Docket No. RM15-14

Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management

Prepared Written Statement of Helen Nalley

On Behalf of the Edison Electric Institute and Southern Company

January 28, 2016

Good morning. My name is Helen Nalley. I am the Director for Operations Compliance at Southern Company in Birmingham, Alabama. I appreciate the opportunity to participate at today's conference on behalf of the Edison Electric Institute (EEI) and Southern Company.

While we agree that supply chain risks require careful consideration in managing critical infrastructure protection (CIP) and cybersecurity, we do not agree that a reliability gap exists in the mandatory cybersecurity standards, CIP version 5, to explicitly address supply chain risks. Without time and experience from the implementation process for CIP version 5, it is premature to conclude these requirements contain any reliability gaps that merit formal review in the standards development process. Instead of a directive for additional mandatory requirements, we believe that several existing supply chain practices and procedures provide a strong portfolio for addressing the risks, including for example, the NIST framework. Today's conference will highlight several of the practices.

This approach is justified and will meet the Commission's objectives because the CIP version 5 standards provide a strong framework that 1) provides a defense-in-depth or risk-based approach to ensure application of the broad range of security controls proportionate to the risks faced by each company, 2) allows companies to adapt their risk management strategies as

new threats arise and technologies evolve, and 3) helps ensure companies can efficiently integrate their NERC-related compliance actions with their enterprise-wide risk management efforts. Industry implementation of this framework requires comprehensive, highly detailed, and candid discussion and negotiations with third party vendors on a broad range of sensitive matters within the supply chain.

We urge the Commission to recognize its jurisdictional responsibilities and boundaries, and consider how to most effectively use them. The complexities of supply chain management, both internally within corporate boundaries, and externally through the business relationships companies maintain with their hardware and software vendors, and the risk-based nature of supply chain risk management practices simply do not offer a good fit with Commission-approved mandatory reliability standards. Moreover, prescriptive mandatory standards may result in the unintended consequence of hampering utility efforts to manage their supply chain risk.

Electric companies take very seriously their public service responsibilities and have strong incentives to maintain high levels of service quality, including bulk power system reliability, under a broad range of federal, state, and local requirements. Industrial control system suppliers operate in an extremely large and dynamic global marketplace and incorporate strong processes to protect against intentional and inadvertent insertion of devices or software code that could damage or destroy various assets controlled by information technology components.

In response to the issues this panel was encouraged to address, I'll start with the challenges to managing supply chain risk. EEI member companies experience three broad categories of

challenges. First, the market for the hardware and software used in industrial control systems is enormous, global, extremely complex, and maintains a fast pace of technology change. Vendors and users specify and purchase hardware and software systems, all of which include numerous components and subcomponents, which may be made by different manufacturers in different parts of the world. The buyers of these systems often do not have full visibility to this complex vendor environment, making managing measurable approaches to supply chain management difficult for users such as utilities.

Second, given the diverse nature of utility assets and asset configurations, we need flexibility to choose products that support our specific risk management strategies and meet the functional needs of the system. Explicit mandatory requirements cannot provide this flexibility.

Third, we already dedicate extensive management time and attention to dealing with software and hardware upgrades and security patches to vendor-provided systems. In other industries, such as automotive, when vulnerability is discovered in a vendor's product, it is the vendor's responsibility to remediate it at no cost to the customer, often through the "recall" process. With utility control systems, there are no obligations for vendors to fix vulnerabilities and the customers usually have to pay maintenance contracts for the privilege of obtaining fixes to the vendor's original problems. At times, very expensive upgrades to new versions are required. This supply chain challenge is also regulated under CIP version 5, which brings me to the second issue on how the CIP standards provide supply chain risk management controls.

In the joint trade association comments filed in this docket, we mapped the CIP V5 requirements to the NIST framework for supply chain controls. For example, CIP-010-2 addresses the prevention and detection of unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromises that could lead to misoperations or instability. CIP-010-2 requires extensive baseline configuration testing and change monitoring, as well as vulnerability assessments. In addition, both CIP-004 access management controls and CIP-011 information protection controls provide further examples of the comprehensive defense-in-depth design of the NERC CIP standards. The CIP requirements provide strong incentives for utilities to work with suppliers and vendors during the acquisition, delivery, and integration phases of the supply chain lifecycle to minimize their compliance risk during the operations stage. While CIP maps to NIST, it is important to recognize that CIP defines formal performance requirements and compliance demonstrations, while NIST offers a broad range of considerations that companies could consider in developing specific strategies.

We view a high and rising likelihood that mandatory requirements inhibit technology innovation and flexibility for tailoring IT strategies and designs. Specifically, we are discovering that CIP version 5 implementation has created some significant challenges for the use of innovative security solutions. For example, CIP version 5 is silent on virtualization, a technology not contemplated at the time the version 5 standards were drafted. Without clarity for demonstrating compliance, companies could seek technology applications that allow more

straightforward compliance demonstrations. This issue could become more troublesome if the Commission required additional mandatory requirements to address supply chain risks.

In addition to inhibiting flexible technology designs and using newer technologies, additional mandatory supply chain requirements will likely hamper negotiations with numerous vendors and could possibly discourage vendors from entering or remaining in the market to serve the utility industry. We strongly believe that requirements will ultimately narrow the market field to only the largest vendors with the most resources, thus stifling innovation and competition, and potentially increasing costs.

Instead of ordering the development of new requirements, we urge the Commission to focus on ensuring that the CIP version 5 requirements set an enduring framework that allow utilities to ensure they achieve reliability objectives, including cybersecurity risk management, and allow for flexibility in deciding how best to efficiently and effectively achieve those outcomes and manage the risks. Companies do not lack incentives for maintaining reliability.

I appreciate the opportunity to represent the EEI member companies and Southern Company at today's conference and look forward to further discussion on these issues.