



WHITE PAPER

How SunSpec Specifications & Certifications Provide a Cybersecurity Framework for FCC Conditional Approval of Foreign-Made Inverters

Enabling Secure Interoperability.
Building Trust at the Grid Edge.



What Manufacturers Need to Know Now

On July 29, 2026, the Federal Communications Commission (FCC) of the United States issued a directive banning certain foreign-made power inverters and robotic devices (see this link for the announcement).

Here is a brief synopsis of the directive:

Headline: FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES ADDITION OF FOREIGN-PRODUCED POWER INVERTERS AND ADVANCED ROBOTIC DEVICES TO FCC COVERED LIST

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

The FCC action applies to "foreign-produced" power inverters. The FCC defines "foreign-produced" by reference to the federal definition of a "domestic end product" in 48 CFR § 25.101(a). Under the generally applicable test for manufactured products, an inverter must be manufactured in the United States and satisfy the applicable domestic-component cost threshold to qualify as a domestic end product. The threshold is 65 percent for products delivered during calendar years 2024 through 2028 and rises to 75 percent beginning in 2029. Manufacturers should obtain legal or regulatory guidance before relying on this classification, particularly because federal acquisition rules contain product-specific provisions and exceptions.

Cybersecurity Rationale & Industry Context for the Foreign Inverter Action

The Federal Communications Commission (FCC) updated its Covered List to include connected power inverters produced in foreign countries (alongside "advanced robotic devices"). This action follows determinations by a White House convened Executive Branch interagency national security body, which concluded that these foreign-made products, regardless of their country of origin (as no specific countries were named), pose "unacceptable risks to the national security of the United States or the safety and security of United States persons."

From a cybersecurity perspective, the interagency rationale centers on the fact that modern inverters manage bidirectional power flows and rely heavily on cellular, Wi-Fi, or Ethernet connectivity. Unsecured remote management interfaces expose the grid to critical vulnerabilities:

- **Grid Instability & Wide-Scale Shutdowns:** Malicious actors exploiting unauthenticated remote access could trigger synchronized shutdowns or alter power profiles, causing severe frequency disruption and grid instability across regional interconnects.
- **Firmware Update Architecture Exploits:** Insecure over-the-air (OTA) update channels or

compromised foreign update servers create vectors for injecting backdoored code, overriding local controls, or maintaining unauthorized persistent access.

- **Data Exfiltration & Surveillance:** Networked inverters continuously transmit granular spatial and operational telemetry, creating exposure risks regarding critical energy infrastructure dependencies.

Given that U.S. Energy Information Administration data shows solar, wind, and battery storage account for 93% of all planned new utility-scale electric generating capacity in the U.S. in 2026, mirroring broader global adoption, this unannounced FCC action creates immediate friction and confusion across global supply chains.

The global energy transition relies on open, competitive markets. **SunSpec encourages the industry itself to take leadership, take these threats seriously, and implement the common sense security measures defined within various SunSpec Specifications.** SunSpec specifications and certification provide a cybersecurity framework to generate evidence of addressing the FCC Cybersecurity concerns.

Since its inception, SunSpec has defined open information standards and best practices for the Distributed Energy Resource (DER) industry to lower costs, mitigate operational risk, and accelerate renewable adoption. By implementing these well-understood technical controls, the industry can directly address the national security risks identified by federal regulators while preserving open global trade, maintaining grid sovereignty, and supporting a secure, abundant energy transition.

Path to Conditional Approval

A foreign-produced inverter may nevertheless qualify for a Conditional Approval if it meets certain criteria. Manufacturers may initiate the process by submitting the information requested in the FCC guidance to conditional-approvals@fcc.gov. The submission will be forwarded to the Department of War and/or Department of Homeland Security for national-security evaluation. Conditional Approval is granted through the applicable federal determination, not through SunSpec or the FCC equipment-testing process alone.

The requested information extends beyond the inverter's physical place of manufacture. Applicants must also disclose matters including the country of origin of onboard software and firmware, ownership of the associated intellectual property, and the entities responsible for software updates. The FCC materials do not yet explain precisely how these software-related factors will be weighed against domestic manufacturing and component content. Manufacturers should therefore document both their hardware supply chain and their software governance, update authority, remote-access architecture, and vulnerability-management practices.

These requirements create two related but distinct questions: whether an inverter is foreign-produced and, if it is, whether its architecture and governance provide sufficient evidence for Conditional Approval. SunSpec Cybersecurity related specifications/certifications are particularly relevant to the second question.

Comparison Table: FCC Concerns vs. SunSpec Coverage

FCC concern or requirement	Secure SunSpec Modbus and SunSpec Certification*	SunSpec Cybersecurity Standards, Best Practices, and Certification*	SunSpec IEEE 2030.5 CSIP Certification *	Coverage Assessment
Secure remote communications	✓	✓	✓	Strong
Strong Encryption and authentication	✓	✓	✓	Strong
Unauthorized remote control or shutdown	✓	✓	✓	Strong, provided all remote interfaces are evaluated
Role-based access control	✓	✓		Strong
Device hardening and secure boot		✓		Strong
Secure firmware and software development		✓		Strong

Vulnerability identification and remediation		✓		Strong
Protection against data exfiltration	✓	✓	✓	Strong
Software and firmware component inventory	Partial	Partial	Partial	Could be strengthened through a required SBOM
Hardware component inventory	Partial	Partial	Partial	Would require a formal HBOM requirement
Supplier and supply-chain risk management	✓	✓	✓	Substantial, but additional FCC-specific disclosures would be needed
Component producers and production locations	✓	Partial	✓	Could be added to the certification evidence package
Component value by country				Not currently covered
Supply-chain concentration by country				Outside SunSpec certification scope
Supply-chain single points of failure				On road-map for Device Certification

Change control for hardware, software, and firmware	Partial	✓		SunSpec policy requires notification by suppliers.
Corporate attestation that disclosures are accurate	✓	✓	✓	SunSpec Certification achieves this
“Domestic end product” determination				Outside SunSpec certification scope
Covered List eligibility				Determined by the FCC
Conditional Approval				Determined by DHS or the Department of War
FCC equipment authorization				Determined through the FCC authorization process
FCC ID and marketing requirements				Administrative and regulatory responsibility of the manufacturer and seller

*SunSpec Certification guarantees the vendor has implemented the SunSpec standard correctly and collects certain information including the firmware version number, name, and a checksum, which are relevant to supply chain security. Base certification requirements also establish the identity of the company and the executive leader. These documents are signed under penalty of perjury.

How SunSpec Open Standards Address FCC Cybersecurity Concerns

FCC Concern / Vulnerability Area	Covered by SunSpec DER Device Cybersecurity Certification?	Covered by Secure SunSpec Modbus Certification?	SunSpec IEEE 2030.5 CSIP Certification	Applicable Open Standard / Guidance
Weak Access Control & Password Exposure	✓	✓		Unique default credentials, mandatory password updates, Role-Based Access Control (RBAC).
Unauthorized Remote Firmware Updates	✓	✓	✓	Cryptographically signed firmware, secure boot, mutual TLS 1.2/1.3 authentication.
Data Interception & Surveillance	✓	✓	✓	End-to-end encryption using modern, standardized cipher suites over TCP/IP.
Unverified Supply Chain / Backdoors	✓			Aligned with IEC 62443-4-2 hardware hardening and vulnerability management.
System Audit & Incident Forensics	✓	✓		Event logging requirements for unauthorized access attempts and system changes.

Conclusion

The U.S., like regulators in the European Union (see the Cyber Resilience Act (CRA) and Network and Information Security 2 (NIS2)) have finally acknowledged that cybersecurity is essential to the distributed energy transition. While the decision to mandate cybersecurity in the U.S. was quite abrupt (and one can argue wrongly conflated with trade policy) there is no doubt that the decision to embrace cybersecurity is a correct one.

As the SunSpec Alliance has advised and advocated for more than a decade, the time to implement cybersecurity as the foundation of distributed energy is now. Fortunately, because of the successful global effort to deploy interoperable communication standards like SunSpec Modbus and IEEE 2030.5, upgrading the cybersecurity foundation of distributed energy networks at the lowest cost—using open SunSpec cybersecurity standards—is possible. SunSpec looks forward to working with all industry partners, from every country, to ensure that distributed and renewable energy continues to be the safest, most resilient, and most cost-effective source of energy for all of humanity.

Resources

- FCC, *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*:
<https://docs.fcc.gov/public/attachments/DOC-422746A1.pdf>
- FCC, *Importation and Marketing of Previously Authorized Covered Equipment*:
<https://docs.fcc.gov/public/attachments/DA-26-635A1.pdf>
- FCC, *Addition of Foreign-Produced Routers to the Covered List*:
<https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf>
- FCC, *Covered List FAQs: Robots and Inverters*: <https://www.fcc.gov/covered-list-faqs-robots-inverters>
- FCC, *List of Equipment and Services Covered by Section 2 of the Secure Networks Act*:
<https://www.fcc.gov/supplychain/coveredlist>
- FCC, *OET Waives Certain Permissive Change Prohibitions*:
<https://www.fcc.gov/document/oet-waives-certain-permissive-change-prohibitions>
- FCC, *Annex A: Guidance on Conditional Approval for Inverters*:
<https://www.fcc.gov/sites/default/files/annex-a-guidance-conditional-approval-inverters.pdf>
- FCC, *FCC Adds Foreign-Produced Power Inverters and Robots to Covered List*:
<https://www.fcc.gov/document/fcc-adds-foreign-produced-power-inverters-and-robots-covered-list>
- IEEE, *IEEE Standard for Smart Energy Profile Application Protocol*
<https://standards.ieee.org/ieee/2030.5/5897/>
- SunSpec Alliance, *Specifications*: <https://sunspec.org/specifications/>
- SunSpec Alliance, *Product Certification Registry*: <https://sunspec.org/product-certification-registry/>