CIP Supply Chain Risk Management (RM15-14-000)
Statement of Jacob S. Olcott
Vice President, BitSight Technologies
January 28, 2016

My name is Jacob Olcott and I am pleased to share some observations on the critical topic of supply chain risk management.

By way of background, I have spent more than a decade working on cybersecurity policy issues affecting the electric grid, including supply chain security. I am currently a vice president with BitSight Technologies, a company that provides cybersecurity ratings to organizations for the purposes of supply chain and third party risk management. From 2005-2011, I served as legal advisor to the Chairmen of the Senate Commerce Committee (Sen. John D. Rockefeller, IV) and House of Representatives Homeland Security Committee (Rep. Bennie G. Thompson), where I worked closely with FERC and NERC staff, bulk power system owners and operators, technology vendors, trade associations, and other key participants to enhance the cybersecurity and resiliency of the bulk power system. From 2011-2014, I consulted with corporate executives on cybersecurity issues affecting their businesses, including with bulk power system owners/operators on supply chain risk management. I authored a paper in 2012, *Confronting Cyber Risk in Critical Infrastructure*, describing key supply chain practices for critical infrastructure owners/operators.

(1) Attacks targeting the supply chain are on the rise, particularly attacks targeting third party service providers.

Generally speaking, supply chain attacks can target either (1) the hardware/software components of a system (thereby creating vulnerabilities that can be exploited by a remote attacker); or (2) a third party service provider who has access to sensitive IT infrastructure or holds/maintains sensitive data. Congressional investigators, regulators, and the media have all highlighted the risk that a malicious actors can insert vulnerabilities into hardware and software at virtually any point in a product's lifecycle. Recent news reports from December 2015 about unauthorized code found in Juniper Networks' software only reaffirm this risk vector. But threat actors are also increasingly targeting an organization's third party service providers - business associates, contractors, and others - in order to obtain sensitive business information or direct access to the first party's information systems.

There is perhaps no more famous supply chain incident highlighting the risk to third party service providers than the 2013 Target breach. In that incident, attackers penetrated the network of Target's HVAC contractor, who had a direct connection into Target's network in order to observe refrigeration units in each of the stores. Gaining access to the HVAC contractor, and exploiting the contractor's privileged access, the attackers rode directly into the Target network and stole millions of credit card numbers. The result was not only a material financial loss for

Target, but also the ousting of Target's CEO, CIO, and near dismissal of several key board members.

Target is just one of a number of organizations that have experienced this type of supply chain breach. T-Mobile, Lowe's, Goodwill, and other retailers have also been victimized through their third parties. And it's not just retailers. The 2015 Office of Personnel Management (OPM) data breach that compromised the data of millions of federal employees began with the theft of OPM credentials from third party business associates. These credentials were then used to gain access to OPM data stored on (yet another) third party server maintained by the Department of Interior.

By now, electric utility organizations are well aware of cyber attacks targeting their own third party supply chain partners. Two attacks in recent years have specifically targeted IT vendors and service providers. In 2012, an industrial automation company disclosed that attackers installed malicious software and stole project files related to one of its SCADA offerings. Though public reports indicated that intellectual property was the target of the attack, the company also advised its customers at the time that it was temporarily disconnecting the links between its organization and customers while the data breach was being assessed. This precaution was taken in order to provide assurance that their compromised systems could not be leveraged to gain direct access to electric sector organizations. In another example, in 2014, an Independent System Operator reported a breach in a third party market monitor, compromising certain sensitive operating cost data for industry participants. The Independent System Operator severed connections between the breached party's information systems.

(2) Regulators in other sectors are focusing on cyber supply chain risk management guidelines for their regulated entities.

Growing concern over supply chain cybersecurity risk has increased involvement by a variety of regulating organizations, including regulators in the financial, defense, health care, retail, and consumer data sectors, which have all adopted requirements or guidance for supply chain risk management. Generally speaking, most regulations clarify the "critical" data or services that are to be protected, the contracting, diligence, and assessment processes that should be implemented, and the duty for the organization to monitor the efforts of its third parties to implement the agreed-upon security requirements.

- In the financial sector, financial institutions are required by various laws and regulations to manage third party risk. Standards have been developed by federal and state financial regulators, including the Office of Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Securities and Exchange Commission. These standards generally require that financial institutions develop vendor risk management programs to ensure that their critical third party vendors are implementing security measures and perform "ongoing monitoring" of those efforts. These vendor risk management guidelines cover the full lifecycle of the process, from performing diligence in a pre-selection stage to contract negotiations to contract implementation.

- In the defense sector, defense industrial base companies holding “unclassified controlled technical information” are now required under a new Defense Federal Acquisition Regulation to manage the risk to this data throughout the supply chain. Defense companies who subcontract with third parties that have access to this type of information are required to create contractual mechanisms to ensure that these third parties are implementing appropriate security measures (typically NIST-aligned practices) and report any security incidents to both the prime contractor and the Department of Defense.

- In the retail sector, third party service providers who have access to cardholder data or the cardholder data environment are now required to be compliant with the PCI Data Security Standards established by the PCI Security Standards Council. There are countless third parties that provide services related to cardholder data, including payment gateways, payment processors, managed services, application hosting, and others. The PCI security requirements obligate retailers to perform due diligence over third parties prior to entering into a business relationship in order to understand how the third party’s security efforts meet the PCI requirements, establish written contractual agreements describing responsibilities and obligations, and monitor third party service providers for compliance with the PCI standards.

- In the health care sector, the Health Information Portability and Accountability Act (HIPAA) and HITECH Act both regulate the use and disclosure of “protected health information” held by health care organizations (known as “covered entities”). These laws also require the protection of health data by any third party service providers working on behalf of the covered entities (known as “business associates”). Covered entities are required to obtain satisfactory assurances that their business associates will use protected health information for limited purposes and will safeguard the information from misuse. A covered entity can be held liable for the acts or omissions of its business associates, including the subcontractors of business associates.

- For organizations handling sensitive consumer information, the Federal Trade Commission has settled several cases which establish general guidelines and practices governing the relationship that businesses should have with their third party service providers. Among the best practices the FTC suggests include being clear and candid about security expectations with third parties (including through contract), taking reasonable steps to select providers who are capable of implementing appropriate security measures, and monitoring/overseeing third parties to ensure that they are meeting the established expectations.

(3) Identifying “critical” third parties for an owner/operator in the bulk power system is an important task that requires input from across the organization and a broad definition of “criticality.”

Cyber risk management has become a whole-of-organization initiative, involving board members, senior executives, and representatives from across the business, including IT, legal, business units, human resources, and acquisition/procurement. Given the cross-cutting analyses that must take place to identify “critical” third parties, supply chain risk management also requires a cross-functional approach. Legal, IT, and procurement all work together to (1) identify and locate the organization’s most critical data or third party connections that could be leveraged to gain unauthorized access into the organization’s systems; and (2) establish the appropriate standards for business partners to meet, develop contract language that binds partners to those standards, and audit/assess the implementation of those standards by business partners.

For owners and operators of the bulk power system, “critical” third parties are those who provide information technology, information communications technology, and/or industrial control systems critical for the operation of the bulk power system, as well as those third parties who maintain connectivity/access to critical bulk power system networks. This is not a trivial assessment. The broad migration of energy systems onto Internet Protocol-based platforms and extensive interconnectivity between IT, ICT, and ICS technologies in the average bulk power system environment, makes the criticality determination an important and significant undertaking.

Furthermore, “critical” vendors in the bulk power system are also those who hold or maintain sensitive bulk power system data. As observed in the attack against the industrial automation company or the data provider to the Independent System Operator, malicious actors target third parties because of the data that they keep about sensitive designs, blueprints, and data relevant to the operations of the bulk power system. If compromised, these critical third parties could provide a roadmap for an attacker to carry out a successful campaign against bulk power system owners and operators. As a consultant, it was not unusual to find a host of organizations who were able to maintain sensitive design information, configuration, use, access control, or other security-sensitive information.

It is crucial for any supply chain security standard to thoroughly address the criticality calculus, including for IT/ICT/ICS vendors as well as the third parties who may pose significant risk to the bulk power system due to their access to sensitive business data.

(4) Methods to assess and continuously monitor cyber risk from third parties are rapidly evolving.

To drive better cybersecurity among critical third party software, hardware, and service providers, organizations use a combination of contractual mechanisms and assessment tools. As supply chain breaches continue to challenge traditional approaches (e.g. questionnaires, document reviews, occasional assessments), organizations are adopting new tools to enhance cybersecurity among critical third parties.

Traditionally, businesses assessed the cybersecurity posture of third parties through questionnaires, review of audits/assessments and other documentation, and the occasional on-site security assessment. To do so, many organizations utilize their procurement and acquisition processes to include requirements that third parties incorporate security into the software development lifecycle, or that third parties implement certain controls to protect their organizations. Sometimes, organizations ask their partners to meet industry-specific standards or best practices (e.g. ISO 27001, the Payment Card Industry data security standards, SOC2, NIST 800-53, SANS Top 20, BSIMM, the Open Trusted Technology Provider standard, the NIST Cybersecurity Framework). Some organizations may describe specific security practices that they want their business partners to follow (e.g. encrypting data, annual penetration testing, mandatory code scanning). For purposes of managing supply chain risk to the bulk power system, the Department of Energy's April 2014 "Cybersecurity Procurement Language for Energy Delivery Systems" provides an excellent overview of elements that bulk power system owners and operators should consider including in procurement language. Among the best practices recommended in this document include provisions allowing for the inspection of documentation regarding a business associate's implemented cybersecurity program and recent assessment results, a periodic on-site assessment performed by the customer (or a designee), and the disclosure of breaches involving the third party's organization or an element of the product's supply chain which may result in the loss of sensitive design information, configuration, use, access control, or other security-sensitive information.

Building security into the underlying contractual relationship between customer and third party is a critical way of driving better cybersecurity. But verifying or validating the security initiatives used by third parties can present significant challenges. Though it is a best practice to request evidence of a business partners' compliance with security standards or practices, partners may not always comply. For instance, it was recently revealed that health insurer Anthem prevented some of its customers from learning information about its security program prior to their massive data breach in 2015.

Many organizations now seek to "trust but verify" the security initiatives that their business partners are implementing. On the software assurance side, scanning and testing third party applications is now a common approach towards reducing vulnerabilities in third party code and there are a growing number of third party providers who perform these assessments on behalf of customers. When it comes to assessing the cybersecurity posture of third party service providers, many organizations want to monitor their business partners' security in real time. Companies like BitSight Technologies can provide continuous, daily ratings of the security posture of vendors based on externally-observable security incidents. This allows companies to gain a better understanding of their business partners' security posture and work with their partners to alleviate security issues in real-time. Hundreds of organizations, including bulk power system owners and operators, use BitSight and our ratings platform to continuously monitor their supply chain partners. BitSight produces an annual industry benchmarking report - BitSight "Insights" - highlighting our general findings about the state of security of various sectors, including the electric grid. This report and others is available at our website, https://info.bitsighttech.com/bitsight-insight-energy-utilities-risk-major-breach.

As FERC considers adopting new supply chain risk management standards, it will be important to highlight and emphasize initiatives that are focused on quantitative, continuous risk management rather than subjective "check the box" compliance activities. Knowledge and awareness of the rapidly developing and emerging market for continuous monitoring solutions for third party vendors in the supply chain would be beneficial for regulators as they consider adoption and enforcement of any new CIP standards.

Conclusion

Supply chain risk management is a critical initiative for any bulk power system owner and operator. Effective supply chain risk management requires assessing the risk from critical software and hardware vendors, but also the service providers who maintain access to sensitive data as well as the corporate network. To drive better cyber risk management throughout the supply chain, a combination of procurement language, assessment tools, and monitoring technologies are available to owners and operators of the bulk power system.

FERC plays a critical role in improving supply chain risk management for the bulk power system. Fortunately, many regulators have adopted approaches in recent years that FERC and the electric industry as a whole can look to for guidance. Of critical importance is that any new CIP requirement be focused on risk management and not be viewed as a simple compliance exercise. History suggests us that when it comes to managing risk from the supply chain, there is no simple solution.