E 6717-01-P

DEPARTMENT OF ENERGY
Federal Energy Regulatory Commission
[Docket No. AD22-12-000]

Joint FERC-DOE Supply Chain Risk Management Technical Conference; Notice Inviting Post-Technical Conference Comments

On Wednesday, December 7, 2022, the Federal Energy Regulatory Commission (Commission) and the U.S. Department of Energy (DOE) convened a Joint Supply Chain Risk Management Technical Conference to discuss supply chain security challenges related to the Bulk-Power System, ongoing supply chain-related activities, and potential measures to secure the supply chain for the grid's hardware, software, computer, and networking equipment.

All interested persons are invited to file post-technical conference comments to address issues raised during the technical conference identified in the Supplemental Notice of Technical Conference issued on December 6, 2022. For reference, the questions included in the Supplemental Notice are included below. Commenters need not answer all of the questions, but are encouraged to organize responses using the numbering and order in the below questions. Commenters are also invited to reference material previously filed in this docket but are encouraged to avoid repetition or replication of their previous comments. Comments must be submitted on or before **60 days** from the date of this Notice.

Comments, identified by docket number, may be filed electronically or paper-filed. Electronic filing through https://www.ferc.gov is preferred. Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format. Instructions are available on the Commission's website: http://www.ferc.gov/docs-filing/efiling.asp.

Although the Commission strongly encourages electronic filing, documents may also be paper-filed. To paper-file, submissions sent via the U.S. Postal Service must be addressed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street NE, Washington, DC 20426. Submissions sent via any other carrier must be addressed to:

Federal Energy Regulatory Commission
Office of the Secretary
12225 Wilkins Avenue
Rockville, Maryland 20852.

For more information about this Notice, please contact:

Simon Slobodnik (Technical Information)
Office of Energy Reliability
(202) 502-6707
Simon.Slobodnik@ferc.gov

Alan J. Rukin (Legal Information)
Office of General Counsel
(202) 502-8502
Alan.Rukin@ferc.gov

Dated: December 19, 2022.

Debbie-Anne A. Reese,
Deputy Secretary.

POST TECHNICAL CONFERENCE QUESTIONS

I. Supply Chain Risks Facing the Bulk-Power System

The U.S. energy sector procures products and services from a globally distributed, highly complex, and increasingly interconnected set of supply chains. Information Technology (IT) and Operational Technology (OT) systems enable increased interconnectivity, process automation, and remote control. As a result, supply chain risks will continue to evolve and likely increase. This panel discussed the state of supply chain risks from a national and geopolitical perspective. Specifically, the panel explored current supply chain risks to the security of grid's hardware, software, computer, and networking equipment and how well-resourced campaigns perpetrated by nation states, such as the SolarWinds incident, affect supply chain risk for the electric sector. Panelists discussed the origins of these risks, their pervasiveness, the possible impacts they could have on Bulk-Power System reliability, and approaches to mitigating them. The panelists also discussed challenges associated with supply chain visibility and covert embedded spyware or other compromising software or hardware in suppliers' products, parts, or services.

Please address the following questions:

1. Describe the types of challenges and risks associated with globally distributed, highly complex, and increasingly interconnected supply chains.
2. Describe the difficulties associated with supply chain visibility and how origins of products or components may be obscured.
3. How are foreign-supplied Bulk-Power System components being manipulated and is there a particular phase in the product lifecycle where the product is manipulated for nefarious intent?
4. How are these supply chain challenges and risks currently being managed?
5. How has the current geopolitical landscape impacted the energy sector's ability to manage supply chain challenges and risks?
6. How can Sector Risk Management Agencies and Regulators promote and/or incentivize supply chain transparency at the earlier stages of product development and manufacturing?
7. Discuss the pathways (e.g., voluntary best practices and guidelines, mandatory standards) that together could address the current supply chain challenges and risks?
8. What actions can government take, both formal regulatory actions and coordination, to help identify and mitigate risks from the global supply chain for the energy sector?

II. Current Supply Chain Risk Management (SCRM) Reliability Standards, Implementation Challenges, Gaps, and Opportunities for Improvement

It has now been more than six years since the Commission directed the development of mandatory Reliability Standards to address supply chain risks, and more than two years since the first set of those tandards became effective.1 As discussed in Panel 1, supply chain risks have continued to grow in that time. In light of that evolving threat, panelists discussed the existing SCRM Reliability Standards, including: (1) their effectiveness in securing the Bulk-Power System; (2) lessons learned from implementation of the current SCRM Reliability Standards; and (3) possible gaps in the currently effective SCRM Reliability Standards. This panel provided an opportunity to discuss any Reliability Standards in development, and how these new standards will help enhance security and help address some of the emerging supply chain threats.

Please address the following questions:

1. Are the currently effective SCRM Reliability Standards sufficient to successfully ensure Bulk-Power System reliability and security in light of existing and emerging risks?
2. What requirements in the SCRM Reliability Standards present implementation challenges for registered entities and for vendors?
3. How are implementation challenges being addressed for utilities and for vendors?
4. Are there alternative methods for implementing the SCRM Reliability Standards that could eliminate challenges or enhance effectiveness moving forward?
5. Based on the current and evolving threat landscape, would the currently effective SCRM Reliability Standards benefit from additional mandatory security control requirements and how would these additional controls improve the security of the Bulk-Power System?
6. Are there currently effective SCRM criteria or standards that manufacturers must adhere to in foreign countries that may be prudent to adopt in the U.S.?

III. The U.S. Department of Energy's Energy Cyber Sense Program

Through the Energy Cyber Sense Program, DOE will provide a comprehensive approach to securing the nation's critical energy infrastructure and supply chains from cyber threats with this voluntary program. The Energy Cyber Sense Program will build upon direction in Section 40122 of the Bipartisan Infrastructure Law, as well as multiple requests from industry, leveraging existing programs and technologies, while also initiating new efforts. Through Energy Cyber Sense, DOE aims to work with

---

[1] The SCRM Reliability Standards include: Reliability Standards CIP-005-7 (Cyber Security — Electronic Security Perimeter(s)), Requirements R2.4, R2.5, R3; CIP-010-4 (Cyber Security — Configuration Change Management and Vulnerability Assessments) Requirement R1.6; CIP-013-2 (Cyber Security - Supply Chain Risk Management).

manufacturers and asset owners to discover, mitigate, and engineer out cyber vulnerabilities in digital components in the Energy Sector Industrial Base critical supply chains. This program will provide a better understanding of the impacts and dependencies of software and systems used in the energy sector; illuminate the digital provenance of subcomponents in energy systems, hardware, and software; apply best-in-class testing to discover and address common mode vulnerabilities; and provide education and awareness, across the sector and the broader supply chain community to optimize management of supply chain risks. This panel discussed specific supply chain risks that Energy Cyber Sense will address, as well as some of the programs and technologies DOE will bring to bear under the program to address the risks.

Please address the following questions:

1. How are emerging orders, standards, and process guidance, such as Executive Order 14017, Executive Order 14028, NIST Special Publication 800-161r1, ISA 62443, Reliability Standard CIP-013-2, and others, changing how we assess our digital supply chain?
2. Given the dependence of OT on application-specific hardware, how could the inclusion and linkage of Hardware Bill of Materials (HBOMs) with Software Bill of Materials (SBOMs) increase our ability to accurately and effectively assess and mitigate supply chain risk? To what degree is this inclusion and linkage of HBOMs with SBOMs taking place today and what steps should be taken to fill any remaining gaps?
3. Given that much of the critical technology used in the energy sector is considered legacy technology, how can manufacturers, vendors, asset owners and operators, aided by the federal government, national laboratories, and other organizations, manage the supply chain risk from legacy technology? How can this risk management be coordinated with newer technologies that are more likely to receive SBOMs, HBOMs, and attestations?
4. Where does testing, for example Cyber Testing for Resilient Industrial Control Systems (CyTRICS) and third-party testing, fit in the universe of "rigorous and predictable mechanisms for ensuring that products function securely, and as intended?"[2]
5. More than ever, developers are building applications on open-source software libraries. How can developers address the risks inherent with open-source software and how can asset owners work with vendors to validate that appropriate open-source risk management measures have been taken?
6. U.S. energy systems have significant dependencies on hardware components, including integrated circuits and semiconductors, most of which are manufactured

---

[2] See Exec. Order No. 14028, 86 Fed. Reg. 26,633, 26,646 (May 12, 2021) (The Executive Order declared that the security of software used by the Federal Government is "vital to the Federal Government's ability to perform its critical functions." The Executive Order further cited a "pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended.")

outside of the US. What tools and technologies are needed to understand the provenance of hardware components used in U.S. energy systems and the risks from foreign manufacture? How will the newly passed CHIPS and Science Act change the risk landscape? What is needed in terms of regulation, standards, and other guidance to strengthen the security of the hardware component supply chain from cyber and other risks?

IV. Enhancing the Supply Chain Security Posture of the Bulk-Power System

This panel discussed forward-looking initiatives that can be used to improve the supply chain security posture of the Bulk-Power System. These initiatives could include vendor accreditation programs, product and service verification, improved internal supply chain security capability, third party services, and private and public partnerships.

Vendor accreditation can be established in various ways. One of the more prominent ways is currently being explored by the North American Transmission Forum through its Supply Chain Security Assessment model and the associated questionnaire.[3] The panel also explored certain programs and practices used by utilities to verify the authenticity and effectiveness of products and services. Internal supply chain security capabilities include hiring people with the appropriate background and knowledge, while also developing relevant skills internally, through training on broad supply chain topics and applying them to the specific needs of the organization. Finally, this panel addressed private and public partnerships on supply chain security and how they can facilitate timely access to information that will help better identify current and future supply chain threats to the Bulk-Power System and best practices to address those risks.

Please address the following questions:

1. What vendor accreditation programs currently exist or are in development? How can entities vet a vendor in the absence of a vendor accreditation program?
2. What are the challenges, benefits, and risks associated with utilizing third-party services for maintaining a supply chain risk management program?
3. What are the best practices and other guidance for security evaluation of vendors?
4. What programs and practices are currently in use to ensure product and service integrity?
5. What processes are used to test products prior to implementation?
6. What is the right balance between vendor and product security and cost? Is there a point of diminishing returns?
7. What are effective strategies for recruiting personnel with the appropriate background and SCRM skills to strengthen internal security practices? How do you provide the

[3] North American Transmission Forum, *Supply Chain Cyber Security Industry Coordination*, https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

training necessary to further develop the skills specific to your unique organizational challenges?

8. What are the best ways to meaningfully assimilate SBOM information and what subsequent analyses can be done to strengthen internal security practices?
9. How can the industry keep informed of the latest supply chain compromises? How do entities currently respond to these compromises to keep their systems secure? Are there ways to improve these responses? What actions can government take, both formal regulatory actions and coordination, to help keep industry informed of supply chain compromises and to facilitate effective responses?
10. What key risk factors do entities need to consider prior to leveraging third party services and how should those risk factors be balanced with an entity's organizational policy? What SCRM controls do you have in place to ensure your systems and products have a reduced risk of compromise? Please discuss any challenges that you have experienced as well as successes.
11. How should government and industry prioritize and coordinate federal cross-agency and private sector collaboration and activities regarding SCRM?

[FR Doc. 2022-27965 Filed: 12/22/2022 8:45 am; Publication Date: 12/23/2022]