COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
COMMONWEALTH KEYSTONE BUILDING
400 NORTH STREET
HARRISBURG, PENNSYLVANIA 17120

November 5, 2026

Cybersecurity Advisory: Foreign-Manufactured Power Inverters Advisory

To All Jurisdictional Electric Distribution Companies:

The Pennsylvania Public Utility Commission (Commission) advises jurisdictional Electric Distribution Companies (EDCs) of emerging cybersecurity and supply-chain risks involving foreign-manufactured, internet-connected power inverters used in solar, wind, battery energy storage systems, and other distributed energy resources (DERs). This advisory comes amid heightened concern regarding cyber activity directed at U.S. critical infrastructure.

Background

Federal agencies—including the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Department of Defense Cyber Crime Center—have warned that foreign nation-state and affiliated cyber actors may target vulnerable U.S. networks and critical infrastructure. Past incidents have included exploitation of internet-connected industrial control systems and operational technology across the energy sector. The Commission encourages EDCs to review CISA's modern Cross-Sector Cybersecurity Performance Goals (CPGs) and related advisories concerning nation-state threats to critical infrastructure.

Emerging Inverter Risk

New cybersecurity concerns have surfaced involving foreign-manufactured power inverters and their remote-management capabilities. U.S. officials have investigated Chinese-manufactured inverters and batteries after identifying undocumented communications components—such as embedded cellular radios—that could allow unauthorized remote access outside utility-approved control channels. The European Commission has similarly designated solar and wind infrastructure as priority cybersecurity risk areas, citing potential manipulation of electricity production, unauthorized access, supply-chain infiltration, and remote disruption of electric systems.

The European Union now restricts the use of EU funds for projects involving high-risk inverter suppliers and continues to assess cybersecurity risks in solar installations. Many assessments highlight significant dependence on Chinese-manufactured inverter technologies—such as equipment produced by Huawei and Sungrow—and note that

some manufacturers or third-party cloud managers possess remote access to interconnected DER assets.

The Commission recommends that EDCs identify and evaluate cybersecurity and supply-chain risks associated with foreign-manufactured, remotely accessible power inverters operating within their distribution territories. These devices may be deployed in utility-scale renewable facilities, battery energy storage systems, commercial installations, distributed generation, and residential solar systems.

While a single residential inverter represents limited localized risk, modern virtual power plants (VPPs) pool these devices via unified cloud links. A coordinated compromise via a single vendor cloud API or thousands of remotely accessible devices could affect wide-scale distribution-system reliability. To ensure alignment with federal guidance and enhance grid security, the Commission recommends the following integrated mitigation strategies:

Recommended Mitigation Strategies

1. Supply-Chain Cybersecurity Controls

- Firmware Authenticity Verification: Require vendors to provide firmware authenticity verification, including digital signatures or cryptographic integrity checks.
- Bill of Materials Documentation: Request and systematically maintain both Software Bills of Materials (SBOMs) and Hardware Bills of Materials (HBOMs) for inverter hardware, firmware, and embedded communications modules to detect unvetted modifications.
- Pre-Deployment Testing: Conduct pre-deployment cybersecurity testing to detect undocumented communication pathways, hidden physical hardware components, or rogue cellular radios.
- Transparency & Disclosure: Require vendors to disclose all remote-access capabilities, automatic update mechanisms, and third-party service dependencies.
- Vendor Risk Architecture: Incorporate supplier security posture into ongoing risk assessments and periodically re-evaluate vendor trustworthiness.

2. Remote-Access Governance

- Access Minimization: Disable manufacturer-provided remote-access functionality unless explicitly needed and approved by utility procedures.
- Gateway Access Isolation: Restrict all remote access to utility-controlled interfaces with multi-factor authentication, encrypted tunnels, and monitored jump hosts.
- Session Management: Ensure vendor access is time-bound, session-controlled, and fully logged, including session recording where feasible.

- Cloud & Aggregator Oversight: Evaluate and tightly control cloud-based vendor monitoring channels and third-party Distributed Energy Resource Aggregator (DERA) / Virtual Power Plant (VPP) APIs to ensure strict integration with utility cybersecurity policies.

3. OT Network Architecture & Segmentation

- Zone Isolation: Place inverter gateways and management interfaces within isolated Operational Technology (OT) network zones separated from corporate or internet-facing networks.
- Unidirectional Data Flow: Deploy unidirectional gateways or data diodes for telemetry-only environments, reducing exposure to command-injection attacks.
- Anomalous Traffic Monitoring: Monitor inverter network traffic for unexpected outbound connections, foreign IP destinations, or anomalous communication patterns.
- Connectivity Documentation: Document all inverter connectivity—including Wi-Fi, cellular, and vendor portals—and eliminate non-essential communication paths.

4. Device Hardening & Configuration Management

- Credential & Interface Hardening: Change all default credentials and disable unused communications interfaces such as Bluetooth, local Wi-Fi, or unsecured web portals.
- Vetted Patch Pipelines: Apply vetted firmware updates and implement a controlled patch-management schedule with integrity verification.
- Least-Privilege Enforcement: Enforce least-privilege access controls, ensuring installers and system owners have only the minimum required permissions.
- Secure Protocol Wrapping: Restrict clear-text, unauthenticated inverter protocols (e.g., standard Modbus RTU/TCP, SunSpec) through firewalls, allow-lists, and port filtering, while transitioning to secure protocols such as IEEE 1547.3, Modbus Secure, or DNP3 Secure Authentication.

5. Monitoring, Detection & Response

- Grid Telemetry Correlation: Deploy anomaly-detection systems capable of flagging unusual inverter behavior, including coordinated generation changes across distinct sites.
- SCADA Harmonization: Correlate inverter telemetry with grid operational and SCADA data to detect suspicious patterns of widespread DER manipulation.
- Incident Response Playbooks: Integrate inverter-specific events into utility cyber-incident response plans, including clear procedures for rapid device isolation and secure firmware rollbacks.

6. Physical & Communications Security

- Hardware Tamper Inspections: Inspect inverter hardware for undocumented communication components or evidence of physical tampering.
- Secure Logistics Assurances: Require integrators to demonstrate secure manufacturing and transit practices, including tamper-evident seals and verified production sourcing.
- Physical Perimeter Controls: Limit physical access to inverter enclosures and control rooms with strong physical access controls and surveillance monitoring.

Conclusion

This advisory ensures that Pennsylvania's EDCs remain aware of the growing cybersecurity and supply-chain risks associated with foreign-manufactured power inverters and incorporate these concerns and mitigation strategies into existing cybersecurity, supply-chain, and risk-management programs. By applying established federal guidance—including NERC CIP standards, DOE CESER principles, CISA OT isolation frameworks, and updated NIST/IEEE smart-inverter security recommendations—EDCs can better protect distribution-system reliability and reduce exposure to nation-state and supply-chain cyber threats.

If you have any questions regarding this advisory, please contact Michael Holko, Director of the Office of Cybersecurity Compliance and Oversight, at 717-425-5327 or via email at miholko@pa.gov.

Sincerely,



Matthew Homsher
Secretary