Panel II: Managing Cyber Security Threats, the CIP Reliability Standards, and Best Practices for the Bulk-Power System

Testimony by Bob Kolasky, Senior Vice President for Critical Infrastructure, Exiger

A growing concern within the energy industry and government is that Bulk Energy Suppliers (BES) are vulnerable to sabotage of their components. Cyber supply chain exploitation by foreign adversaries threatens U.S. critical energy infrastructure, with the U.S. especially vulnerable because it has historically sourced key BES componentry from international suppliers, including China. It is vital for energy sector asset owners and associated vendors to identify, assess, and mitigate supply chain relationships that pose risks.

The risk picture

Cyber risk from sub-tier suppliers can arise from information technology and operations technology (OT). Many, if not all, OT components have built-in smart devices that offer real-time diagnostics to provide feedback on the components' production and efficiency. It is possible that when creating these components, foreign governments could insert backdoors into hardware or software equipment, or they could make use of "bugdoors," which are vulnerabilities created during coding that a government forces the manufacturer to keep in place for exploitation. For example, in 2015, certain U.S. companies determined that hardware backdoors, which were not included in any original product design, had been embedded into hardware components manufactured by circuitry subcontractors based in China.

Counterfeit components can also make their way into distribution channels and degrade system performance and present cyber risk. Maintenance and repair activities — software upgrades, hardware replacements, or equipment services, whether done onsite or remotely — also create an opportunity to corrupt or compromise systems, which can have grave national security implications. Additionally, manufacturers and developers can potentially include unauthorized code or malware in the industrial control system devices that allow the program to "call home" once installed. Capable adversaries could gather useful information on the types of equipment used at a facility in order to undermine security controls. As noted by the Midwest Reliability Organization, there is also increased risk if, within an organization, "project timelines and operational needs reduce allotted time for device vulnerability assessments, and if procurement practices do not adequately consider and weight security factors and vetting."

In the last few years the U.S. has faced multiple attacks to its energy sector, although these have not all been specific to the supply chain. This is particularly true through OT-attack vectors. For example, my former colleagues at CISA, working with the FBI and DOE, found that from 2011-2018 that the Russian FSB conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.

Risk mitigation challenges

Despite the numerous foreign ownership and control (FOCI) cyber risks facing the energy sector, the industry is still grappling with the creation of compliance controls or standardized governance processes among businesses and vendors to address these risks or potential supply chain risks from

sub-tier suppliers, with the exception of Office of Foreign Assets Control (OFAC) sanctions compliance programs and NERC Critical Infrastructure Protection (CIP) requirements, which impose physical controls, incident reporting and cybersecurity requirements on businesses and vendors. As a result, the BPS industry's assessment and management of sub-tier vendors varies greatly. Sub-tier vendor governance by transmission and generation providers is bespoke, inconsistent and dependent on multiple factors; these factors include the providers' business size, or model and supply needs.

The lack of standardized governance may be surprising considering the multiple Reliability Standards that have been adopted to mitigate supply chain risk. Indeed, over the last five years, a substantial volume of regulatory requirements, guidance and best practices have emerged to address the supply chain risk of the BPS industry. These resources contemplate nuanced and robust cybersecurity risk practices. However, the Reliability Standards (and other resources) relate specifically to cyber intrusions, including cyber-attacks, unauthorized physical or logical access to systems, or the introduction of malware that could affect the reliable operation of the BPS. Any governance that exists for vendor management does not focus on managing internal threats or sub-tier vendors, or only touches on these issues, leaving a gap that can create enormous vulnerabilities for the BPS industry.

The Federal Energy Regulatory Commission (FERC) Order No. 829, which directed NERC to establish the supply chain risk management Reliability Standards, for example, addressed the following primary security objectives: 1) Software integrity and authenticity; 2) Vendor remote access; 3) Information systems and planning; 4) Vendor risk management and procurement controls.

Although the order lists vendor risk management as the fourth objective of the requested Reliability Standards, it specifically states that the "cyber threat landscape, exemplified by recent malware campaigns targeting supply chain vendors, have highlighted a gap in the Critical Infrastructure Protection," emphasizing the requirement to establish controls that protect asset owners and vendors from external malware or malicious software and ensuring that vendors are assessed for cyber preparedness. The order mentioned external malware and malicious software threats almost 30 times as the impetus for the directive. Internal threats to sub-tier vendors were not mentioned at all. Similarly, Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1, approved through FERC Order No. 850, focused almost exclusively on cybersecurity preparedness of the supply chain, electronic security perimeters, and cyber security change management and vulnerability assessments. Thus, these Reliability Standards were not designed to mitigate the risk of an adversarial vendor, intentional sabotage by a direct or sub-tier vendor, or activity directed by a state-actor with control or influence over a direct contractor or sub-tier vendors. Nor did they envision a holistic assessment of the reliability, conduct, adversarial control or influence, or financial duress of the vendors working for BPS asset owners, much less comprehensive due diligence two or three tiers down the supply chain.

Toward a path forward

As a starting point to addressing foreign-ownership related cyber risks, the BPS industry should consider leveraging existing procurement guidance. DOE guidance can be used to formulate enhanced contract language or procurement guidance to reveal and mitigate supply chain vulnerabilities.

Edison Electric Institute (EEI) has also played a valuable role in addressing the procurement language requirements of effectively implementing the CIP-013-1 Reliability Standard and published suggested language in May 2020. This language does not address all of the core supply chain risks, but it serves as an initial framework for mitigating risks related to sub-tier vendors.

Additionally, the BPS industry could leverage and enhance existing third-party risk management best practices as guidance. These include assessing risk against a multitude of factors to include sanctions, cyber protection, export control failings, anti-bribery, anti-corruption policies and State ownership.

Furthermore, the industry should be:

- Identifying sub-tier parties related to critical or logic bearing componentry;
- Reviewing procurement documentation;
- Identifying and clarifying, as appropriate, political connections identified regarding the subjects and any inappropriate use of those political connections;
- Identifying and providing insight into any corruption or bribery allegations against the subjects;
- Developing information regarding the history, track record, and reputation of the subjects; Gaining details and insight on the company's business activities and sectoral reputation;
- Identifying and assessing adverse information about the company's performance, including any allegations of corruption or financial malfeasance by its management;
- Identifying the operational and financial stability of the supplier;
- Assessing the potential for the supplier to be intentionally or unintentionally subject to counterfeit products;
- Identifying undisclosed material interests or activities prejudicing commercial conduct; and
- Identifying potential corporate governance or ethical issues.

Using the factors previously described, entities should conduct an initial third-party/vendor risk assessment targeting FOCI risk to identify FOCI exposure in their supply chain and to understand what, if any, controls are either in place, or could be introduced, to mitigate that specific risk. In some cases, to ensure that they are adequately addressing their risks, energy sector businesses should consider retaining a third-party consultant to examine existing compliance programs and related security systems, and to identify whether the current environment requires augmenting the existing infrastructure or developing a new compliance program.

Following a completed risk assessment and final report of an entity's needs for any specific compliance program, controls should be documented in existing or new policies and procedures, and enhanced as necessary, with periodic testing to assure that they are operating as intended. In many cases, the entity will retain a third-party consultant to develop these recommended policies and procedures and/or to enhance existing compliance documents.

Resource considerations

The resources that entities must commit to meet new regulatory requirements can be substantial and require creative, thoughtful solutions that must embrace technological advances. Many supply chain vulnerabilities arise through a lack of transparency within the third-party network of a power supplier, where a vulnerability in a compromised or high-risk second-tier supplier or original

equipment manufacturer becomes a national security vulnerability when incorporated into the bulk power supply chain.

Conducting the type of control implementation, particularly the due diligence described herein, on potentially thousands of vendors, for example, could create an onerous burden for the energy industry. Some of the largest U.S. utilities have more than 10,000 suppliers and sub-tier vendors, meaning that annual costs could run into the hundreds of thousands or even millions of dollars, depending on the frequency of procurement of sensitive BPS equipment and an affected entity's risk threshold for requiring the performance of enhanced due diligence on given suppliers, especially small businesses. But, much of this due diligence has been automated through artificial intelligence in the last five years. It would therefore be less costly to implement and sustain than in the past, significantly reducing the economic burden of potential regulation.

Resource challenges could be particularly acute for small businesses, including the need for additional staffing to execute, assure, and monitor compliance. Small businesses may also lack bargaining power to demand vendors agree to specific contract terms if renegotiations are necessary in light of regulatory burdens. Under these circumstances, it will be especially important that the regulations encourage small businesses to apply a risk-based approach where appropriate, making the burden of compliance proportionate to the magnitude of the risk faced.

Information sharing solutions may also help small businesses. The industry has existing information sharing mechanisms that could be models for a collaborative hardening of the BPS. Practice guides, questionnaires, reference documents, and common standards can be all shared with the market. NERC has also established a Supply Chain Working Group overseen by the Reliability and Security Technical Committee, a working group of technical and operational experts that is a central coordination point across NERC, industry groups, and federal government agencies for supply chain risk management issues. The Electricity Information Sharing and Analysis Center (E-ISAC) is also a central hub for cyber risk and physical threat management, providing an existing bi-directional platform for sharing critical risks and guidance

Conclusion

Over the last few years, there has been heightened awareness and increased concern by federal officials of foreign influences on critical U.S. sectors, including the energy industry, and their impact on cyber risks. Any disruptions to — or attacks on — the BPS can have wide-reaching consequences for the entire nation. The disabling of only a very small number of generators or substations could result in widespread power loss and disruption. Although additional regulatory guidance will naturally pose challenges to the U.S. energy sector, it also presents an invaluable and long overdue opportunity to bolster the nation's defenses against foreign adversaries' sabotage or subversion of our critical electricity infrastructure — which could prove catastrophic to our national security and way of life.