IEEE-USA

POSITION STATEMENT

Cybersecurity and the Electrical Power Grid

Approved by IEEE-USA
Board of Directors (February 13, 2026)

The electric power systems in the United States are under persistent, escalating cyberattacks. Although a broad spectrum of new initiatives to enhance grid security have been introduced, these new measures are insufficient to reverse the recent massive increase in vulnerability to coordinated attacks by hostile state actors or similar organized groups.

This increased vulnerability is primarily driven by four factors:

- **Cyberattack Software Proliferation:** The widespread leakage of globally developed cyberattack software and methods, such as those associated with Stuxnet-type operations, has put U.S. infrastructure at risk.
- **Increasing Networked Control:** The growing need for and use of networked control systems in power grids to enhance reliability, energy security, and efficiency has expanded the potential attack surface. The integration of distributed energy resources (DERs) and the Internet of Things (IoT) has further complicated the threat landscape.
- **Third-Party Reliance Vulnerabilities:** There are increasing issues with the sources and maintenance of core operating systems that software vendors rely on when supplying services to grid operators. The increasing reliance on third-party vendors also introduces significant supply chain risks, making the grid vulnerable to malware and hardware compromises.
- **The Use of AI and Hybrid Threats:** Malicious actors are increasingly using artificial intelligence to automate and scale attacks. Additionally, the emergence of hybrid threats that combine cyberattacks with physical sabotage poses a heightened risk to the nation's critical infrastructure.

The electric power grid is an enabling system for all other critical public utilities. A cyberattack on the grid poses a severe risk of cascading failures across sectors. A sustained power outage can disrupt the operation of public infrastructure, including water and wastewater systems, transportation networks, telecommunications networks, and energy infrastructure. For example, a power disruption can halt pumping stations,

leading to a loss of clean water, and cut power to natural gas compressor stations, which can cause fuel shortages for gas-fired power plants. This interconnectedness means that a grid attack is not a single-sector event but a national emergency.

Historically, the U.S. government relied on managing backdoors in operating systems, chips, and communication systems to monitor hostile parties and conduct offensive cyber operations. The Information Assurance component of the National Security Agency (NSA) previously managed and limited access to these backdoors, in part by supporting to prevent the U.S. power grid from being vulnerable to a reverse Stuxnet-style attack.

However, this strategic advantage has dissolved, and it would be imprudent to base future policy on the assumption that the U.S. will recover. The U.S. must now confront this loss of advantage and move swiftly to address our vulnerability. While it may be challenging to restore security while retaining our prior offensive capabilities, technology should enable us to re-establish a balance between privacy and traditional intelligence-gathering capabilities.

The security of the power grid requires planning across the entire system, from operating systems and communications systems to cyber defenses and supply chains. There are opportunities for quick, impactful cybersecurity improvements. Advanced operating systems can be built with defenses by using artificial intelligence to detect anomalies and respond quickly. Advanced systems can use authentication by enforcing strict control over critical system sectors, ensuring access is limited to a small, authorized group of administrators. Comprehensive risk management techniques can be used to secure supply chains. Communications systems can be built to encrypt and filter messages. Finally, integrating security concerns into everyone's job is critical to safeguarding our power grid.

Recommendations

IEEE-USA recommends:

- **Establish a National Cybersecurity Strategy for the Grid:** Move beyond a reactive stance by setting clear, outcome-based goals for cyber resilience. This must be a proactive, strategic national plan that fosters whole-of-nation collaboration and integrates a flexible security framework. The goal is to mitigate risk before major incidents occur and to ensure the framework can evolve as quickly as the threat landscape evolves.
- **Integrate Artificial Intelligence for Predictive Defense**: Leverage AI as a tool that can analyze massive amounts of data, detect anomalies, and respond within milliseconds. Policies should encourage the use of AI for threat detection,

automated response, and predictive defense against emerging threats, including those posed by adversarial AI, with human review of these programs. We should also continue to invest in advances in artificial intelligence systems to support electrical grids through fundamental research, which will help with system restoration and service quality, and build the future workforce.

- **Develop Secure Operating Systems (OS):** Accelerate research, development, and demonstration (RD&D) of new, highly secure operating systems specifically for critical grid infrastructure. These systems should employ formal methods to ensure the absence of backdoors and be validated through transparent, open-source machine validation. This effort includes creating specialized OS software for embedded control chips in the growing Internet of Things (IoT) and adapting the technology for the parallel computing systems needed for future grid control.
- **Enhance Supply Chain Security:** Mandate comprehensive supply chain risk management programs for all critical grid operators. This includes requiring a Software Bill of Materials (SBOM) for all software and firmware, which provides a detailed list of components to facilitate the identification and rapid patching of vulnerabilities. Policy should also incentivize the domestic manufacturing of critical components and empower regulators, such as FERC and NERC, to strengthen the auditing and enforcement of supply chain security. All products, both hardware and software, should be thoroughly tested before being put into service in the power grid.
- **Secure Grid Communications:** Promote and invest in resilient communication pathways for the grid, leveraging redundant, diverse networks beyond public infrastructure. Establish and enforce robust cybersecurity standards for all internet-connected devices, including IoT and smart devices, and facilitate the real-time sharing of threat intelligence among grid operators, communication providers, and government agencies to enable a faster, more coordinated response.
- **Implement Zero Trust Architecture:** Require it across the entire grid. This security model operates on the principle of "never trust, always verify," ensuring that all users and devices, regardless of location, are continuously authenticated and authorized before gaining access to grid systems. This approach provides a strong focus on securing every part of the operational environment, from the largest control systems to the smallest sensor.
- **Administrative Processes:** Advanced operating systems offer the opportunity for quick, impactful cybersecurity improvements. They can simplify authentication by enforcing strict control over critical system sectors, ensuring access is limited to a small, authorized group of administrators. However, this technical capability is inherently vulnerable without a rigorous and immediate human administrative process for credential and access management; specifically, all administrator credentials and system access must be instantly revoked and disabled the moment an individual departs the organization, regardless of the circumstances,

as a failure to manage this human process effectively negates the security gains provided by the OS architecture.

The IEEE-USA Energy Policy Committee developed this statement, representing the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 160,000 engineering, computing, and allied professionals who are U.S. members of the IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE or its other organizational units.

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: https://www.ieeeusa.org