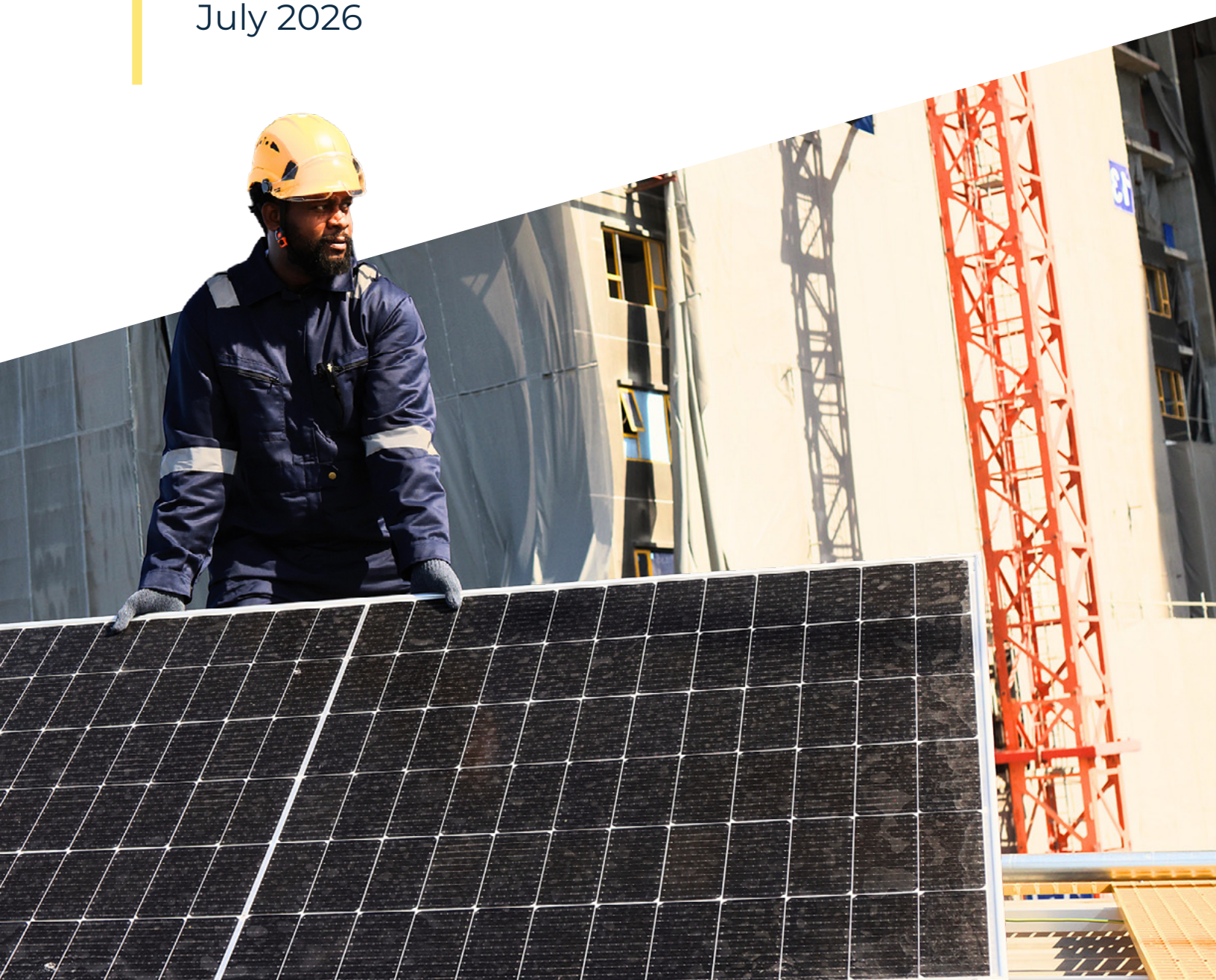
SEIA Solar Energy Industries Association®

Cybersecurity Priorities for America's Solar & Storage Industry

July 2026



Introduction

As electricity demand grows and costs rise, solar and energy storage are essential to building a reliable, secure, and affordable energy system. These technologies already make up the majority of new generation capacity additions in the United States. Combined, solar and storage accounted for nearly 80% of new capacity added to the grid in 2025.[1] The solar and storage industry plays a critical role in ensuring U.S. energy security and serves an increasingly important role in meeting rising demand. At the same time, cybersecurity threats facing the broader energy sector continue to evolve and grow. It is imperative that the systems, networks, devices, and components that make up the solar and storage ecosystem are secure against cybersecurity threats.

For this reason, the Solar Energy Industries Association (SEIA) is working with industry and government partners to advance cybersecurity practices that secure American solar and storage.

To support our vision for safe, secure, and reliable energy systems, SEIA has outlined the following **key priorities** for strengthening the cybersecurity of the solar and storage industry:

Support supply chain security for solar and storage

Enhance visibility, awareness, and risk reduction

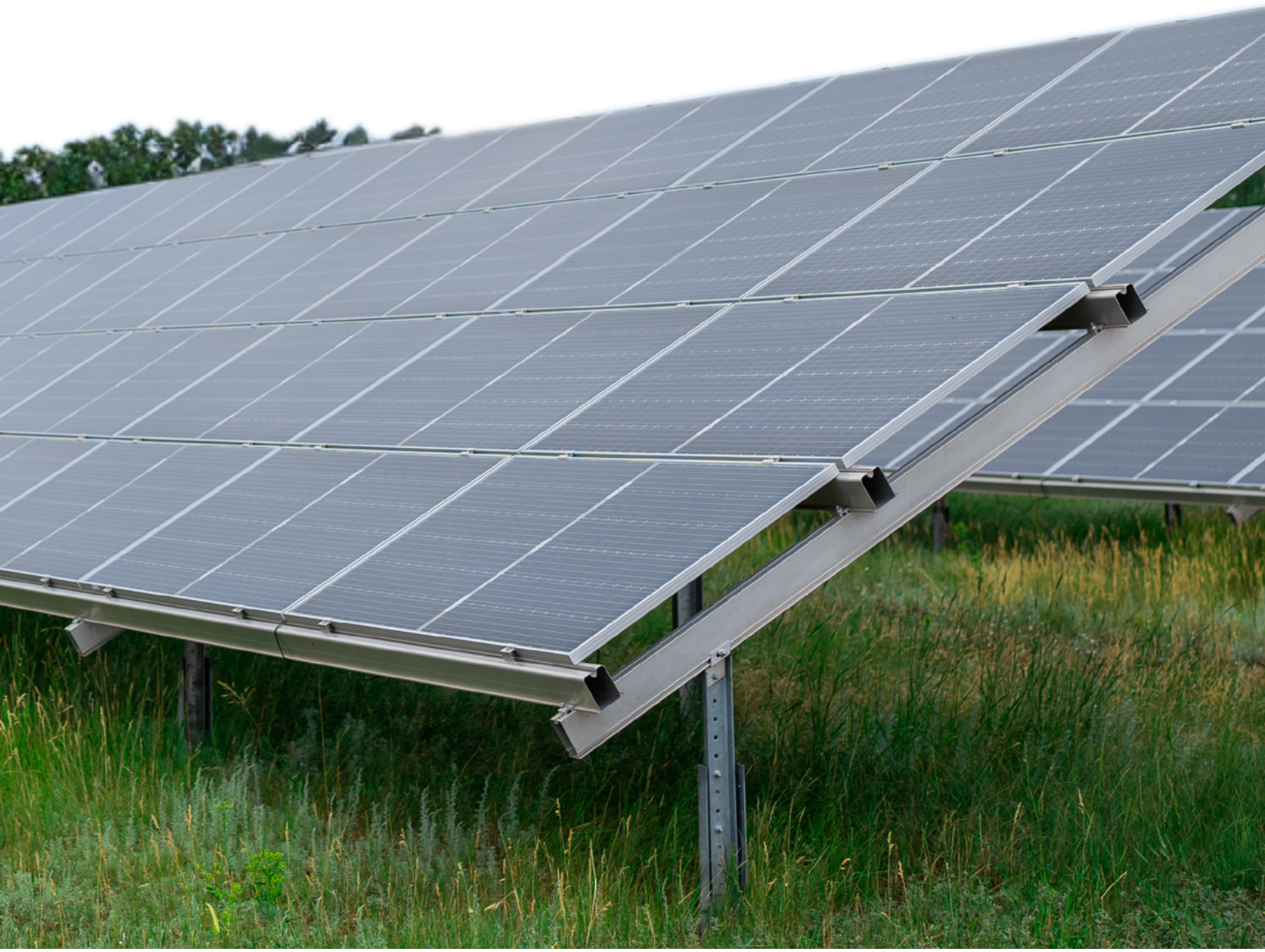
Strengthen baseline cybersecurity practices

With support from policymakers, regulators, and industry, these focus areas can help make solar and storage some of the most secure assets on the grid.

Solar and Storage Are Essential to Energy Security

Amid rising energy costs[2], growing demand from data centers, AI, and increasing energy needs from the electrification of transportation and heating loads, the United States needs every available electron on the grid to meet the moment.

Solar and storage continue to prove themselves as strategic assets for securing America's energy future. Ensuring these critical assets are secure against cybersecurity threats and that they continue to provide reliable, affordable energy is a top priority for the industry.



Cybersecurity Threats to the Energy Sector

From nation-state advanced persistent threat groups motivated by espionage or prepositioning for future disruptions, to ransomware gangs seeking financial gain, hacktivists advancing ideological agendas, and insider threats, attackers continue to target critical infrastructure, including the energy sector.[3] The security of the energy sector is uniquely critical to national security, as energy powers all other critical infrastructure including healthcare, transportation, water, telecommunications, and defense sectors.[4]

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. However, as solar and storage continue to grow, cybersecurity protections become increasingly important to support grid reliability and resilience. SEIA is supporting the industry to proactively implement strong cybersecurity defenses as their importance on the grid increases.

Select History of Attacks in the Energy Sector

Cyber incidents affecting solar and storage continue to constitute a very small proportion of attacks against the energy sector. It is important for the industry to understand and defend against common tactics, techniques, and procedures used by cyber adversaries against the energy sector, including conventional grid infrastructure. This summary is intended to illustrate cyber threats to energy systems generally, not because solar and storage were the main targets of these incidents.

Past attacks in the energy sector reinforce the importance of maintaining a strong cybersecurity program and implementing foundational cybersecurity controls like using multifactor authentication wherever possible, eliminating default and shared credentials, managing vulnerabilities, securing remote access pathways, segmenting networks, applying intrusion detection and response, and exercising incident response plans.

2019

Attack on U.S. Independent Power Producer, SPower

In 2019, independent power producer, SPower, lost visibility to field equipment and generation sites after an attacker exploited a known vulnerability in a firewall, causing it to repeatedly forcibly reboot. While this was the first known cyber event against energy infrastructure in the United States, the attack had no effect on generation.

2021

Attack on Colonial Pipeline

In 2021, oil pipeline operator, Colonial Pipeline, was the victim of the largest cyberattack against U.S. oil infrastructure in history. Attackers used a compromised VPN password to access the company's IT systems and held 100 gigabytes of data for ransom. In response, Colonial Pipeline preemptively shutdown thousands of miles of its pipeline to contain the attack, causing widespread fuel disruptions along the East Coast and prompting President Biden to declare a state of emergency. The attack resulted in significant financial losses, reputational damage, and legal consequences for the organization.

2015, 2016, 2022

Attacks on Ukrainian Energy Infrastructure

Ukrainian energy infrastructure has been the target of several of the most disruptive and destructive cyberattacks in history. In December 2015, attackers attributed to Russian advanced persistent threat group, Sandworm, launched a coordinated attack against three distribution networks, becoming the first cyberattack to cause a power outage, with over 230,000 customers losing power.[5]

Then in December 2016, the same adversary targeted a transmission substation, cutting power to one-fifth of Kyiv for an hour in the dead of winter. This attack was considered to be a large-scale test for refining attacks on critical infrastructure.[6] In October 2022, Ukrainian energy infrastructure was again targeted by Sandworm with a disruptive cyberattack that switched off substations and deployed a wiper malware within the IT environment. The event coincided with missile strikes on critical infrastructure on multiple Ukrainian cities.[7]

2022–2023

Attacks on German Wind Operations

Three separate attacks affected wind operations in Germany between 2022 and 2023. In 2022, Germany wind operator, Enercon, was collateral damage to a Russian attack originally targeting satellite infrastructure in Ukraine, disrupting satellite communications used for remote monitoring and control of wind sites and causing two months of operational disruption. The second event was a ransomware attack against the IT infrastructure of wind turbine manufacturer, Nordex. Then in 2023, a third-party service provider, Deutsche Windtechnik, was attacked, leading to a loss of remote data monitoring capabilities to roughly 2,000 turbines.

2025

Attack on Polish Distributed Energy Resources

In December 2025, Poland successfully thwarted what officials have described as the largest cyberattack on its energy infrastructure in years.[8] The attack targeted combined heat and power plants as well as the management systems of several wind and solar sites.[9] While the attack led to the destruction of some field devices, effective defenses ensured there were no impacts to generation.

Key Cybersecurity Considerations in the Solar and Storage Industry

As solar and storage resources continue to grow and serve an increasingly important part of the electricity generation mix, their influence on grid security and reliability also grows. That is why SEIA is committed to supporting its members to proactively defend against threats and address key cybersecurity considerations in the solar and storage industry at every scale of deployment. Page 10 describes the activities SEIA has undertaken to support members in understanding, managing, and mitigating these challenges.

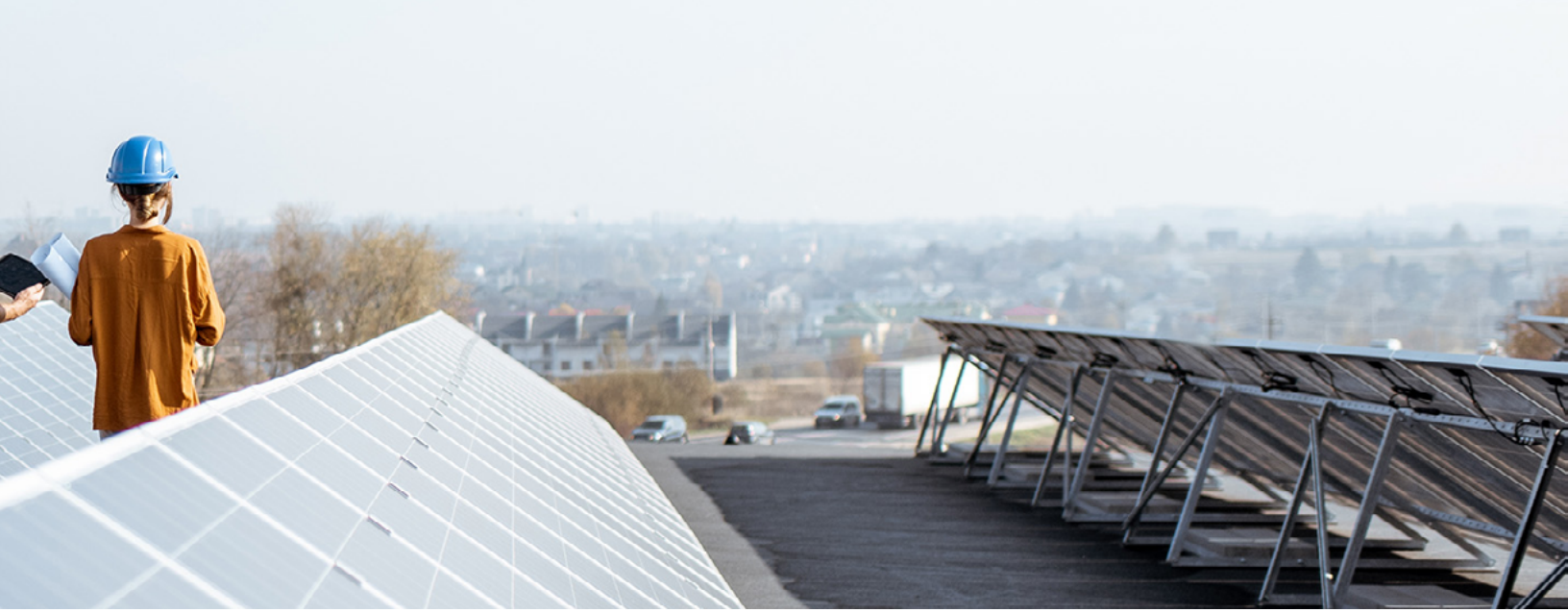
Utility-Scale & Distributed Systems

Utility-scale solar installations are large facilities that sell electricity to wholesale utility buyers, rather than to end-consumers. Projects continue to grow in size with an average project size of 120 MW in 2024.[10] Many modern utility-scale solar plants also include large-scale battery systems to dispatch energy at night or during peak demand. Large-scale installations with a nameplate capacity of greater than or equal to 75 MW interconnected at voltages greater than or equal to 100kV must comply with several mandatory cybersecurity requirements from the North American Electric Reliability Corporation (NERC) called Critical Infrastructure Protections (NERC CIP). While NERC CIP requirements provide an important foundation for securing the Bulk Electric System (BES), they represent minimum compliance requirements that are further strengthened with a proactive, defense-in-depth strategy.

Distributed generation and distributed storage are assets connected to the distribution grid that serve commercial, industrial, and residential customers at or near the point of consumption. Unlike utility-scale installations, smaller-scale solar and storage systems fall outside of NERC-CIP jurisdiction, leading to inconsistent baseline protections across the ecosystem. Further, the aggregation of many distributed assets can introduce cybersecurity challenges. Innovations like virtual power plants, which aggregate large groups of distributed energy resources (DERs) like solar and storage through a centralized management and control platform, require additional cybersecurity considerations. Additionally, unlike most utility-scale installations, many distributed systems rely on connections to the internet to connect to the grid and for monitoring and control functions. Internet-connected devices have been and continue to be attractive targets for attackers. Further, these systems are typically customer- or third party-owned, potentially with limited cybersecurity knowledge or resources.

Remote Access

Many solar and storage assets rely on remote communications and management to support monitoring, maintenance and operational control to optimize performance and improve efficiency. These remote access pathways must be properly protected and managed to mitigate unauthorized access.



Shared Responsibility

Solar and storage installations may be utility-owned, developer-owned, or customer-owned, with many parties that share responsibility for cybersecurity. Asset owners, operators, engineering, procurement, and construction companies, vendors, and other third parties all interact with the system in different ways, whether deploying the operational technology (OT) system, maintaining remote access, or holding compliance obligations. It can be difficult for these stakeholders to clearly define shared responsibilities for cybersecurity and even more challenging to navigate and operationalize each entity's role in the event of a cyber incident.

Artificial Intelligence

Emerging technologies, including the deployment of advanced artificial intelligence models to optimize energy assets, create new cybersecurity risks and expand the attack surface. AI deployment, if compromised, can create impacts ranging from loss of operational efficiency, mistakes from AI decision support tools, and the potential for misoperations or failure of grid components. Further, while defenders are rapidly adopting AI to increase visibility and identify and remediate threats, AI can also lower the bar for bad actors to target OT environments and increase the speed at which vulnerabilities are exploited.

Supply Chain Risks

Supply chain interdependencies with vendors and third parties, including fleet management platforms, cloud providers, managed service providers, and telecommunications providers, introduces cybersecurity risks, necessitating robust third-party risk management processes.

Policy & Organizational Challenges

Policy volatility not only creates reliability risks[11] and threatens industry growth, it also complicates cybersecurity planning. Unpredictable federal policy and regulations make it difficult for organizations to anticipate future requirements, align procurement decisions, and invest in security measures consistent with policy priorities.

Lastly, many organizations face internal challenges embedding cybersecurity into engineering, operations, and maintenance functions. Ensuring these various teams are aligned on cybersecurity objectives and operationalize security protections can be difficult, as it requires a significant shift in how OT systems were traditionally engineered, operated, and maintained.

While every part of the energy sector faces cybersecurity challenges, the solar and storage industry increasingly provides reliability services to the grid. Proactively addressing cybersecurity challenges in the industry is essential to supporting its continued growth.

Current State of Energy Sector Cybersecurity Policy in the U.S.

SEIA is dedicated to advancing pragmatic cybersecurity policies and approaches that are threat-informed, consequence-driven, and grounded in established standards and best practices that improve the baseline cybersecurity protections for solar and storage installations, regardless of size.

The state of cybersecurity policy for the solar and storage industry looks different depending on the scale of deployment. As of 2026, mandatory NERC CIP cybersecurity requirements are limited to facilities that meet the threshold of 75 MVA connected at voltages above 100 kV to be considered part of the bulk power system.

NERC CIP reliability standards traditionally only covered large, centralized power generation facilities. However, grid transformation, largely spurred by growth of solar and other renewables, has reshaped NERC reliability standards in recent years. This includes a new threshold for compliance, new criteria for evaluating the impact levels of inverter-based resources, and new standards.

NERC's IBR Registration initiative will require additional IBRs to register with NERC and conform with NERC Reliability standards. New registration criteria include generator owner and operators of IBRs with an aggregate nameplate capacity over 20 MVA per IBR plant connected at voltages above 60 kVs, also known as Category 2. NERC indicates that this change will mean 97.5% of IBRs impacting BES will be subject to NERC Reliability standards.[12] As of May 2026, 561 newly registered Category 2 entities[13] are required to comply with eight NERC Reliability standards related to operations and planning.[14] While no CIP standards are currently active and enforceable for these entities, NERC intends to modify at least some existing CIP standards prior to being considered applicable and enforceable for these newly registered entities.[14] These changes will create new cybersecurity requirements for solar and storage entities not previously under NERC jurisdiction.

In addition, NERC categorizes assets into low, medium, and high impact, mandating different levels of security requirements based on the severity of consequences if compromised. In 2025, NERC made a significant shift toward revising classification of historically low-impact assets like IBRs to require stricter security controls or even classifying them as medium impact.

New NERC CIP standards are further reshaping cybersecurity for solar and storage operations. For instance, NERC CIP-003-9, effective April 2026, mandates robust vendor remote access cybersecurity controls for low impact systems, acknowledging the critical role the supply chain and third-party vendors play in security. Additionally, FERC's recent approval of CIP-003-11, which will come into enforcement in the coming years, will require new baseline electronic access cybersecurity safeguards for low impact BES Cyber Systems. SEIA is committed to supporting members navigating these significant shifts in the regulatory landscape and encouraging proactive cybersecurity implementations as these standards continue to evolve.

Despite these significant changes for the BES, distribution-connected solar and storage sites fall outside of NERC CIP applicability. SEIA is working with industry and government partners to proactively implement standards, best practices, and guidelines to improve security across the industry. Some examples include:

IEEE 1547.3	A guide for distributed energy resources interconnected to electric power systems, including resources like solar, wind, electric vehicles and battery storage.
UL2941	A cybersecurity certification standard offering testable requirements for distributed energy resources and inverter-based resources.
SunSpec Cybersecurity Certification Program	Offers a certification program for securing distributed energy resources.
IEC 62443	A series of cybersecurity standards for industrial and automation control systems, which can be applied to solar and storage technologies and systems.
Cross-Sector Cybersecurity Performance Goals	Created by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) are a set of voluntary cybersecurity practices that can be tailored to specific sectors.
The National Institute of Standards and Technology (NIST) Guidance Documents	Including the Cybersecurity Framework, Guidelines for Smart Grid Cybersecurity, Cybersecurity for Smart Inverters, Securing Distributed Energy Resources, and a Guide to Operational Technology, among others, may be applied to improve the security of solar and storage industry.
Cybersecurity Baselines for Electric Distribution Systems and DER	Developed by the U.S. Department of Energy (DOE) and the National Association of Regulatory Utility Commissioners (NARUC), offers voluntary cybersecurity practices drawn from common frameworks, standards, and guidelines.

SEIA is actively supporting the solar and storage industry to comply with regulations and adhere to best practices and standards that improve the industry's security and resilience against evolving cyber threats. For example:

- SEIA, together with NERC, DOE, and Sandia National Laboratories developed Recommendations for Solar Energy that includes high-priority controls and security recommendations to enhance the cybersecurity posture of the industry.[15]
- SEIA played an active role in the development of the Cybersecurity Baselines for Electric Distribution Systems and DER in collaboration with NARUC and DOE.
- SEIA served as a key member of the Cybersecurity Advisory Team for State Solar (CATSS) to mitigate cybersecurity risks and consequences in solar energy developments.
- SEIA serves as an industry advisory board member on the DOE's Securing Solar for the Grid program.
- SEIA's longstanding Secure Renewables education series brings together industry leaders through virtual and in-person education sessions and workshops to educate and inform the industry on emerging cybersecurity trends and topics.
- SEIA contributes to the development and improvement of industry standards and best practices including engagement with NERC, NATF, NIST, IEEE, UL, national laboratories, and more.
- SEIA runs a monthly cybersecurity working group dedicated to disseminating the latest cybersecurity policy and threat information, sharing key insights, and discussing industry best practices and techniques for defending solar and storage from cyber threats.
- SEIA presents and participates in industry and government conferences and events to educate and communicate the latest cybersecurity developments, best practices, and practical steps to protect solar and storage systems.

SEIA Pillars for a Cybersecure Solar and Storage Industry

Building reliable, affordable energy systems will require solar and storage to be secure and resilient against evolving cybersecurity threats. To meet America's growing energy needs, cybersecurity must be at the forefront of the industry's rapid growth. SEIA is committed to achieving this vision by providing advocacy, partnership, and leadership on cutting edge cybersecurity issues facing the industry. These pillars will support SEIA members by improving their knowledge and awareness of the cyber threat landscape, strengthening their defenses, and enhancing the industry's overall security posture.

Support supply chain security for solar and storage

Advance supply-chain resilience, transparency, and trusted manufacturing capacity

SEIA supports policies that strengthen domestic manufacturing, supply chain resilience, supplier transparency, trusted manufacturing capacity, and demand certainty across the solar and storage ecosystem. Domestic inverter manufacturing capacity has already grown significantly in recent years, with total capacity as of July 2026 reaching 55GWac.[16] SEIA is committed to supporting that continued growth. NERC has recognized that supply chain constraints can affect grid reliability, including limited U.S. manufacturing capacity and long procurement timelines for large power transformers and high-voltage direct current transmission equipment.[17]

NERC's broader reliability work also identifies comparable planning and operational challenges in other parts of the energy system, including natural gas supply, transportation and delivery risks, pipeline constraints, electricity-dependent gas infrastructure[18], scheduling gaps, fuel-assurance challenges, and backup-fuel limitations.[19] SEIA supports a technology-neutral, risk-based approach that improves visibility, procurement discipline, vendor and supplier risk management, lifecycle security, and the consistent application of cybersecurity controls and best practices across the energy sector.

Supporting robust cybersecurity controls and defenses

SEIA supports the industry in navigating operational supply chain challenges and third-party risk management. SEIA works with partners and industry to promote a robust and cyber-informed approach to the implementation of the highest impact organizational and technical controls and best practices necessary for the security and resilience of the supply chain and its key dependencies throughout the lifecycle of solar and storage systems.

Strengthen baseline cybersecurity practices

Support cybersecurity compliance

Keeping pace with the cybersecurity compliance landscape can be a significant challenge, particularly for entities that are anticipating or implementing cybersecurity requirements for the first time. SEIA communicates and participates in security and reliability standards processes that affect the solar and storage industry to ensure members understand their obligations and successfully navigate regulatory and compliance changes. As new standards are introduced, SEIA will continue supporting the industry in developing proactive approaches to security, rather than waiting for enforcement actions to take effect.

Support national guidance on the cybersecurity of distributed energy resources

While NERC CIP requirements protect an increasing number of solar and storage installations, the cybersecurity of distribution-connected systems is guided by a variety of interconnection and contractual requirements as well as voluntary standards and frameworks, which can lead to inconsistent baseline cybersecurity practices. SEIA supports standardized, national cybersecurity guidelines for distributed energy resources that can cover those entities and projects. These guidelines could then be used as the foundation for implementing state-level policies that impose minimum standards for compliance. The groundwork for these national guidelines has already been laid through existing resources like DOE/NARUC's Cybersecurity Baselines for Electric Distribution Systems and DER, IEEE 1547.3, NIST Special Publication 1800-32A, Securing Distributed Energy Resources, and IEC 62443 Security for Industrial Automation and Control Systems.

Visibility, awareness, and risk reduction

Support information and resource sharing for industry

SEIA members often lack visibility into emerging threats specific to the solar and storage industry. SEIA will continue to collaborate with partners like the Electricity Information Sharing and Analysis Center (E-ISAC), the Cybersecurity and Infrastructure Security Agency (CISA), and the Energy Threat Analysis Center (ETAC), among others, to support timely, secure, and actionable information that is relevant to the solar and storage industry. Information sharing is vital to proactive defense against the evolving threat landscape and collaborating on effective countermeasures that strengthens resilience across the energy sector.

Risk communication and risk reduction

A perennial problem in cybersecurity is communicating and measuring the effectiveness of cybersecurity investments that reduce cyber risks. SEIA will continue to engage with industry partners on tools and best practices to help industry better understand cybersecurity risks, communicate those risks more clearly to decision makers, and make cybersecurity decisions that reduce risks.

Increase cybersecurity awareness and education to the solar and storage industry

Cybersecurity is a highly dynamic and complex topic. Technologies, threats, regulations, and best practices evolve quickly, making continuous education and awareness essential to securing solar and storage systems. SEIA is committed to providing best-in-class educational content to make security accessible and actionable for stakeholders across the industry.

Conclusion

The solar and storage industry is an increasingly important part of the energy sector in the United States and its security and resilience is paramount. Advancing the cybersecurity of solar and storage systems is a priority for SEIA. SEIA will continue to work with industry members and policymakers to advance the strategic priorities that reduce risk, increase awareness, and improve security outcomes for the industry.

References

[1] https://seia.org/research-resources/solar-market-insight-report-2025-year-in-review/

[2] https://www.pewresearch.org/short-reads/2026/05/06/many-americans-hold-utility-companies-responsible-for-their-rising-home-energy-bills/

[3] https://www.nerc.com/globalassets/our-work/guidelines/security/sg_voluntary_physical_security_protection_best_practices_at_entity_facilities.pdf

[4] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector

[5] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[6] https://www.vice.com/en/article/ukrainian-power-station-hacking-december-2016-report/

[7] https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

[8] https://www.reuters.com/sustainability/climate-energy/massive-cyberattack-polish-power-system-december-failed-minister-says-2026-01-13/

[9] https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure

[10] https://emp.lbl.gov/sites/default/files/2025-10/Utility%20Scale%20Solar%202025%20Edition%20Slides.pdf

[11] https://www.nerc.com/globalassets/our-work/reports/ero-reliability-risk-priorities-report/2025_risc_ero_priorities_report.pdf

[12] https://www.mro.net/document/about-the-ibr-registration-initiative/?download

[13] https://www.nerc.com/globalassets/who-we-are/legal--regulatory/filings--orders/nerc-filings-to-ferc/2026/ibr-workplan-filing_apr-2026_signed.pdf

[14] https://www.nerc.com/globalassets/standards/projects/2024-01/compliancedatesforgos_gops.pdf

[15] https://seia.org/wp-content/uploads/2024/08/Recommendations-for-Solar-Energy-Cybersecurity-SAND2023-04512O.pdf

[16] https://seia.org/research-resources/solar-storage-supply-chain-dashboard/

[17] https://www.nerc.com/globalassets/who-we-are/news/2026/06/reliability-insights-supply-chain-security.pdf

[18] https://www.nerc.com/globalassets/initiatives/electric-gas-interdependence/electricity_natural_gas_strategy.pdf

[19] https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/egwg/fuel_assurance_and_fuel-related_reliability_risk_analysis_for_the_bulk_power_system.pdf