Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management
Docket No. RM15-14-000

Nick Weber, Cyber and Physical Security Auditor
Western Electricity Coordinating Council

January 28, 2016

Good afternoon, my name is Nick Weber; I serve as an auditor on the Western Electricity Coordinating Council Cyber Security Team. I appreciate the opportunity to discuss supply chain concerns related to the Bulk Power System. The goal of my remarks is to provide an overview of current and previous supply chain security initiatives as well as opportunities to build on that work.

Understanding the complex web of suppliers necessary to create many of the components critical to the reliable operation of the Bulk Power System is no easy task. Nevertheless, continued effort to understand and reduce vulnerabilities through this vector is a necessary endeavor.

Procurement and supply chain security is not a new concept; the U.S. Department of Defense has been working on this task for decades. During my own short tenure at the U.S. Department of Homeland Security I was a part of no less than three separate interagency initiatives to address supply chain security and resilience. It is imperative that attributes of previous work be recognized and incorporated in any future standards or guidance to industry. I would like to draw attention to three such bodies of work as well as one anecdotal example of supply chain security success through information sharing.

NIST Special Publication 800-161 identifies the following three types of information communication technology supply chain vulnerabilities:

- The systems/components within the System Development Life Cycle (SDLC) (i.e., being developed and integrated);
- The development and operational environment directly impacting the SDLC; and
- The logistics/delivery environment that transports ICT systems and components (logically or physically).

NIST 800-161 provides guidance to Federal Agencies in identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations. The scope of NIST 800-161 is germane to this discussion as the target audience and devices revolve around federal ICT, not energy delivery systems. While tenets of NIST 800-161 certainly apply, it should not be considered a one size fits all answer to supply chain risk management. Critical infrastructure owners and operators can reference this in developing their own SCRM practices.

The American National Standards Institute (ANSI) has partnered with ASIS International to develop ANSI/ASIS SCRM.1-2014 *Supply Chain Risk Management: A Compilation of Best Practices*. SCRM.1-2014 provides best practices from understanding the supply chain threat landscape through protection and incident response to steady state management and supply chain incident response.

ISO 28000:2007 provides a voluntary set of standards around supply chain security. While the ISO standards provide some excellent steps in securing the supply chain, they do not reflect the restraints of cost nor the ability for a governing body or even the consumer to force adherence to those standards.

Balancing standard requirements and cost is not a new concept within the realm of reliability standards, particularly the CIP standards but is a concern that must continually be addressed. These costs will come both in the form of increased overhead to meet the compliance burden and increased prices from vendors who are unlikely to allow any external requirements to impact their margins.

As an auditor, I am concerned with the ability to effectively oversee and audit a supply chain security standard since the parties with the greatest impact are beyond our reach. This is where understanding of best practices and existing standards should be leveraged to identify where the procuring entity can have the greatest impact on the integrity of their supply chain. Some of those areas might include supply chain mapping, public/private information sharing, and procurement language.

Combining effective supply chain mapping and information sharing, particularly between owner/operators and the Intelligence Community can yield a significant increase in the purchasing entity's awareness and ability to understand risks brought on by specific links in the supply chain. The single best example I've seen of this collaboration occurred during my time at the Department of Homeland Security. During one of our classified briefs to owner/operators an analyst shared a picture of a particular device and asked the audience to come see him after his presentation if they had a similar device in their system as a number of them had been compromised in the development phase.

The Energy Sector Control System Working Group (ESCSWG) developed *Cybersecurity Procurement Language for Energy Delivery Systems* through a public/private partnership with the U.S. Department of Energy and other government agencies in April 2014. This document provides a strong starting place for any discussion of future standards. This document provides sample procurement language for energy companies to leverage when drafting a request for proposal (RFP). Given the limited capability of FERC, NERC, and Regional Entities to provide oversight of vendors and by extension, their supply chains, future reliability standards should focus on the procurement of cyber assets critical to reliability of the Bulk Power System.

Understanding and mitigating supply chain risks is a very complex and time-consuming process that will require a high level of collaboration between Bulk Power System entities, cyber asset vendors, and government agencies.

I’d like to thank the Commission and Commission Staff for providing me the opportunity to share my perspective and look forward to a meaningful dialogue and discussion as part of this panel.