Prepared Remarks

FERC Technical Conference on Supply Chain Risk Management
(Docket No. RM15-14-000)

Edna Conway
Chief Security Officer, Global Value Chain

Our Overall View:

It is my privilege to be a part of this conversation with each of the experts here today. Thank you for allowing Cisco to join you.

We are all acutely aware of the convergence of Operational Technology and Information Technology. The pure cybersecurity risks that arise from that convergence are not necessarily unique, however, to the electric industry.

Step One is identifying the goal – While chicken vs. egg debates occur over which is the top level domain, risk management or security; a holistic approach makes the answer clear. Security is indeed the top level domain and nothing short of comprehensive security must be the goal. It should include resiliency, privacy, data protection and trustworthiness.

Some recent publications have narrowly focused only on preparedness for an extended operational failure of the Grid, rather than taking a holistic approach to resiliency. We propose that a broader lens must be taken. A lens that goes far beyond preparedness for a failure, when approaching the superset of comprehensive supply chain security in your industry.

Suggestions For An Approach by FERC:

The first next step is to articulate the threats to the goal. Only then can a layered approach to prevention, detection and mitigation efforts against those threats be developed. State the threats and use them as your north star. For the ICT industry (and I propose the electric industry supply chain) these threats are counterfeit, taint, and manipulation and disruption. Let me share the lens through which we view supply chain security risk. It allows for two

complementary but distinct foci. First, a focus on the role of Information and Communication Technology in cyber risk itself. Second, a focus on the full end-to end spectrum of the ICT supply chain.

We believe that FERC would do well to keep both these focus areas in mind as it addresses comprehensive cybersecurity within the industry's supply chain.

We believe that the expansion of the NERC CIP to include a new standard on supply chain risk management is not the optimal path. In fact, imposing a new standard would effectively negate FERC's statement that "the reliability standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities." The inevitable outcome of an imposition on the industry's registered entities would be to perpetuate the "flow down" effect and impact multiple tiers of commercial members of the supply chain, possibly without any tangible additional security or enhanced risk management.

As an alternative, we offer a number of foundational elements which can form a path to addressing this challenge effectively. Let me highlight some of those foundational elements:

- Embracing the goal of retaining a supplier's flexibility to deploy the right security, in the right node of its own supply chain at the right time.

- Deploying the right security in the right node at the right time in a risk-based manner to ensure economic and operational viability.

- Avoiding the pitfall of proliferation of new, albeit well-intended standards, certification or accreditation schemes or guidelines. Leveraging those already in place should allow swifter implementation and broader adoption. These include standards in the NERC CIP today, international standards mentioned by other colleagues, together with standards such as ISO 27001, the NIST cybersecurity framework and ISO 15408 (the Common Criteria).

- Confidentially weighing the existence and robustness of a supplier's own supply chain security and resiliency programs as part of procurement decisions should serve to move the needle more swiftly while still allowing for the proprietary innovation that supplier brings to the table.

Given those foundational elements, the next step is building a flexible security architecture that can be shared and serve as a participation differentiator, across your entire supply chain.

What Could the Security Risk Management Architecture of the Supply Chain Include?

We suggest identifying core domains within the architecture. For us, those include 11 domains
Note: only the Text in yellow will be part of actual stated remarks:

	Domain	Description
1	Security Governance	The security governance domain details requirements for supplier's overall governance strategy to manage supply chain security and compliance related risks by establishing requisite policies, standards and procedures.
2	Security in Manufacturing and Operations	The security in manufacturing and operations domain details requirements that a supplier must meet in their manufacturing and operating procedures in order to protect the company's material assets and IP.
3	Asset Management	The asset management domain details requirements that a supplier must implement for securing IT and manufacturing assets throughout their life cycle.
4	Security Incident Management	The security incident management domain details requirements that a supplier must implement to establish a robust incident management (IM) process that should be followed for activities such as logging, recording and resolving of security incidents and anomalies.
5	Security Service Management	The service management domain details requirements, a) for the delivery of services in accordance with agreed upon delivery timeframes. b) establishing a business continuity plan/program in an event of a service disruption.
6	Security in Logistics and Storage	The security in logistics and storage domain details supplier security requirements that should be followed during storage and distribution of raw materials, inventory and finished goods along the company's supply chain.
7	Physical and Environmental Security	The physical and environmental security domain details requirements that a supplier must design and implement to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm.
8	Personnel Security	The personnel security domain details requirements to ensure that all supplier personnel who have access to any proprietary items and company IP have the required authorizations, training, and contractual agreements including appropriate clearances, if required.
9	Information Protection	The information protection domain details requirements for protection of the company's proprietary data through its lifecycle, such as data classification, handling, cryptographic controls and disposal. It also lists the requirements to be implemented on information systems that store or process the company's IP.

10	**Security Engineering and Architecture**	The security engineering and architecture domain details requirements to be followed during design, development, testing and rollout of products and services to and on behalf of the company.
11	**3rd Tier Partner Security**	The 3rd tier partner security domain details requirements focused on information security controls that must be implemented at downstream suppliers and partner (4th parties, e.g. cloud service providers) in relation to procurement of goods and services.

Leveraging an architecture containing these 11 domains can allow all members of the supply chain to collaborate. FERC's use of existing industry taxonomy, a clear architecture and procurement-based validation methods will ensure both enhanced risk management while permitting the flexibility and innovation essential to our public/private success.