FERC Technical Conference on Supply Chain Risk Management – January 28, 2016

Andrew A. Bochman, Senior Cyber and Energy Security Strategist, Idaho National Lab

---

I am here on behalf of the US Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE), and the DOE's complex of 17 national laboratories, one of which is the Idaho National Lab, my employer.

INL has a long history of cyber-physical security research, which has its origins in the development of some of the world's first nuclear energy generation technologies.

This work involved designing and testing nuclear generation plants, as well as the first industrial control systems (ICS), essential for monitoring and managing nuclear processes at a safe distance.

Over time, this led to working in close collaboration with a variety of energy and communications systems suppliers, as all parties sought to achieve maximum safety and security goals.

In large part based on these experiences, INL was tagged by DOE-OE to perform ICS assessments and impact demonstrations on a large number of systems involving many suppliers and asset owners.

DOE-OE has undertaken a number of initiatives intent on improving the nation's stance vis-à-vis energy sector supply chain vulnerabilities and related challenges, particularly to the electric and oil and natural gas (ONG) subsectors.

Among these is the Cybersecurity Capabilities Maturity Model (C2M2), which includes ten principle security domains, one of which is: Supply Chain and External Dependencies Management.

It addresses cybersecurity requirements for electric utilities (and other asset owners) and their suppliers and third parties, such as requiring suppliers to notify customers if and when they themselves:

- Have cybersecurity incidents, or
- Uncover or otherwise learn of vulnerability-inducing product defects throughout the intended life cycle

Asset owners are also encouraged to monitor other information sources closely to identify and avoid supply chain threats.

In addition, DOE-OE and the Energy Sector Control Systems Working Group (ESCSWG), along with help from FERC, Edison Electric Institute (EEI), the Utilities Telecom Council (UTC), the American Public Power Association (APPA), the American Gas Association (AGA), INL and others, released procurement language guidance, updated in 2014, intended to help guide utilities and other asset owners in their acquisition of more secure products and services.

One other thing I definitely want to share with you is the formation of a new Energy Sector Critical Manufacturing Working Group (ESCMWG), a collaborative effort between the DHS Office of Infrastructure Protection and DOE-OE that will work with the energy and critical manufacturing sectors to evaluate the security and integrity of delivering devices, equipment and services that support the Nation's energy infrastructure. This supply chain-focused effort will provide a forum for asset owners

and manufacturers to discuss critical issues that might impact the energy sector, and provide recommendations for areas of improvement.

Here are a few early details for you. As currently envisioned, the ESCMWG will:

- Be composed of members from the Critical Manufacturing Sector Coordination Council (SCC), the Electricity SCC and ONG SCC
- Provide an open dialogue in a CIPAC environment where critical manufacturers and energy sector asset owners can discuss issues that impact the energy sector via critical manufacturers and the supply chain
- Bring in, as necessary, subject matter experts (SMEs) in supply chain management, trade organizations, etc. to contribute their specific expertise on the issues being discussed

We briefed the concept for this working group at the Association of Electric Equipment Manufacturers (NEMA) annual conference as well as at the Electricity Subsector Coordinating Council (ESCC) and ONG SCC meetings last November and December and got very strong approval to proceed.

If the ESCMWG is successful, one tangible result you may envision is that at the next national grid security and resilience exercise, GridEx IV in 2017, not only will asset owner and government agency senior leaders be at the Executive Tabletop, but so will Critical Manufacturers, or in other words, some of the most important energy sector suppliers, to help steer us towards the best possible responses when the security of the grid and the nation are at stake.

Thanks again for the opportunity to share this update with you.