Reliability Insights

Supply Chain Security

June 2026

North America's grid reliability is heavily dependent on the security of the energy sector's supply chain, which is inherently sensitive to geopolitical events, manufacturing shortfalls, and cyber attacks. This dependence is expected to intensify as industry transitions to the grid of the future, expanding transmission infrastructure and adding new generation resources that further strain an already vulnerable supply chain. Taking a proactive approach through robust mitigation measures such as information sharing, enhanced risk management practices, and situational awareness will better position the electric industry to mitigate the significant risks that supply chain security presents.

Two Sides of the Supply Chain Security Coin

The phrase "supply chain security" is commonly used as an all-encompassing term but has two distinct definitions:

1. Securing against risks associated with the availability and reliability of the supply chain
2. Securing against cyber security risks within the supply chain

It is important for entities to clearly define the policies and practices and training associated with each when implementing a supply chain risk management program.

How Availability Affects Reliability and Security

The need to modernize and increase the capacity of the North American electric grid to meet the significant increase in demand for electricity and address aging infrastructure has revealed significant gaps in the sector's supply chain reliability. In response to this, the current U.S. administration issued a presidential memorandum classifying the United States' constrained electric grid as a threat to national defense and stating that risks to the electric supply chain leave the United States vulnerable in the event of "war, disaster, or economic disruption."

Overreliance on imported parts and equipment coupled with long production lead times poses the most significant risk to supply chain reliability. Domestic manufacturing capacity for many of the critical components supporting grid operations is limited; in particular, the United States is severely lacking the ability to manufacture large power transformers (LPT) and high-voltage direct current (HVdc) transmission in a timely and reliable manner. The testing and procurement of new or replacement equipment can involve lead times of up to 10 years. The ongoing integration of more renewable energy resources, such as solar photovoltaic and battery storage assets, creates additional vulnerability as the manufacture of parts and equipment is dominated by foreign suppliers. Reliance on imports, for both new assets and those nearing end of life, leaves organizations vulnerable to market shifts, disruptions, and trade policies, all of which are affected by major world events and geopolitical maneuvering.

Cyber Security Risks Within the Supply Chain

The electric supply chain is inherently complex, with a single system potentially containing hundreds of subcomponents sourced from global third-party manufacturers and vendors, many of which may retain remote access into the system for services or maintenance. The continued integration of renewable energy resources and associated third-party services has deepened this complexity, introducing new suppliers into the grid ecosystem and increasing reliance on remote monitoring and access tools. Occasionally, unexpected connectivity not reflected in a bill of materials may be present, introducing a potential pathway into sensitive systems, whether that connectivity was placed there with malicious intent or not. The hardware, software, and services provided by third parties, who may have a weaker security posture than industry organizations, have become targets of compromise that further extend industry's exposure.

Common Supply Chain Cyber Attack Types

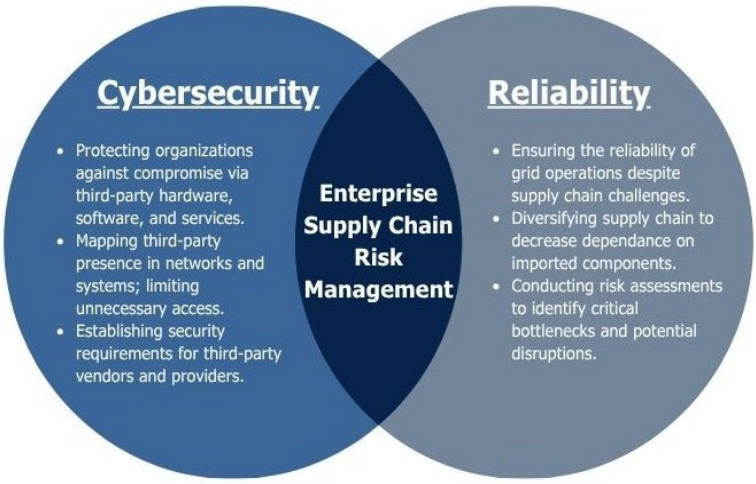
- **Attacks on Hardware:** Threat actors can pre-install malware onto hardware devices during manufacturing or distribution.
- **Attacks on Software:** Threat actors compromise legitimate, commercial software products by injecting malicious code into updates or patches.
- **Attacks on Services:** Threat actors exploit vulnerabilities in third-party service providers, such as lack of remote access security or unpatched vulnerabilities, to access client networks and systems.

State-sponsored threat actors pose a significant threat to supply chain security. Government agencies associated with these groups could potentially demand that manufacturers place malicious code within their products before exporting them to foreign buyers, providing a back door for future cyber attacks. Availability constraints may further exacerbate this threat by driving entities to rely upon second- or third-tier suppliers with potential ties to adversarial government entities.

Understanding the cyber threat landscape by acting on and sharing intelligence with the Electricity Information Sharing and Analysis Center (E-ISAC) strengthens industry's cyber supply chain security. The E-ISAC's Vendor Affiliate Program also engages with many of the critical equipment and technology vendors that support industry by providing an additional path to promote collective supply chain security.

Recommended Actions to Enhance Supply Chain Security Risk Management

Supply chain security is a shared responsibility among the electric industry, policymakers, manufacturers, vendors, and service providers. Entities should have the appropriate policies, procedures, and training in place to address the different but equally critical aspects of supply chain security and protect themselves against supply chain-



related attacks, scarcity, and risks. Key actions include the following:

- Identifying who from your organization needs to be involved in supply chain security activities. Include subject matter experts from cyber security, IT, acquisitions and procurement, legal, logistics, and senior leadership.
- Developing and implementing a supply chain security program, including policies and standard operating procedures.
- Reviewing resource documents and guidelines such as NERC's *Supply Chain Risk Management Plans - Implementation Guidance for CIP-013-1* and the U.S. Department of Energy's *Supply Chain Cybersecurity Principles*.
- Conducting a comprehensive supply chain risk assessment that includes mapping where your organization procures its assets, hardware, software, and services.
- Establishing security requirements for vendors that are included within your organization's procurement language. Conduct continuous monitoring and evaluation to ensure continued vendor compliance.
- Diversifying your organization's supply chain when possible to avoid the risks associated with limited manufacturing or dependence on imported components.
- Identifying end-of-life timelines for critical assets and developing replacement strategies to mitigate risks associated with long lead times.
- Joining the E-ISAC and sharing supply chain-related information and intelligence.