TESTIMONY OF Dr. Emma M. Stewart

Chief Power Grid Scientist, IDAHO NATIONAL LABORATORY

before the

UNITED STATES HOUSE OF REPRESENTATIVES
SELECT COMMITTEE ON THE CHINESE COMMUNIST PARTY

concerning

"*End the Typhoons: How to Deter Beijing's Cyber Actions and Enhance America's Lackluster Cyber Defenses*"

MARCH 5, 2025

Chairman Moolenaar, ranking member Krishnamoorthi, and members of the select committee, thank you for the opportunity to testify on a topic critical to our nation's security. My name is Emma Stewart, and I am the chief power grid scientist at the Idaho National Laboratory (INL), focused on securing the electric grid and the nation's energy delivery system. The work I perform at INL sits at the intersection of energy security, cybersecurity, and national resilience. Our critical infrastructure cybersecurity resilience, research, development, and deployment efforts enable asset owners and stakeholders to understand and to realistically mitigate the most consequential threats. While I hold the title scientist, I am an electrical engineer by education and trade and believe electricity is the fundamental source of stability and economic prosperity in the U.S. and globally.

INL, managed by Battelle Energy Alliance, is one of 17 U.S. Department of Energy (DOE) national laboratories. Located in Idaho Falls, Idaho, INL employs more than 6,300 researchers and support staff with a common vision: to change the world's energy future and secure our nation's critical infrastructure. INL's national security mission focuses on protecting the nation's critical infrastructure, preventing the proliferation of weapons of mass destruction, and providing direct support to America's warfighters. From our decades-long work in building and testing more than 50 nuclear reactors in the high desert west of Idaho Falls, INL has developed a deep understanding of operational technology and of the cybersecurity and engineering needed to secure systems and provide critical-function assurance. I have worked in this role at INL for nearly two years and have over two decades of experience in the field, working at national

laboratories and in industry as an engineer and leader in power systems, integration, resilience, and reliability. For most of my career, I have supported programs focused on civilian and defense national security priorities. I have developed and deployed innovative solutions to electric utility concerns, including developing cybersecurity and resilience programs for rural electric cooperatives.

Background

The backbone of our society is energy, with the United States having the largest, most complex, interconnected, and reliable electric grid in the world. Resilient, reliable power delivery, through the series of 3,000 electric utilities, cooperatives and municipal utilities, and 55,000 substations, transformers, poles, and wires,[1]—with world-leading "up time"—is the foundation of U.S. prosperity.[2] The capability and flexibility of electricity at any time and to any level as a foundation of our economy enables military missions, delivers clean water, provides medical resources, and supports innovation. My entire career has been in the pursuit of keeping the lights on.

The grid, as we know it, faces numerous threats to its continued reliability and needs to exponentially increase load-handling capabilities to serve artificial intelligence and Big Data; overcome the challenges of catastrophic weather events that cause significant, expensive, long-term damage; and get ahead of damaging cyberattacks from adversarial state actors.[3] We also must—in parallel—modernize and adapt grid technology to dominate in energy delivery on the global stage, using electronic and digital transformation to advance these goals and escalate consumer choice, growth, and economic prosperity while ensuring the U.S. power systems are secure from malicious intent.

---

[1] USDOE Office of Policy. "Achieving American Leadership in the Electric Grid Supply Chain Factsheet." , Jun. 2022

[2] NCSL. n.d. "As the Electric Grid Evolves, Reliability and Resilience Are Top Priorities", National Conference of State Legislators. Accessed Feb 28 2025, https://www.ncsl.org/state-legislatures-news/details/as-the-electric-grid-evolves-reliability-and-resilience-are-top-priorities

[3] NERC. N.d. "2024 Long-Term Reliability Assessment", North American Reliability Corporation. Accessed Feb 28 2025, https://www.nerc.com/pa/RAPA/ra/Pages/default.aspx

At this time, we face an unprecedented and multifaceted threat from Chinese Communist Party (CCP) actors,[4] given their ability and reported[5] attempts to deliver cyberattacks, which could catastrophically impact our way of life and disrupt our world-leading ability to deliver power to U.S. citizens and military assets. The growing threat to the critical functions of our infrastructure is demonstrated through reports on Volt Typhoon[6] and Salt Typhoon,[7]which describe capabilities ranging from pre-positioning access to our water, power, and gas in Volt and intrusion, mass data collection, and espionage on our critical communications infrastructure with Salt. Quoting the most recent Cisco Talos report into Salt Typhoon,[8] "there are several reasons to believe this activity is being carried out by a well-funded threat actor, including the targeted nature of the campaign…furthermore, the long timeline of this campaign suggests a high degree of coordination, planning and, patience". While these are often considered similar events, the pre-positioning of Volt Typhoon, in water and power, is a severe and clear indication of intent and capability towards our ability to delivery energy .

These actions are not just a bell weather, they are a clear and present danger to critical resources—one which we must enable asset owners to actionably defend against and excise from their systems. To keep the threat at bay, we must implement defensive controls, develop a deterrence portfolio and build barriers in all layers of our infrastructure, from supply chain, to contracts, to information technology and operational technology networking. Volt and Salt Typhoon could be referred to as intrusions through the

---

[4] FBI. n.d. "Chinese Government poses broad and unrelenting threat". Federal Bureau of Investigation, Accessed Feb 28 2025, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says

[5] Dragos. n.d. "2025 OT ICS Cybersecurity Report – a Year in Review, Accessed Feb 28 2025, https://www.dragos.com/resources/reports/2025-ot-ics-cybersecurity-report-a-year-in-review/

[6] DHS CISA, n.d. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure". Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Feb 7 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[7] DHS CISA, n.d. "Strengthening America's Resilience Against the PRC Cyber Threats". Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Jan 15 2025, https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

[8] Cisco, n.d. "Weathering the storm: In the midst of a Typhoon", Cisco Talos Threat Intelligence, Fev 20 2025, https://blog.talosintelligence.com/salt-typhoon-analysis/

back door of our country, leveraging known vulnerabilities and challenges in legacy equipment management and monitoring[9]. We must close those doors, remediate, and detect future evolutions of adversarial activity rapidly. We also must urgently address what could be referred to as a front door threat: the supply chain for the fundamental control layers, hardware, software, and power electronics on which our electric system relies.

Challenges and Recommendations 1: Supply Chains and Operational Technology

The electric grid on which we depend is not just poles, blades, steel, copper, and other hard goods. The control systems, which enable synchronized operation, load control, safety, switching, and generation dispatch, are a layer of devices and systemically integrated digital controls that rely on modernized power electronics, chips, communications systems, firmware, software, and programmable logic controllers. These technologies are highly digital devices with a complex control system and supply chain.[10][11]

A recent study sponsored by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) analyzed key manufacturers in the battery energy storage systems (BESS) space and evaluated the impact of the integration of high volumes of battery storage from People's Republic of China (PRC) manufacturers across the country.[12] Modern generation technologies, such as battery energy storage systems, provide services to the electric grid and unlock capacity from natural gas during high load days throughout major locations. The study identified a web of manufacturers, asset owners, operators, and

---

[9] Tenable, n,d, "salt Typhoon Analysis of Vulnerabilities Exploited by this State Sponsored Actor", Accessed Feb 28 2025, https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor

[10] EIA. n.d. "Battery Storage in the United States: An Update on Market Trends." U.S. Energy Information Administration. Accessed April 4, 2024.Accessed April 4, 2024. https://www.eia.gov/analysis/studies/electricity/batterystorage/.

[11] H. Krejsa, CMIST n.d. "SUN SHIELD: How Clean Tech and Americas Energy Expansion can Stop Chinese Cyber Threats", Carnegie Mellon Institute for Strategy and Technology, Jan 2025, https://www.cmu.edu/cmist/tech-and-policy/sun-shield/krejsa-jan2025.html

[12] USDOE. n.d. "Battery Energy Storage Systems" U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response . Jan 2025 . https://www.energy.gov/ceser/articles/new-ceser-report-offers-supply-chain-mitigation-strategies-battery-storage-systems

integrators that indicated the specific path from raw material to finished product was a significant job to untangle. This study also prioritized a portfolio of solutions and recommendations—which are available to implement today—that were developed commercially and by DOE CESER, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA), and the U.S. Department of Defense over the past eight years. These solutions and recommendations can protect, defend, and enable us to securely operate around and through compromise from malicious supply chain action. While this study and deployment of solutions focused initially on BESS, its process and recommendations can be applied across the electric grid technology space. There are over 23 GW[13] of BESS installed on our network, and inverters and power modules are also in homes and businesses connected to communications towers for backup generation. BESS are performing key grid services, including supporting the dispatch of natural gas generation, and are installed inside and beside data centers, providing power quality remediation and consistency.

PRC manufacturers dominate in production of power electronics, battery technology, control components, sensors, and devices, with at least 70% of manufacture being PRC based, and over 90% having at least one critical component from PRC. China has dominated this market through a systematic 20-year strategy to acquire intellectual property, grow the manufacturing base, and flood the market. Their market domination has risen to the point that the U.S. does not yet have a solution that could be considered completely U.S.-manufactured. Technologies that currently meet requirements for Buy America do so because of assembly performed in the U.S., but the creation of hardware and software—inherently, the source of technical risk, and therefore threat[14]—is non-domestic. While the study focused on BESS, the situation is comparable for most new and emerging energy technologies. This is also not a future threat; it

[13] EIA. n.d. “Today in Energy” U.S. Energy Information Administration. Accessed Feb 28 2025. https://www.eia.gov/todayinenergy/detail.php?id=61424

[14] Culler, Megan Jordan, et al. "Securing Solar for the Grid (S2G) Cybersecurity for Solar Systems Workshop at RE+: Fall 2024 IAB Meeting." , Oct. 2024, https://www.osti.gov/biblio/2473249

is fully present in our energy systems. This leaves the proverbial front door, previously mentioned, hanging wide open.

Though a lot of federal research has been focused on risks stemming from the non-U.S. battery cell material and its move to onshoring cell manufacturing, this study highlighted that technical risk from non-U.S. control system components to the electric grid and the generation asset far outweigh risks related to battery cell material. Furthermore, the U.S. reliance on foreign sources for critical materials and strategic minerals used in high-end electronics and control systems components underscores the urgent need for investment in domestic capabilities.

U.S. companies seeking to sell BESS in the U.S. have no domestic option for sourcing hardware and firmware, and this is not the only challenge. Chinese companies manufacturing BESS have contract and procurement power, and U.S. companies experience many prohibiting inspections of systems and security controls under the guise of intellectual property protection.[15]

The following is a sample of the recommendations from the DOE CESER-sponsored report.

Short Term Technical Recommendations for the current install base include the following:

- Strategic replacement of control components in high-consequence locations
- Hunt and threat identification in selected installed units, utilizing both commercial OT Monitoring and Forensics[16] and open source[17] tooling
- Communications isolation and security, data triage, and network segmentation

For the in-design or near-term solutions, recommendations are as follows:

- Inspection of contract and procurement negotiation to allow inspection of systems and security controls.

---

[15] Stewart, Emma Mary, et al. "Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance." , Oct. 2024. https://doi.org/10.2172/2473239

[16] Market Leading Examples include Dragos, Claroty, Nozomi https://www.gartner.com/reviews/market/cps-protection-platforms and Insane Cyber https://insanecyber.com/

[17] INL. n.d. “Malcolm: A Network Traffic Analysis Tool Suite.” Accessed April 4, 2024. https://inl.gov/national-security/ics-malcolm/.

- Removing harmful clauses which give Chinese companies control and protection from closer inspection
- Adoption of cyber-informed engineering (CIE)[18] design and development of engineering controls[19]
- Software replacement and repatriation of hardware, enabling secure-by-design software packages to replace insecure foreign developed types

Long-term policy solution recommendations include:

- Equipment inspection and vulnerability analysis as best practice for all equipment irrespective of sourcing
- U.S. manufacture incentives for power electronics and control technology, developing secure designs and dominating the U.S. market with our own innovative designs
- Training and workforce development, enabling new defenders and engineers to build a more secure future

An INL team, funded through both DOE CESER and the DOE Grid Deployment Office (GDO),[20] is already providing technical assistance activities to asset owners, hunting for adversary activity, guiding cyber-informed project design, and developing security controls, to remediate known issues in these supply chains. Working with U.S. integrators and businesses, they provide secure designs through CIE, hunt activities and threat reporting, and perform strategic site network monitoring. This program is ongoing and is extended to all digital controls such that asset owners and operators can rapidly, with continued resourcing, remediate and continue secure operation of these fleets. We cannot fix every problem, but in this case, we can remove the low hanging issues and make the nation's energy security more difficult to compromise or entities not as attractive of a target. This solution set has recently been extended to states and local entities to increase the protection provided to the U.S. grid. The team also worked with the largest U.S. BESS vendors to design around these threats while growing the U.S. supply

---

[18] INL. n.d. "Cyber-Informed Engineering." Idaho National Laboratory, Idaho Falls, ID. Accessed April 4, 2024. https://inl.gov/national-security/cie/.

[19] https://www.osti.gov/biblio/2522008

[20] DOE. n.d., "GRIP Technical Assistance for Securing Digital Energy", Department of Energy: Grid Deployment Office., Feb 2025, https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center

chain. These vendors are working with CIE tools[21] and the CIE process, requesting equipment inspection and operational technology monitoring solutions.

I believe through the continuation and coordination of the critical efforts in DOE CESER and GDO, we can mitigate many of the most consequential threats. This would include extension of technology programs, such as Cyber Testing for Resilient Industrial Control Systems (CyTRICS [22]), strategic ramp up of commercial OT analysis products, leveraging supply chain research and development to create next generation products for emerging technology [23]. Workforce engagement is a critical component to this solution set which is encouraged through programs like the OT Defender Fellowship[24], along with introduction of these kinds of scenarios during exercises such as GridEx and Liberty Eclipse[25]. With the continued support of federal funding INL, and their industry partners can enable grid operators and asset owners to defend against these scenarios if and when the time comes. Continuing and scaling this pilot of a coordinated defense and deployment strategy would provide consistent and more cohesive defense and deterrence across the sectors.

Challenge and Solution 2: Coordination of Deployment and Deterrence Activities

This PRC dominance and front door access to our most critical of controls must change for the prosperity of our U.S. energy sector and for improving our nation's defensive and deterrent posture. This leaves us with a critical conundrum of how to enable exponential growth and dominate the energy delivery market while countering the capabilities of CCP directed actors to disrupt and destroy. We in the national labs, industry, and the federal government have wide range of solutions. Solutions we believe—with rapid

---

[21] INL, "Cyber Informed Engineering Guide to Battery Energy Storage Systems", Idaho National Laboratory, Feb 2025, https://www.osti.gov/biblio/2522008

[22] DOE. n.d. "CyTRICS Cyber Testing for Resilient Industrial Control Systems." Department of Energy: Office of Cybersecurity, Energy Security, and Emergency Response." Accessed April 4, 2024. https://cytrics.inl.gov/

[23] DOE. n.d. "Energy Cyber Sense Program" Accessed Feb 2025. https://www.energy.gov/ceser/energy-cyber-sense-program

[24] DOE. n.d. "Operational Technology Defender Fellowship [Fact Sheet]." Accessed April 4, 2024. https://otdefender.inl.gov/.

[25] DOE. n.d. "Liberty Eclipse" Accessed Feb 2025, https://www.energy.gov/ceser/liberty-eclipse

application and strategic ramp up of engagement and assistance—can mitigate the most consequential impacts. We do not have a coordinated deployment strategy, and market forces do not enable effective portfolios to be built or customized. Our strategic defensive capabilities for the OT space are currently split into factions, such as national labs, private industry, and federal entities. There are significant and successful attempts to coordinate through programs such as DHS's Joint Cyber Defense Collaborative (JCDC) and the DOE Energy Threat Analysis Center (ETAC). Along with significant private partnerships to enable rapid remediation of Volt Typhoon (and similar) in small water and power such as UnDisruptable27 [26]. These efforts include a component of what level of strategic defense is needed, but none can implement and deter rapidly enough without unifying and coordinating the deployment, tooling, capabilities, and information flows. Information sharing often becomes the only solution, and it is not enough. Strategic unification of solution deployment would deter CCP from exploiting the weak points in our human defenses and provide the level of deterrence the civilian infrastructure on which our military defense and outward reaching actions also need to operate.

Coordination and unification of deployable resources, with a strategic lead and partnership in a single working group—with federal and state backing—along with streamlined authorities to perform remediation actions at the executive level will enable our defense to grow and effectively deter future attacks . Coordination through a singular CCP Defense task force for deployment assistance, tools and resources to excise and deter further engagement in the energy, water, and related sectors will streamline and unify efforts across existing entities. By engaging resources across the Electricity Information Sharing and Analysis Center (E-ISAC) [27], trade associations, national labs, volunteer and commercial organizations a more complete perspective on problem sets can be achieved with asset owner involvement. The OT civil defense cohort would have targeted and efficient deployment of resources, and a library of technical tooling – rapidly remediating known and unknown issues.

---

[26] https://securityandtechnology.org/undisruptable27/

[27] E-ISAC, Electricity Information Sharing and Analysis Center, https://www.eisac.com/s/

The elephant in the room: Rip and Replace

Rip and replace is often recommended as a first line of defense when Chinese components are found in critical locations,[28] [29]from a cybersecurity and national security perspective. In many cases, that is an effective solution for removing the dominance of particular vendors with malicious intent.

The removal of the Contemporary Amperex Technology Co., Limited, or CATL, battery from Camp Lejune in late 2024[30] made a clear statement that we as a country would not continue to enable this front door intrusion. CATL, though are one of approximately 70 different Chinese vendors of BESS product, and are both embedded and visible throughout the electric grid, with interwoven supply chain issues across the field [31]. Power electronics and controls, critical to their operation, are provided from a different vendor, who is one of the most common global Chinese power electronic makers [32]. There are hundreds of inverter and power electronics, with the top market share globally including Huawei, Sungrow, and GroWatt [33]. At present, removal of all these technologies would damage our resilience and reliability and detract from our ability to grow a U.S.-dominant supply chain. We have alternate and complimentary options and can take strategic steps to mitigate, but it requires collaboration and a partnership with federal, local, private, and public entities to get it done. We can replace the highest consequence and most critical sites; place strategic engineering mitigations for locations of less criticality; incentivize strategic

---

[28] "H.R.2670 - 118th Congress (2023-2024): National Defense Authorization Act for Fiscal Year 2024." *Congress.gov*, Library of Congress, 22 December 2023, https://www.congress.gov/bill/118th-congress/house-bill/2670.

[29] Reuters n.d., "US House to vote to provide $3 billion to remove Chinese telecoms equipment", Accessed Feb 2025, https://www.reuters.com/world/us/us-house-vote-provide-3-billion-remove-chinese-telecoms-equipment-2024-12-08/

[30] Reuters, "Duke Energy Disconnects CATL Batteries" https://www.reuters.com/world/us/duke-energy-disconnects-catl-batteries-marine-corps-base-camp-lejeune-2023-12-06/

[31] G. Weaver, M. Culler and E. M. Stewart, "Organizational Influence on Supply Chain for Digital Energy Infrastructure: Business Models, and Policy Landscape," *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, Washington, DC, USA, 2024, pp. 524-530, doi: 10.1109/TPS-ISA62245.2024.00071

[32] CATL n.d., "CATL Signs Strategic Cooperation Agreement with Sungrow", Accessed Feb 20 2025, https://www.catl.com/en/news/1018.html

[33] Bloomberg NEF, 1Q 2024, Global Market Outlook https://about.bnef.com/blog/1q-2024-global-pv-market-outlook/

repatriation of the technology in place through hardware, firmware, and software replacement and improvement; and invest to grow a successful U.S. and allied manufacture base, prioritizing secure and innovative component design in the next few years. This pathway can be completed, but it requires a focused, urgent, and prioritized strategy, outlined in the above Challenge Sets 1 & 2.

Summary

Our electric grid is the lifeblood of the U.S. economic and global leadership strategy. It is without a doubt facing some of the most prevalent threats to its stability that have been experienced in many of our lifetimes. We face external threats from CCP actors, who exploit weak points to establish dominance and persistence in our communications and control networks, as well as installed and supply chain threats, which leave the front door open to potential catastrophic events. This challenge is not without solutions, and with strategic and urgent application of a portfolio of capabilities, we can utilize U.S. technology and innovation and cybersecurity communities to effectively defend and operate through these challenges. INL and their partners in national labs and the federal government have and will continue to develop solutions, which could increase our ability to manufacture in the U.S, provide a strategic deterrent to attack, and enable the U.S. to demonstrate its strategic advantage in innovation and technology. We have world-leading capabilities in cybersecurity, engineering, and technology, along with national policy drivers, which can and will enable our continued domination in this field. However, we must apply these with the utmost urgency, collaborating across public-private boundaries, and with streamlined pathways to counter the rapidly increasing and present risk to our national security that CCP supply chain and threat actors pose.