NATIONAL SUPPLY CHAIN INTEGRITY MONTH

A SPOTLIGHT ON

ENERGY

Fortifying U.S. Energy Supply Chains

“America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition” is the Department of Energy’s (DOE) one-year review required by Executive Order 14017, America’s Supply Chains. DOE recognizes a fortified supply chain is critical during the energy sector transitions corresponding with U.S. commitments to create a power sector free of carbon pollution by 2035 in pursuit of achieving net-zero emissions economy-wide by 2050. This report examines the risks and challenges facing U.S. energy supply chains, describes the federal government’s plans to address them, and identifies strategic policies for leveraging the opportunities presented. While the focus of this report emphasizes these risks, this NCSC Supply Chain Spotlight concentrates on counterintelligence cyber threats highlighted in the stated risks from the DOE report.

Counterintelligence Risks

Among the risks identified in DOE’s one-year review, cybersecurity concerns pose the broadest challenges to U.S. energy interests, exposing attack points for adversarial cyber operations at virtually all positions along the energy supply chain. In particular, the energy sector must fortify its industrial control systems and supervisory control and data acquisition control systems (ICS/SCADA) to prevent unauthorized access and limit the scope of potential disruptions. Moreover, the May 2021 ransomware attack against Colonial Pipeline, which the Federal Bureau of Investigation attributed to the Darkside cyber-criminal group, showed why software supply chain risk management, strong cybersecurity incident practices and well-prepared contingency plans are also critical for administrative and business networks that drive the energy supply chain.

Securing the Information Communications Technology (ICT) supply chain is essential to protecting the integrity required to clearly understand where potential vulnerabilities lie in the energy supply chain. ICS/SCADA systems allow the convergence of information technology (IT) and operational technologies (OT), which offer great efficiencies as well as associated risks. However, employing ICT supply chain security best practices like a software bill of materials (SBOM), offer rapid identification of significant vulnerabilities such as the Log4shell exploit or the SolarWinds Orion software supply chain attack that could disrupt the energy supply chain. Thus, protecting the ICT supply chain is essential to protecting all other critical supply chains, including the energy supply chain.

Although U.S. energy supply chains face multiple risks, these challenges also offer corresponding opportunities to fortify and improve U.S. energy capacity, efficiency, and resiliency. DOE’s one-year review offers strategic policies as well as commercial planning that will ensure U.S. energy supply chains are robust and secure while supporting commitments for a brighter, cleaner future.

NOTE: This NCSC Supply Chain Spotlight summarizes relevant information from the subject report to highlight CI and security issues. Please review the report in full to understand all supply chain risks identified by the authoring department. https://www.energy.gov/policy/supplychains