FERC Docket No. RM15-14

Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management

Prepared Written Statement of Michael Kuberski

Pepco Holdings, Inc.

January 28, 2016

Good afternoon members of the Commission staff. I am Michael Kuberski, Manager, Grid Protection and Automation, for Pepco Holdings, Inc. (PHI). Thank you for the opportunity to participate in today's Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management.

Pepco Holdings, Inc. is one of the largest energy delivery companies in the Mid-Atlantic region, serving about 2 million customers in Delaware, the District of Columbia, Maryland and New Jersey. PHI utility subsidiaries Pepco, Delmarva Power and Atlantic City Electric provide regulated electricity service; Delmarva Power also provides retail natural gas service in Delaware.

As the service provider for our nation's capital, we recognize our responsibility to employ effective processes and risk mitigation plans to maintain the safety and reliability of the nation's electric grid. We respect and share the Commission's goals to focus on the security and reliability of critical infrastructure.

Consistent with Edison Electric Institute (EEI) and the joint trade association comments filed in this docket, PHI does not believe that a new or modified North American Electric Reliability Corporation (NERC) Reliability Standard is needed on top of existing standards to

continue to achieve these goals. Primarily we feel Version 5 of the mandatory NERC critical infrastructure protection (CIP) cybersecurity standards are reasonable and appropriate requirements that will facilitate supply chain risk management.

Electric utilities are similar due to the critical service we provide; however, utilities do not fit a one size fits all approach. There are differences in the operational, information and communications technology (ICT) assets we procure to safely and reliably deliver electricity to our diverse service territories.

We find ICT asset suppliers are constantly innovating and driving better solutions in the marketplace. Utilities need the flexibility to adopt these solutions. Additional requirements may hinder marketplace advancements if they are not modified fast enough to keep pace with new technology that falls outside of the existing scope of products. We should avoid the scenario where technology exists that is better for security and reliability, but not usable because it is not part of the Standard or creates compliance risk. We also do not want to drive innovative suppliers from the electric market allowing for attackers to focus on smaller lists of vendors to attempt to attack and exploit.

As previously stated, PHI views the CIP version 5 requirements as appropriate and reasonable. A risk of supply chain compromise that could introduce products with malicious functionality is a cybersecurity threat, and for a number of reasons not under the full control of the utilities or vendors. Therefore, the risk of supply chain compromise cannot be fully mitigated. Since PHI uses a number of vendors that may use multiple third-party suppliers for components in their technologies, PHI views the supply chain risk management as a shared

responsibility that requires collaboration and well-defined expectations. Various government activities can also support these collaborative efforts by sharing information on product vulnerabilities.

PHI supports existing NERC CIP version 5 controls, which effectively provide utility controls for supply chain risk while not overburdening suppliers. We feel supply chain processes should not be regulated, but controlled by the organizations that must tailor them to their unique environments. We support ongoing efforts for developing voluntary guidelines through industry groups along with new supply chain cybersecurity risk management processes and technologies. PHI believes it can adapt quicker to a changing cyber environment than a regulatory process can adapt.

Vendors have demonstrated a vested interest to use secure manufacturing and development practices if for no other reason than to protect their name brand and market share. PHI strongly believes that it has in place effective processes and policies to review vendors' practices before integrating technologies into critical systems, which supports CIP version 5 requirements. Review and validation of processes used by vendors and ICT providers takes place when PHI conducts requests for proposals for ICT products and services. PHI strongly recommends that the Commission avoid seeking to incorporate various purchasing practices or policies into NERC mandatory requirements.

Cyber asset contracts should include terms and conditions that specifically address matters of cybersecurity while providing audit rights to assess vendor adherence to contractual commitments. PHI believes in thoroughly vetting vendor security practices and supports

consideration of all steps of the manufacturing process from design though build to ongoing support. It is important to note that we should be setting guidelines and not prescriptive measures so that we do not negatively impact innovation in this space. PHI supports vendor testing and digital inspection of cyber assets. Recurring security assessments with frequency based on asset risk and criticality should be leveraged.

PHI and its vendor partners will continue to exercise change management controls on cyber asset firmware and software to minimize potential exploitable vulnerabilities. PHI conducts periodic threat and risk assessments with vendors and also conducts advanced risk assessments with third-party experts. Based on the findings of the risk assessment, we determine methods to mitigate the risks. Mitigation methods should be evaluated as key components or architectural changes need to be made.

If it is determined that a standard is required to address supply chain, which we feel is adequately addressed in the existing NERC CIP V5 Standards, it would be necessary to include key stakeholders in development of this standard. FERC should not deploy further standards drafting without the informed input of the key stakeholders (vendors of operational technology and ICT equipment, utilities, and standards organizations).

The new NERC CIP V5 standards to be implemented in April 2016 will provide still further incentives for PHI to have controls in place to manage risk. PHI recommends that the Commission allow CIP version 5's implementation to inform evaluation of the standards' strength and effectiveness, and not create yet another standard. This will allow PHI and vendors to continue to improve upon industry technical standards and approaches for the ICT

systems that enable critical business processes with an emphasis on the secure functionality of hardware devices and software applications. For example, creating internal utility technical review boards to guide such approaches as well as research and development of new operational technology (OT) and information technology (IT) would be helpful. Vendors play a key role in the early stages of the supply chain lifecycle and we have to ensure that they are aware of our critical security requirements and the implications of non-conformance.

While the existing NERC CIP Standards represent strong progress in mitigating cyber risks to the bulk power system, PHI has concerns that additional standards may stifle market competition and technical innovation. While oversight and collaboration with vendors is necessary and exists today in the form of tested, mature and effective procurement processes, PHI does not wish to hinder its supplier relationships or reduce the number of potential vendors in the marketplace with requirements that would cause inefficient or costly outcomes, or to reduce the company's ability to negotiate with potential suppliers.

We support continued industry collaboration, including development and implementation of guidelines that are not prescriptive, and the existing frameworks offered by NIST, DOE and IEEE. Together we can maintain the agility needed to protect our critical systems while staying on the leading edge of technological advancements that enhance the reliability and security of our systems.

Thank you again for the opportunity to participate in today's conference and I look forward to further discussion about this important topic.