NUVATION ENERGY

CROSSROADS OF CHANGE: Cybersecurity Across the Battery & Energy Ecosystem

Presented by Michael Worry, CEO & CTO, Nuvation Energy

Agenda

- **Intention: Offer the American and Canadian perspective on Cybersecurity in energy storage.**

- Speaker introduction
- Why does Cybersecurity matter?
- What is Cybersecurity?
  - Network Security
  - Supply Chain Security
- NAATBatt Cybersecurity Committee
- Stratification of Risk for Components
- Threat Matrix
- Government Laws and Perspectives Impacting Energy Storage
  - US State Level
  - US Federal Level
  - Canada
- Energy Storage Case Studies

Speaker Introduction

Michael Worry

- CEO, CTO Nuvation Energy
- Electrical Engineer, University of Waterloo, Canada
- Born and raised in Canada, now lives in the US
- Founded Nuvation in 1997
- Co-Chair NAATBatt Cybersecurity Committee
- Email: Michael.worry@nuvationenergy.com

Nuvation Energy - What We Do

Nuvation Energy designs and manufactures all our products in US and Canada.

Battery Management Systems

UL 1973 Recognized battery management systems for large-scale stationary energy storage.

Energy Management Solutions

Energy storage controllers for demand management, solar integration, power backup, and other applications.

Energy Storage Engineering Design Services

Design and integration services for ESS solutions, customer-specific BMS variants for new battery technologies.

Why Does Cybersecurity Matter in Energy Storage?

Potential Risks

- Lithium batteries can be dangerous if not properly managed and operated. Failure to do so could result in thermal runaway battery fires.
- The purpose of a Battery Management System (BMS) is to prevent lithium battery fires.
- The same way a BMS is a system to prevent battery fires, it could be manipulated by a bad actor to cause battery fires.
- Risks include:

A. Bad actor intentionally operating a system to cause fire and infrastructure damage.

B. Unauthorized control of assets connected to the grid causing grid instability and/or loss of power.

C. Shutdown by government organizations enforcing Cybersecurity laws.

Moss Landing Fire in Jan 2025

Image Source: https://www.latimes.com/california/story/2025-05-15/la-me-monterey-county-vistra-fire-lithium-battery-pge

What is Cybersecurity?

How Do We Ensure Grid Security?

Cybersecurity is the practice of protecting systems, networks, devices, and data from digital attacks, unauthorized access, or damage.

There are two parts:

Network Security

The conventional technologies, practices and policies put in place for protecting against remote bad actors and cyber attacks. This is typically things such as firewalls, user authentication, encryption, etc.

Example: Russia hacks into and shuts down Ukraine power station

Supply Chain Security

The methods to exclude a bad actor from the supply chain who could have motivation to tamper with or embed a backdoor that provides unwarranted access that bypasses Network Security. The bad actor could be the system provider or a subcomponent provider.

Example: Israel infiltrates Hezbollah supply chain

NAATBatt Cybersecurity Committee

Throughout 2025 we saw great momentum in government relations work to ensure our critical infrastructure is secure. With the help of the NAATBatt Cybersecurity Committee some highlights include:

Policy Engagement

- Ongoing education of elected officials
- Focus on foreign control risks in critical infrastructure

Regulatory Momentum

- States tightening restrictions on foreign adversary electronics
- Utilities increasingly requiring domestic or allied control systems – **both for design and manufacturing**

Cybersecurity Standards

- 62443 is the most common Cybersecurity standard for energy storage in US and Canada

FEOC & IRA Impacts

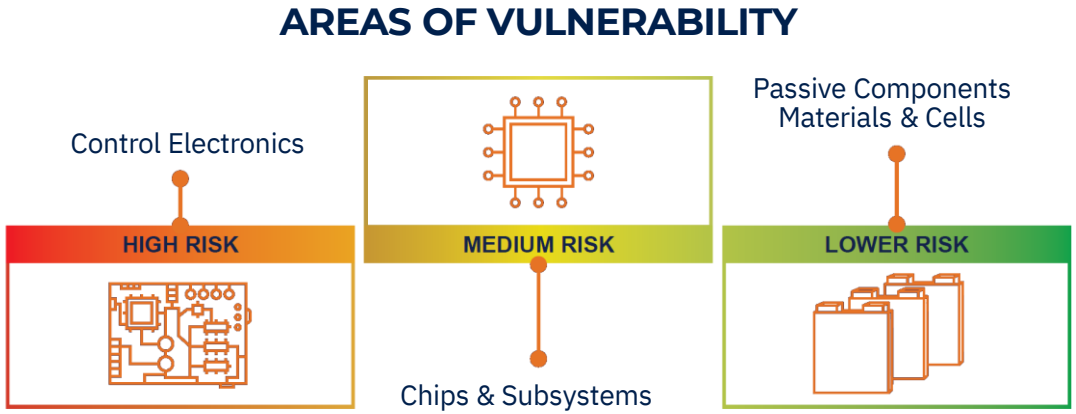
- Stricter FEOC requirements under OBBBA (One Big Beautiful Bill Act)
- Tax credits unavailable for projects with Chinese ownership, control, or material assistance
- Applies to IRA Sections 45X, 45Y, and 48E

Federal Attention

- U.S. Select Committee on the CCP continues to raise national security concerns
- Energy storage included in formal request for Commerce investigation

Stratification of Risk

- Not all parts carry equal risk. While it is established technologies to embed backdoors that go undetected in a circuit board, it is much more difficult to do the same in materials, passive components, and battery cells.
- Control electronics (both the hardware and software) are what carry the highest risk and should be the first targeted area to protect. This includes:
  - Battery Management Systems (BMS)
  - Power Conversion Systems (PCS)
  - Energy Management Systems (EMS)
  - Other control systems (fire, thermal management, etc.)
- Restricting the high-risk control electronics from FEOCs, while still allowing sourcing of lower risk components also maps to the production capabilities of North America.
- While today we still need to buy battery cells from China, we have the supply chain in North America to supply all our own control electronics locally.



Threat Matrix

- This matrix provides an assessment of the potential risk of a control electronic based on the origin of several factors
- **Design and company ownership hold the greatest weight when it comes to assessing the potential risk, particularly for the board design and software coding.**
- Chip design can also be important as these components form the main processing of the circuit board. Many US and allied chip companies exist.
- Manufacturing location, while still carrying some weight in risk assessment, is less important. **Foreign designed electronics are not made more safe by being manufactured in North America.**
- Understanding the supply chain of critical components important is important to also protect against white-labelling practices

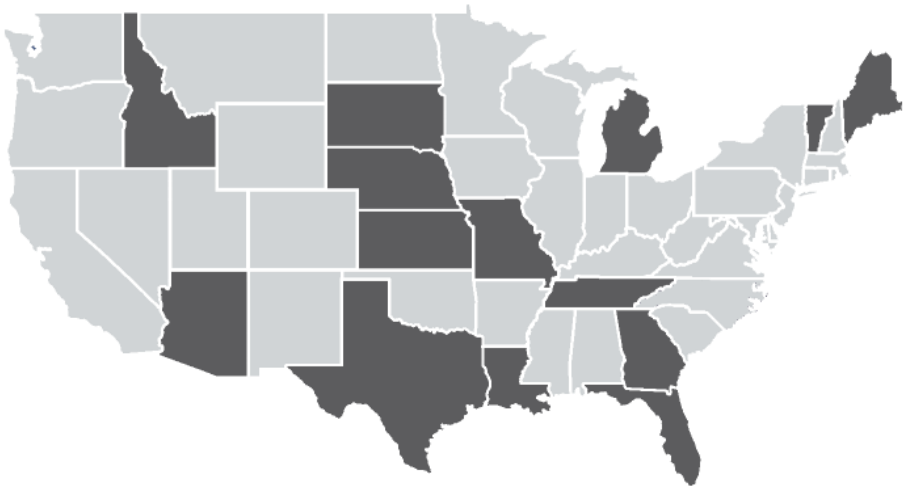
Higher Risk Factor → Lower Risk Factor

Control Electronic Company Ownership	HW and SW Design	Board Manufacturing	IC Company Ownership	IC Manufacturing	Overall Risk
China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
		US / Ally	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
	US / Ally	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
		US / Ally	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
US / Ally	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
		US / Ally	China / Foreign Adversary	China / Foreign Adversary	High Threat
				US / Ally	High Threat
			US / Ally	China / Foreign Adversary	High Threat
				US / Ally	High Threat
	US / Ally	China / Foreign Adversary	China / Foreign Adversary	China / Foreign Adversary	Medium Threat
				US / Ally	Medium Threat
			US / Ally	China / Foreign Adversary	Medium Threat
				US / Ally	Medium Threat
		US / Ally	China / Foreign Adversary	China / Foreign Adversary	Medium Threat
				US / Ally	Medium Threat
			US / Ally	China / Foreign Adversary	Low Threat
				US / Ally	Minimal Threat

White Labelled electronics are here. There is no reduction in threat by taking the same product and changing the logo.

U.S. States

- Several states have moved policy through legislative or executive action that have restricted or, at the very least, scrutinized relationships with companies from foreign adversaries.



TEXAS
Lone Star Infrastructure Protection Act (2021) safeguards critical infrastructure from foreign adversary influence.[1]

MICHIGAN
HB 4236 (2025) would prohibit state contracts with entities linked to China, Russia, Iran, and other adversarial nations.[3]

ARIZONA
HB 2696 (2025) would prohibit the use of equipment in critical infrastructure that is manufactured or controlled by companies headquartered in foreign adversaries.[5]

MISSOURI
HB 1231 (2025) would restrict companies and government entities from agreements that allow a foreign adversary to access or control critical infrastructure.[7]

NEBRASKA
Statue 73-903 (2024) revised to prohibit contracts for technology related products with companies controlled by the government of a foreign adversary.[9]

MAINE
Legislative Document 877 (2024) prohibits state contracts with companies owned or operated by the Chinese government.[11]

VERMONT
Cybersecurity Standard Update 2023-01 enforces NDAA Section 889 (2021) to prohibit all state government agencies from buying ICTS from firms owned, controlled, or connected to the Chinese government.[13]

FLORIDA
Executive Order 22-216 (2022) prohibits state and local government entities from buying or using information & communications technology produced, owned, or controlled by companies based in Foreign countries of concern.[2]

GEORGIA
SB 346 (2022) prohibits Chinese government-owned or -operated companies from bidding on or submitting proposals for state contracts. [4]

TENNESEE
Procurement Protection Act (HB 1841) prohibits foreign entities, including China, from submitting bids for state contracts and requires disclosures and certifications.[6]

LOUISIANA
SB 229 (2025) prohibits state agencies and political subdivisions from purchasing computer hardware from companies based in the People's Republic of China.[8]

SOUTH DAKOTA
SB 189 (2023) prohibits state agencies from contracting with companies owned or controlled by certain foreign governments deemed hostile to the US, including China.[10]

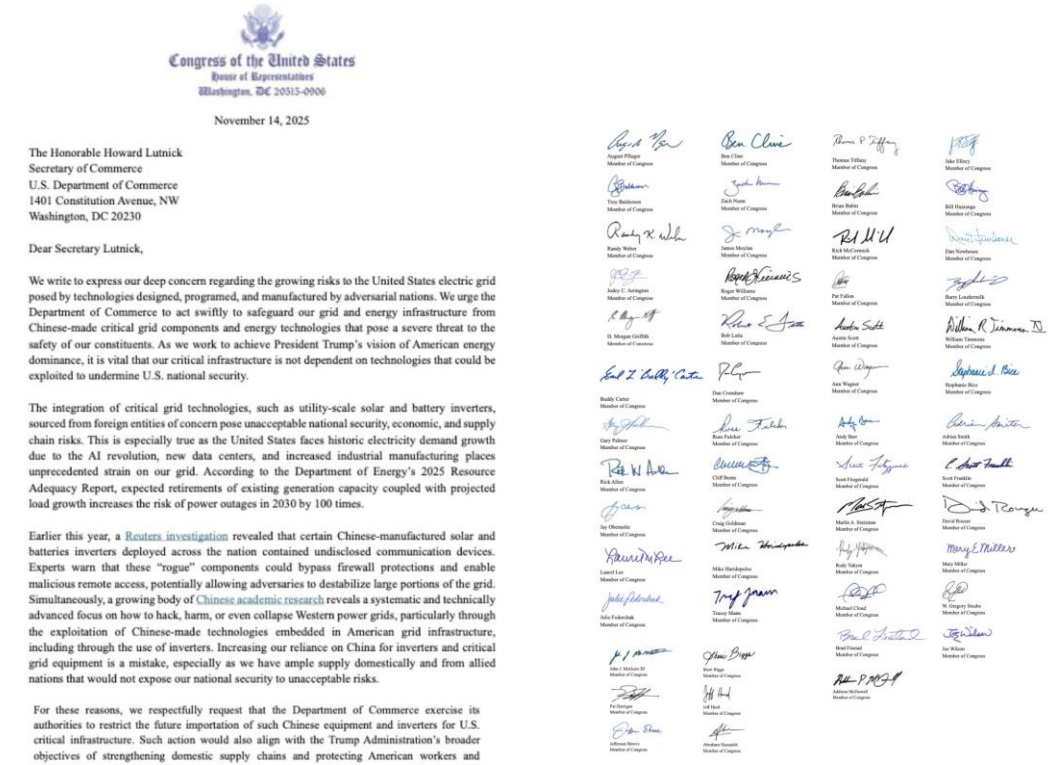
KANSAS
HB 2711 (2024) prohibits state investment in companies domiciled in countries of concern, including China.[12]

IDAHO
HB 294 (2023) prohibits public contracts with companies owned or operated by the government of China.[14]

U.S. Federal

- There is strong federal bipartisan alignment with house representatives to restrict FEOC control electronics from accessing critical infrastructure.
- Development of legislation and determining the appropriate representative to sponsor a corresponding bill are actively being worked on.
- 55 Republicans warn Commerce Secretary Howard Lutnick that Chinese-manufactured solar panels and battery inverters deployed across America threaten public safety, economic security, and national defense.

“The integration of critical grid technologies, such as utility-scale solar and battery inverters, sourced from foreign entities of concern pose unacceptable national security, economic, and supply chain risks.” There is also a reference to Chinese academic research on how to "hack, harm, or even collapse Western power grids, particularly through the exploitation of Chinese-made technologies embedded in American grid infrastructure." The letter concludes, "For these reasons, we respectfully request that the Department of Commerce exercise its authorities to restrict the future importation of such Chinese equipment and inverters for U.S. critical infrastructure.”



Congress of the United States
House of Representatives
Washington, DC 20515-0906

November 14, 2025

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Dear Secretary Lutnick,

We write to express our deep concern regarding the growing risks to the United States electric grid posed by technologies designed, programed, and manufactured by adversarial nations. We urge the Department of Commerce to act swiftly to safeguard our grid and energy infrastructure from Chinese-made critical grid components and energy technologies that pose a severe threat to the safety of our constituents. As we work to achieve President Trump's vision of American energy dominance, it is vital that our critical infrastructure is not dependent on technologies that could be exploited to undermine U.S. national security.

The integration of critical grid technologies, such as utility-scale solar and battery inverters, sourced from foreign entities of concern pose unacceptable national security, economic, and supply chain risks. This is especially true as the United States faces historic electricity demand growth due to the AI revolution, new data centers, and increased industrial manufacturing places unprecedented strain on our grid. According to the Department of Energy's 2025 Resource Adequacy Report, expected retirements of existing generation capacity coupled with projected load growth increases the risk of power outages in 2030 by 100 times.

Earlier this year, a Reuters investigation revealed that certain Chinese-manufactured solar and batteries inverters deployed across the nation contained undisclosed communication devices. Experts warn that these “rogue” components could bypass firewall protections and enable malicious remote access, potentially allowing adversaries to destabilize large portions of the grid. Simultaneously, a growing body of Chinese academic research reveals a systematic and technically advanced focus on how to hack, harm, or even collapse Western power grids, particularly through the exploitation of Chinese-made technologies embedded in American grid infrastructure, including through the use of inverters. Increasing our reliance on China for inverters and critical grid equipment is a mistake, especially as we have ample supply domestically and from allied nations that would not expose our national security to unacceptable risks.

For these reasons, we respectfully request that the Department of Commerce exercise its authorities to restrict the future importation of such Chinese equipment and inverters for U.S. critical infrastructure. Such action would also align with the Trump Administration's broader objectives of strengthening domestic supply chains and protecting American workers and consumers. We appreciate your attention to this matter, and we stand ready to work with you and your team to ensure the security and resilience of our grid.

Respectfully,

Canada

Canada has strong alignment with the U.S. regarding security concerns with foreign adversaries.

In Ontario:

- Ontario encompasses the majority of BESS installations within Canada.
- It is also leading the way in Canada for protecting the electrical grid from foreign interference through several enacted bills in 2025:
  - Bill-5: Protect Ontario by Unleashing our Economy Act, 2025
  - Bill-40: Protect Ontario by Securing Affordable Energy for Generations Act, 2025
  - Bill-72: Buy Ontario Act, 2025

Energy Storage Cybersecurity Case Studies

- **Attorney General Ken Paxton Launches Investigation into Use of CCP-Aligned Tech Products in Critical State Infrastructure**
- Date: November 24, 2025
- Report: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigation-use-ccp-aligned-tech-products-critical-state
- Summary: Lone Star Infrastructure Protection Act prohibits business entities from entering into agreements that would grant a Chinese-controlled business direct or remote access to critical Texas infrastructure. However, a power storage station currently under construction near Mabank, Texas, has used CATL components for critical pieces that have also failed to pass certain tests. Attorney General Paxton has opened an investigation to determine if the use of CCP-aligned CATL products violates Texas law by enabling access to critical infrastructure by prohibited actors, posing a substantial risk to Texas's power grid.

"Texas must not allow foreign communists to infiltrate, interfere, or otherwise undermine our power grid or other parts of our state infrastructure," said Attorney General Paxton. "The CCP is a bad actor, and it is unlawful for aligned companies to meddle in our state in order to grant backdoor access to their handlers. If you mess with Texas, I will come after you."

Energy Storage Cybersecurity Case Studies

- **Duke Energy to remove Chinese battery giant CATL from Marine Corps Base**
- Date: February 9 2024
- Report: https://www.reuters.com/business/energy/duke-energy-remove-chinese-battery-giant-catl-marine-corps-base-2024-02-09/
- Summary: U.S. utility Duke Energy has decided to decommission and remove energy-storage batteries made by Chinese company CATL from a large Marine Corps base at Camp Lejeune, North Carolina. The move follows pressure from the U.S. Congress and national security concerns. Lawmakers have warned that batteries made by CATL—whose leadership has ties to China's ruling Communist Party—could present cybersecurity risks to critical infrastructure like the power grid.

"The decision, which has not been previously reported, comes as top U.S. officials warn that hackers linked to the Chinese government are targeting network-linked critical U.S. infrastructure, including the power grid."

Even if a system is installed compliant with existing laws, if it incorporates foreign adversary components, the US government may deem it a national security risk and shut it down.

How are Policies Implemented?

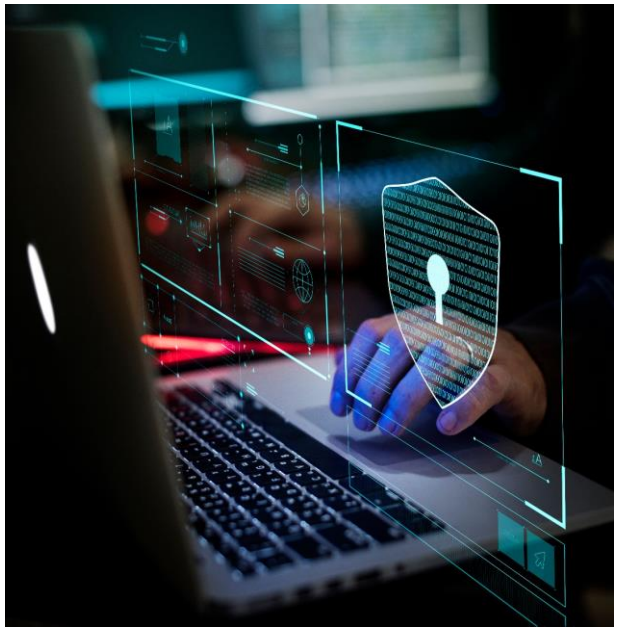
- The NAATBatt Cybersecurity Committee has developed a Hierarchy of Influence for how policy adherence is practically achieved through the various parties involved in energy storage.

Hierarchy of Influence

Government (NERC, DOE, DOD, Federal, State, Provincial)	Sets laws to guide industry
Utilities, IPPs, Facility Owners (Data Centers)	Writes RFPs to meeting their interests. Compliance with laws is expected but not always enforced
Developers & EPCs	Orders ESS based on the RFP requirements
System Integrators & Battery Manufacturers	Design ESS that meets RFP requirements

Key Takeaways

1) Cybersecurity is comprised of network security and supply chain security. Both are required to keep our grid safe.
2) Where something is designed is more important for cybersecurity than where it happens to be manufactured.
3) It is essential to ensure that control electronics used are compliant with applicable laws, regulations, and RFP requirements. Failure to follow Cybersecurity best practices may result in significant financial and operational consequences.
4) For the North American market, choose domestic North American control electronics with pedigree of field deployments, strong cybersecurity compliance, and that are both designed and manufactured in North America.



NUVATION® ENERGY

INFO@NUVATIONENERGY.COM

NUVATIONENERGY.COM

855-261-0507