Inverter & Supply Chain Cybersecurity

Policymakers should continue to **incentivize domestic manufacturing of inverters.** We must build on existing standards and best practices for protecting power systems to develop and ensure compliance with **unified cybersecurity requirements** that secure evolving energy systems and close security gaps.

Cyberattacks against critical infrastructure and the energy sector[1] are on the rise.[2] While cyberattacks on the solar and storage industry have not been nearly as frequent or severe as other areas of the energy sector or other critical infrastructure, as solar and storage continue to grow, cybersecurity protections become increasingly important to grid reliability and resilience.

The Solar Energy Industries Association (SEIA) is working proactively with industry and government partners to ensure that solar and storage energy systems and components are secure by design[3], and that risks can be mitigated and managed. The security and resilience of our supply chains and critical cyber assets like inverters is inextricably linked to national security.

Inverters are integral digital components in solar and storage energy delivery. They play a critical role in power conversion, grid support functions, monitoring, and communications to the grid. Because of these important functions, inverters are also critical cyber assets that must be prioritized in both policy and technical solutions. According to Idaho National Laboratory's component criticality scoring criteria, **power conversion systems (PCS) and inverters are among the most critical digital components** that should be prioritized for short-term and long-term security controls and policy solutions.[4]

Supply Chain & Cyber Risks

A critical part of fortifying inverter technology is **ensuring the security and resilience of its supply chain.** While global sourcing in the energy sector has enabled cost-savings and technological advancements, an overreliance on foreign sources could introduce new cybersecurity risks. Addressing supply chain and other cybersecurity risks from global sources requires a multipronged approach. This includes security controls that strengthen transparency including software and hardware bill of materials, rights to inspection of products, detailed documentation, and procurement security requirements. This also includes adherence to cybersecurity standards, as well as best practices, principles, and policies that promote growing the domestic supply chain.

Another key element of inverter cybersecurity is **implementing technical and organizational controls to protect digital components.** Inverters rely on software and firmware that can be remotely accessed and managed to improve efficiency, automate maintenance, monitor device health, vulnerability and patch management, and more. However, remote access must be properly managed to mitigate potential cyberattacks. Well-implemented organizational and technical controls can and do provide the necessary guardrails to reduce exposure to cyber threats for solar and storage systems.

POLICY RECOMMENDATION

Given the important role inverters play in the cybersecurity of solar and storage systems, policymakers should **prioritize and incentivize industry towards increasing the domestic manufacturing of inverters,** building on past domestic content policy incentives. In fact, the solar and storage industry has made significant investments in recent years in the domestic production of inverters and other critical components of the supply chain.

According to SEIA's Solar and Storage Supply Chain Dashboard, U.S. manufacturing for inverters has grown by nearly 50% since the end of 2024.[3] However, significant industry uncertainty stemming from certain U.S. government policies, regulations, and trade actions has the potential to slow that progress. Future policy should directly incentivize domestic manufacturing of inverters to address cybersecurity and national security risks and support continued growth in the industry.

Unified Cybersecurity Requirements

SEIA is proactively engaged in educating the industry about cybersecurity, developing best practices[6], implementing existing standards and guidelines to mitigate and manage supply chain risks, and implementing strong cybersecurity for inverters, including those below. In addition, significant changes are underway to incorporate more inverter-based resources under NERC mandatory cybersecurity standards.[7]

POLICY RECOMMENDATION

Notwithstanding the advances illustrated by this set of standards, the United States still lacks a common framework for cybersecurity protections that cover all solar and energy storage systems. Policymakers should draw upon existing standards and best practices like the DOE/NARUC Cybersecurity Baselines for Electric Distribution Systems and DER[8] and IEEE 1547.3 guide for distributed energy resources interconnected to electric power systems[9] to **develop unified cybersecurity requirements** that secure evolving energy systems and close security gaps.

Existing Standards & Best Practices for Supply Chain & Inverter Cybersecurity

DOE Procurement, Contracting, & Supply Chain Risk Management Guidance	Provides guidance to embed cybersecurity and supply chain risk management into contracting and vendor selection including contract terms for transparent communications pathways and secure remote access methods.
DOE Supply Chain Cybersecurity Principles	Offers practical approaches to deliver strong cybersecurity throughout energy sector supply chains. Many industry partners have already expressed support for the principles which include important cybersecurity concepts and objectives for the energy supply chain.
ISA/IEC 62443	A series of cybersecurity standards for industrial and automation control systems which includes the supply chain, organizational-, systems-, and device-level controls that can be used to build a holistic, end-to-end cybersecurity program.
UL2941	A cybersecurity certification standard offering device-level, testable requirements for distributed energy resources and inverter base resources.
NIST IR 8498	Offers guidelines on cybersecurity for smart inverters specifically for residential and light commercial solar energy systems.
IEEE 1547.3	A cybersecurity guide for distributed energy resources interconnected to electric power systems, including resources like solar and energy storage systems.
NARUC/DOE Cybersecurity Baselines for Electric Distribution Systems & DER	Offers foundational cybersecurity practices to mitigate DER cyber risk and enhance grid security.

[1] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
[2] https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report--cyber-security-report-2025
[3] https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf
[4] https://csdet.inl.gov/content/uploads/45/2025/03/BESS_OnePager_ConsequenceAnalysis_12202024.pdf
[5] https://seia.org/research-resources/solar-storage-supply-chain-dashboard/
[6] https://seia.org/wp-content/uploads/2024/08/Recommendations-for-Solar-Energy-Cybersecurity-SAND2023-04512O.pdf
[7] https://www.nerc.com/globalassets/who-we-are/news/2024/nerc-e-isac-and-ibr-registration-101.pdf
[8] https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/
[9] https://ieeexplore.ieee.org/document/10352402