Prepared Remarks for FERC Technical Conference on Supply Chain Risk Management

(Docket No. RM15-14-000)

Nadya Bartol

Vice President, Industry Affairs and Cybersecurity Strategist

Utilities Telecom Council (UTC)

Good morning and thank you for the opportunity to participate in this important initiative.

Managing cybersecurity risks in supply chains has emerged as a challenge relatively recently. The US electric utility industry comes to this challenge well-served by a comprehensive set of standards that address cyber supply chain risks under the control of the registered entities. And while NERC CIP Versions 5/6 standards do not cover supplier processes, FERC noted in the NOPR in this proceeding that "[a] reliability standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities."

Cyber supply chain risk management is a relatively young discipline. However, there are a remarkable number of available standards, guidelines, best practices, and similar materials. These include:

- A four-part international standard on information security in supplier relationships, ISO/IEC 27036, that addresses general security requirements in any procurement, security guidelines for ICT supply chain security, and security guidelines for security of cloud services.
- A special publication by the National Institute of Standards and Technology (NIST) on supply chain risk management for federal systems and organizations, NIST SP 800-161.
- An international standard on security program requirements for industrial control systems (ICS) providers, IEC 62443-2-4.
- An international standard that provides guidelines for reducing the risk of counterfeit and taint

(malicious code) in ICT products, ISO/IEC 20243. There is also a certification body that will certify conformance with this standard administered by The Open Group.

- Cybersecurity Procurement Language for Energy Delivery Systems published by the Department of Energy in 2014.
- National Electrical Manufacturers Association (NEMA) Supply Chain Best Practices document.
- Utilities Telecom Council (UTC) Cyber Supply Chain Risk Management for Utilities—Roadmap for Implementation.

This is not a full list. I know we will hear about some of these efforts in more detail later today. Most of these documents reference each other and many of them share the same content DNA.

Challenges

So why are we still challenged and what are the challenges? Cyber supply chain risks evolve continuously, and managing these risks is a shared responsibility between acquirers and suppliers. Many of the practices and processes to address these risks are being implemented within the electric utility ecosystem and across other industries including the US and other governments, IT, communications, and financial services sectors. The challenges are:

1. Limited acquirer influence, visibility, and transparency into what happens upstream in the supplier supply chain.
2. ICT suppliers who assemble and integrate solutions are similarly challenged with influencing their own supply chains. A number of suppliers have successfully implemented robust supply chain risk management processes, but many suppliers have not yet done so.
3. Knowledge of best practice is not uniform across utility and supplier communities.
4. New ICT companies continuously enter the electric utility market. Some of these companies do not have the background in ICT, or the knowledge of how to make or deliver secure ICT.

5. Managing and coordinating supply chain activities is already complex. Adding security requirements should be done carefully to reduce the risks of disruption to the timely delivery of critical products and services, and to reduce negative financial impact to utilities and their customers.

Current Coverage

The current NERC CIP standards provide comprehensive coverage of cyber supply chain risk management activities within the control of the registered entities. This includes supplier personnel with access to utility systems and facilities. Examples of such areas include security awareness and training (CIP-004-5.1 R1 and R2), personnel risk assessments (CIP-004-5.1 R3) with an explicit reference to contractors and service vendors, access management and revocation (CIP-004-5.1 R4 and R5), interactive remote access management (CIP-005-5 R2), visitor control (CIP-006-5 R2), security patch management (CIP-007-5 R2), malicious code prevention (CIP-007-5 R3), system access control (CIP-007-5 R5), configuration change management and monitoring (CIP-010-1 R1 and R2), vulnerability assessments (CIP-010-1 R3), and BES cyber asset reuse and disposal (CIP-011-1 R2).

As I mentioned earlier, the current NERC CIP standards do not address supplier practices because those are outside of FERC's purview. Examples of applicable supplier practices are secure lifecycle, secure development environment, qualifications of supplier personnel, and suppliers' ability to manage cybersecurity risks in their own ICT supply chains. I should note that these practices may be proprietary to how suppliers conduct their business.

Incentivize or inhibit introduction of more secure technology

Current standards encourage the development and implementation of a minimum responsible set of security features, such as multifactor authentication, unique passwords, configuration management and monitoring, and so on. We know from our member organizations (both utilities and utility technology partners) that NERC CIP requirements are discussed during technology procurements. Solutions that facilitate NERC CIP compliance are viewed favorably in the market. However, the current standards do not encourage truly innovative security practices and techniques that go above and beyond NERC CIP requirements. Implementing those practices may constitute a compliance risk, which makes entities reluctant to pursue improved security opportunities.

Possible other approaches

We believe that FERC should refrain from directing development of a new CIP standard to address cyber supply chain risk management. However, FERC can engage in a number of activities to reduce the shared risks and to help facilitate productive dialogue among acquirers and suppliers about effective practices and lessons learned. Specifically FERC could:

- Commission a study that would collect, summarize, and make available to the industry existing standards and guidelines. The study would capture the list of existing standards, guidelines, and best practices, as well as lessons learned from implementing organizations within and outside of the electricity sector, e.g. government, IT, communications, and finance.
- Continue encouraging dialogue on the topic among utilities and suppliers about better solutions.
- Continue convening the industry to hold these important discussions in a structured format (like today) and unstructured format (such as workshops and facilitated discussions).

This is a complex challenge that transcends multiple disciplines and organizational silos. It transcends entire organizations. Collective education and collaborative work across the electric utility ecosystem is required to eventually address this problem.

Thank you.