installed equipment. This includes leveraging tools specifically designed for ICS protocols and conducting periodic forensic analysis of selected units.

- **Network security controls**: Implement communications isolation, strategic network segmentation and data flow restrictions to limit potential impact from compromised devices. This includes restricting remote access capabilities, implementing strict firewall rules and monitoring all external communications from inverter systems.

Near-term recommendations (systems in design or procurement)
For projects currently in development or procurement, additional measures can address risks before deployment:

- **Contract and procurement reform**: Review and revise procurement agreements to ensure the right to conduct independent security inspections and test systems and components. Remove contractual clauses that prevent detailed technical analysis under the guise of intellectual property protection.

- **Cyber-Informed Engineering (CIE) adoption**: Integrate CIE principles into system design processes. This approach uses engineering controls and design decisions to eliminate or mitigate cyber-enabled attacks, focusing on preventing unacceptable physical consequences rather than solely addressing IT security concerns.

- **Software replacement and hardware repatriation**: Where technically feasible, replace foreign-developed software with secure-by-design alternatives developed domestically or by trusted partners. In some cases, it's possible to retain hardware components while replacing and hardening control software.

- **Independent security testing**: Require third-party cybersecurity and hardware assurance testing — like the methodologies used in programs like Cyber Testing for Resilient

Industrial Control Systems (CyTRICS) — for major equipment purchases. These include both software vulnerability analysis and hardware-level inspection.

Long-term policy and strategic recommendations
Achieving sustainable security improvements requires structural changes to the market and regulatory environment:

- **Universal equipment inspection standards**: Establish equipment inspection and vulnerability analysis as standard practice for all grid-connected equipment, regardless of country of origin or manufacturer. This levels the playing field and ensures consistent security baselines.

- **Domestic manufacturing incentives**: Develop targeted incentive programs to encourage U.S.-based manufacturing of power electronics and control technologies. These should prioritize not just assembly, but also design and production of critical hardware and firmware components. Incentives might include:
    - Tax credits for domestic manufacturing facilities
    - Accelerated permitting for power electronics factories
    - Long-term procurement commitments to provide market certainty
    - Research and development funding for secure-by-design innovations

- **Workforce development and training**: Invest in programs that develop the specialized expertise needed for both defending OT systems and designing secure energy infrastructure. This includes:
    - Specialized training programs for utilities and operators
    - Academic programs integrating OT cybersecurity into engineering curricula
    - Hands-on training facilities and fellowships
    - Professional certification programs for OT security specialists

- **Supply chain transparency requirements**: Implement requirements for comprehensive Software Bills of Materials (SBOMs) and Hardware Bills of Materials (HBOMs) for all major grid equipment, enabling operators to understand component origins and manage supply chain risk effectively.

Implementation considerations
These strategies should be implemented in a phased manner that balances security improvements with grid reliability and economic considerations. Removing all foreign-manufactured components in the near term could create reliability risks and slow the deployment of technologies needed for grid modernization. A strategic, prioritized approach that addresses the highest-consequence scenarios first, while building domestic manufacturing capacity in parallel, offers the most practical path forward.

Q4. What collaboration between the private and public sectors is needed to develop countermeasures to protect the U.S. grid against these vulnerabilities?

Answer: Protecting the nation's electric grid requires unprecedented public-private collaboration. This partnership is essential because approximately 85% of critical energy infrastructure is owned and operated by the private sector, yet government agencies possess unique threat intelligence and research capabilities that industry needs to mount an effective defense.

Enhanced information sharing and threat intelligence

Effective collaboration begins with robust information sharing. We must continue strengthening platforms like the Electricity Information Sharing and Analysis Center (E-ISAC) and similar, sector-specific ISACs that enable real-time threat intelligence sharing. We must also develop frameworks allowing properly cleared, private sector personnel to access sensitive and classified threat information needed to protect critical infrastructure.

Workforce development

A critical gap exists in cybersecurity professionals who understand OT and ICS. Unlike IT security, OT cybersecurity requires deep knowledge of physical processes, control systems engineering and potential physical consequences of cyber incidents. Public-private collaboration must address this gap through specialized training programs, hands-on learning environments, professional certifications and academic curriculum development. Organizations like Cyber Florida at USF, the Forge Institute and university partnerships with utilities provide successful models for building this talent pipeline.

Cyber-Informed Engineering

The long-term solution lies in fundamentally changing how we design critical infrastructure through CIE. Rather than bolting security onto existing systems, CIE uses design decisions and engineering controls to eliminate or mitigate cyber-enabled attacks from the outset. Following the National Defense Authorization Act for Fiscal Year 2020 mandate, the Securing Energy Infrastructure Executive Task Force — comprising senior leaders from DOE, the department of War and Homeland Security, energy companies, equipment vendors and standards organizations — developed a National CIE Strategy to guide this transformation across all 16 critical infrastructure sectors. CIE is now actively being implemented, but full-scale adoption will take additional time and resources.

High Assurance Industrial Systems

Achieving CIE's promise requires formal methods-based approaches through initiatives like High Assurance Industrial Systems (HAIS) and the Mathematically Formalized Assurance for National Security (MFANS) alliance. These efforts — coordinated across national laboratories, industry partners like Amazon and GE, and universities — develop tools that mathematically prove security properties rather than relying solely on testing. This represents collaboration among DOE, the White House Office of the National Cyber Director, the Defense Advanced Research Projects Agency and industry to establish provable security foundations for critical systems.

Interim protection

While advancing toward fully cyber-informed systems, proven methodologies protect current critical assets. Consequence-driven Cyber-Informed Engineering provides a systematic process for identifying critical functions, understanding attack vectors and implementing targeted mitigations. Major utilities have successfully applied this approach, and licensed partnerships with firms like Burns & McDonnell, Black & Veatch and West Yost are scaling deployment across the sector.

Similarly, the multi-laboratory CyTRICS program addresses supply chain risks through deep, component-level analysis in partnership with major equipment vendors including Schneider Electric, GE Vernova, Hitachi Energy and Schweitzer Engineering Laboratories. This collaboration enables both vendors and utilities to identify and mitigate systemic vulnerabilities before they're exploited.

Advanced analytics and coordination

Cross-sector collaboration through programs like the North American Energy Resilience Model — where national laboratories coordinate communications and modeling capabilities — provides utilities with sophisticated tools to understand infrastructure interdependencies and cascading consequences. The Cybersecurity Manufacturing Innovation Institute — a Manufacturing USA institute led by the University of Texas at San Antonio with participation from nine research institutions and over 60 industry members — demonstrates how public-private consortia can address supply chain security while supporting 50,000 small and medium manufacturers.

Research partnerships with organizations like the National Electric Energy Testing Research and Applications Center and the Electric Power Research Institute are accelerating validation and deployment of new technologies, including advanced transmission conductors and protective relay systems, ensuring innovations meet both operational and security requirements before widespread adoption.

The path forward

The Department of Energy's national laboratory system serves as a neutral convener and technical resource in this collaborative ecosystem. National laboratories are uniquely positioned to address these complex challenges because they operate at the intersection of fundamental research and applied deployment, maintain unique research facilities that industry cannot replicate, conduct long-horizon research beyond typical market timescales, and serve as trusted, noncompetitive partners to both government and industry.

Multi-laboratory and industry collaborations demonstrate coordinated approaches to grid security challenges. Through specialized training programs, world-class testing facilities including full-scale test beds, standards development and direct technical assistance, the national labs work with major utilities, equipment manufacturers, system integrators and government agencies to advance grid security. These sustained partnerships — spanning industry, academia, government

and international organizations — recognize that grid security is a shared responsibility requiring collaboration built on trust, transparency and aligned incentives across the entire energy sector.

Q5. What regulatory measures should be imposed to prevent the proliferation of embedded technologies in inverters to secure critical infrastructure, like the U.S. electric grid?

Answer: Effectively regulating power electronics and control systems requires a phased approach that balances immediate security improvements with practical supply chain realities and grid reliability needs.

Phase 1: Risk transparency and testing (Years 1-2)

Immediate prohibitions:

- Battery Management Systems, integrated Battery Energy Storage Systems and control software from foreign entities of concern (FEOC)
- Offshore communications and remote access systems that transmit U.S. grid data internationally

Transparency and inspection requirements:

- Mandatory SBOM and HBOM disclosures for all power conversion systems
- Required "right to inspect" clauses enabling independent cybersecurity and hardware assurance testing
- Pre-deployment security certification for federally funded or regulated projects

Infrastructure investment:

- Federal support for chip-level assurance capabilities, testing infrastructure and trusted-foundry programs

Application scope: These requirements would apply immediately to new federally funded or regulated projects, with continuity provisions for projects already in interconnection queues with contracted equipment.

Phase 2: Broad application and supply chain development (Years 3-5)

Expanded requirements:

- FEOC-free power conversion systems, battery management systems and software for all new interconnection applications once domestic and allied supply chains demonstrate adequate capacity
- Extension of prohibitions to all new builds and major retrofits while maintaining existing commercial commitments

Incentive programs:

- Accelerated permitting for domestic power electronics manufacturing facilities
- Long-term procurement contracts providing market certainty
- Tax incentives and R & D funding for FEOC-free supply chains
- Technical assistance for utilities transitioning to compliant equipment

Key implementation principles

Regulations should be:

- Risk-based, prioritizing highest-consequence applications first
- Technology-neutral, focusing on security outcomes rather than specific technologies
- Economically viable, with timelines aligned to realistic supply chain development
- Regularly reviewed to adapt to evolving technology and threats

Requirements should apply consistently based on transparent security criteria and coordinate across federal, state and international frameworks to avoid conflicting mandates.

This phased approach enables immediate risk reduction while providing clear timelines for industry to transition to more secure supply chains, balancing national security imperatives with grid reliability and economic growth requirements.

Q6. How might ongoing Trump administration efforts to onshore supply chains and promote domestic manufacturing in the energy sector protect the U.S. electric grid from national security risks?

Answer: Onshoring supply chains and promoting domestic manufacturing can enhance grid security through multiple pathways, extending beyond direct security improvements to encompass innovation, quality control and strategic independence.

Direct security benefits

Domestic manufacturing enables thorough oversight of design, development and production processes, allowing security requirements to be integrated from initial design stages rather than retrofitted later. Manufacturing within U.S. jurisdiction permits meaningful enforcement of security standards and consequences for noncompliance.

Shorter, more transparent supply chains with fewer international handoffs reduce opportunities for malicious tampering, counterfeit component insertion or firmware manipulation. Domestic production enables better provenance tracking and authentication of critical components. When design and manufacturing occur domestically, vulnerability disclosure, patch development and remediation can proceed more rapidly without international coordination challenges that sometimes delay security updates.

Addressing current vulnerabilities

Recent vulnerability disclosures in inverters and power electronics highlight persistent security challenges. Many current products contain hard-coded vendor passwords, insufficient authentication mechanisms and inadequately reviewed open-source software components. Domestic manufacturers operating under U.S. security requirements would be subject to more rigorous, secure development practices.

The software and hardware update processes for deployed equipment create ongoing vulnerability risks. Domestic control of the maintenance supply chain enables better verification

of updates and stronger supply chain security for replacement components. Current contractual provisions also sometimes prevent thorough security analysis under intellectual property protection claims. Domestic manufacturers operating under U.S. legal frameworks can be required to permit independent security testing and vulnerability analysis.

Innovation and strategic benefits
A robust domestic manufacturing base enables the United States to lead international standards development for power electronics security, ensuring global standards align with U.S. priorities. U.S.-based manufacturers can more readily incorporate cutting-edge security technologies developed through federal research programs, including formal verification methods, hardware-based security features, advanced authentication capabilities and secure boot processes.

Domestic manufacturing creates employment opportunities for engineers and security specialists with expertise in secure power electronics, building a knowledge base that enhances both manufacturing capabilities and operational security. This facilitates partnerships between manufacturers, universities and national laboratories to advance manufacturing technology and security innovation.

Supply chain resilience
Domestic manufacturing reduces vulnerability to international supply disruptions from geopolitical tensions, trade disputes or global crises, ensuring continuity of supply for grid modernization and maintenance needs. Manufacturing under consistent regulatory frameworks improves product quality and reliability while enabling more effective recall and replacement processes when issues are identified.

Implementation considerations
Realizing these benefits requires more than relocating manufacturing facilities. Effective onshoring efforts should include secure-by-design requirements in federal procurement programs, supply chain verification even for domestically manufactured equipment, competitive market development with multiple suppliers and coordination with allied nations where complete domestic sourcing is not feasible. Near-term strategies must manage risks in the existing installed base while domestic manufacturing capacity develops.

The Honorable Mariannette Miller-Meeks (R-IA)

Q1: You mentioned that CyTRICS conducts rigorous testing of hardware and software components in the energy supply chain. Given that you've identified China's embedding of hardware vulnerabilities as a major structural risk, how effective are these testing programs at detecting backdoors or vulnerabilities built into Chinese-manufactured equipment? And can these programs scale to address the volume of Chinese components currently in our infrastructure?

Answer: CyTRICS has a strong track record of identifying and mitigating vulnerabilities in energy infrastructure. However, not all components require the level of skill and effort that CyTRICS demonstrates. Most Chinese-sourced components in critical infrastructure are simple electrical parts that can be functionally verified and tested by manufacturers. CyTRICS analyzes

digital supply chains and identifies vulnerabilities and mitigations in energy infrastructure regardless of equipment country of origin.

Just as technology changes at a rapid pace, the methods and techniques used to evaluate that technology must also evolve and keep pace. CyTRICS is constantly improving the state of the art and the state of the practice for supply chain research. The national laboratories that participate in CyTRICS are constantly striving to scale the work that we perform through automation and integration of new technologies. CyTRICS also works with vendor and asset owner partners to share directly with industry the methods and lessons that empower private industry to join in defense against supply chain attacks.

The identification of vulnerabilities or backdoors is only a single part of a needed defense-in-depth strategy. This strategy includes programs like CIE, which are necessary to protect against vulnerabilities that either avoid detection or that emerge through usage of a system or changes to surrounding technology. Importantly, both CyTRICS and CIE are important to secure our energy infrastructure.