U.S. DEPARTMENT OF ENERGY

Achieving American Leadership in Cybersecurity and Digital Components

Summary

The Biden Administration's efforts to meet 100% clean electricity by 2035 and net-zero greenhouse gas emissions by 2050 has created opportunities to rebuildAmerican supply chains create new jobs, strengthen community engagement, and spur U.S. economic growth. DOE's strategy for success in the transition to a clean energy economy hinges on building and maintaining technology supply chains that are advanced, secure, and resilient to cyber threats.

As the energy sector grows increasingly globalized, complex, and digitized, the supply chain for digital components of energy systems – including software, virtual platforms and services, and data – is facing greater threats. Nearly all digital components of U.S. energy sector systems are vulnerable to cyber supply chain instability, stemming from a variety of causes and shared among a broad set of interdependent stakeholders. Overall, supply chain risks for digital components in energy sector systems will continue to evolve and likely increase as these systems are increasingly interconnected, digitized, and remotely operated.

Key Findings and Opportunities

Energy Sector Supply Chain Risks are Growing:

Increasingly sophisticated cyber adversaries have targeted and exploited vulnerabilities in digital assets across energy sector systems. Key cyber vulnerabilities include reliance on untrusted foreign suppliers and software developers; reliance on opaque and highly dynamic global supply chains for digital goods and services; high and often unrecognized reliance on certain ubiquitous key digital components in energy sector systems that have the potential for cascading effects if concurrently compromised; and fragmentation and inconsistent oversight of interdependent cyber supply chains. Major cyber threats include national security threats from adversary nations with sophisticated intelligence collection and cyber capabilities and threats from criminal actors employing supply chain attacks similar to the SolarWinds supply chain attack in 2020.

Mitigating Future Vulnerabilities - Digitalization, Decentralization, Decarbonization:

Cyber supply chain risks for legacy systems will continue to be a concern that requires active and holistic management and mitigation. As new technologies like renewables and distributed energy systems are introduced, and operational efficiencies, including the use of virtual platforms and Artificial intelligence and machine learning (AI/ML) technologies are increasingly pursued, there is an opportunity to ensure that the supply chains for these digital assets are developed with cybersecurity in mind.

Securing Distributed Energy Resource Management Systems and Endpoint Devices:

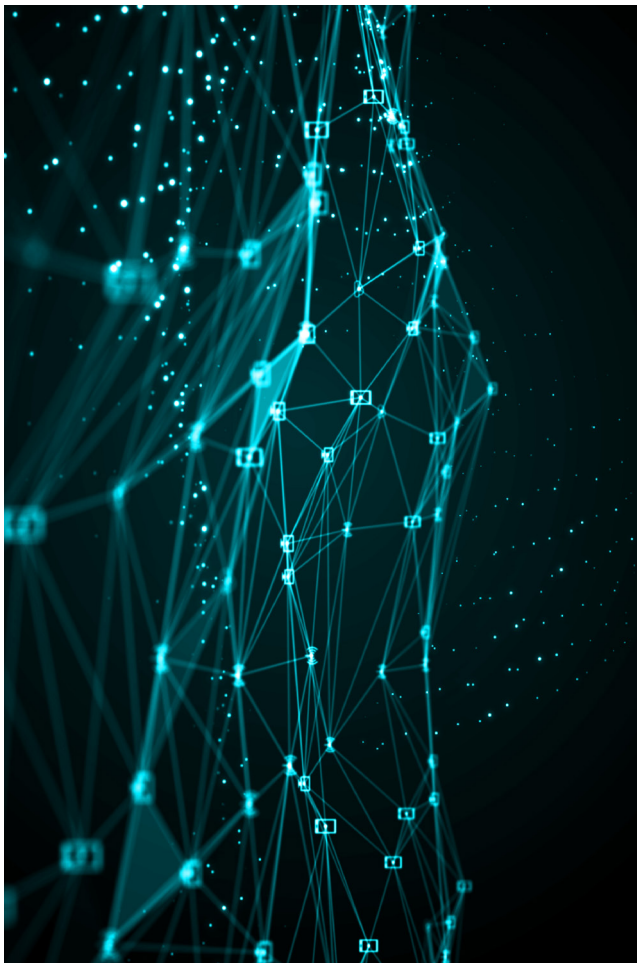
As the grid is modernized and decarbonized, increasing numbers of endpoint devices – like consumer electric vehicle chargers – will be connected to the grid. Proactive security investments must be made to ensure the integrity of the cyber supply chain for firmware on connected devices and the software systems used to connect and manage them. Emerging technologies that support the energy sector should be developed with approaches to illuminate the risk of sub-tier suppliers in mind.

Securing Virtual Platforms:

The efficiency-driven trend towards more flexible operation of industrial control systems (ICS) will continue. Consequently, the security of third party-hosted virtual platforms and virtual services provided to the energy sector by the ESIB will become an increasingly important cyber supply chain risk to manage. Modern technology architectures should reflect principles of Cyber-Informed Engineering (security-by-design), not just in the systems themselves, but also in the digital supply chains that support them.

Boosting Cybersecurity for High-Integrity Data:

Artificial intelligence and machine learning are emerging technologies critical to the current and future national and economic security of the United States. Data is the key raw ingredient for AI/ML, and the ever-larger datasets needed to fuel AI/ML are impractical to move. This data presents a cyber supply chain risk similar to that posed by software. With the increasing application of AI/ML capabilities to the operation and defense of U.S. energy sector systems, and the centrality of DOE AI/ML research and development efforts (at DOE National Laboratories) to national and economic security, a proactive approach to ensuring cybersecurity and integrity of the global supply chain for data is critical.



Policy Next Steps

To boost cybersecurity of digital components, virtual platforms, and data, policy strategies and next steps are included in the report, America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition. A high-level summary is included below.

Improve Data and Analytic Capabilities:

To understand current and emerging supply chain threats, risks, vulnerabilities, and opportunities, it is important to have access to supply chain data and analytical tools for decision support in improving and maintaining resilient digital supply chains. Current information and analytical tools are fragmented, inconsistent, and incomplete. Comprehensive and normalized data are fundamental to illuminating, analyzing, and baselining systemic digital supply chain risks, as well as tracking progress. DOE will partner with other federal agencies to develop an ESIB Database and analytical decision modeling capabilities.

Develop a Secure Digital Component Supply Chain Strategy:

Because cyber supply chain risks are shared among interconnected energy systems, a more holistic approach is needed to effectively increase resilience and digital supply chain security. Engaging government and private sector stakeholders to develop a strategic approach will enable key ESIB-wide functions, including defining and prioritizing critical digital supply chains; baselining and defining goals; and planning for changes anticipated as the drive to modernize and decarbonize the grid accelerates.

Update Oversight and Guidelines:

Developing more cohesive policies and consistent guidelines, standards, and processes to manage shared cybersecurity risks for the ESIB will help improve the fragmented and inconsistent oversight of supply chain risks for digital components in critical energy systems. Leveraging and building upon existing standards and emerging guidelines such as those identified in E.O. 14028 "Improving the Nation's Cybersecurity," in partnership with key government and ESIB stakeholders, will improve ESIB-wide consistency. ■

Download the full document and the corresponding other documents that are part of the DOE response to the supply chain executive order at: www.energy.gov/policy/supplychains