

**UNITED STATES OF AMERICA  
FEDERAL ENERGY REGULATORY COMMISSION**

**Technical Conference on Version 5 Critical Infrastructure Protection Reliability Standards  
(RM13-5-000)**

**Prepared Statement of James Boone for Panel #2  
April 29, 2014**

Good afternoon members of the Commission Staff. I am James Boone, manager, strategic initiatives at Pepco Holdings Inc. (PHI). PHI is one of the largest energy delivery companies in the Mid-Atlantic region, serving approximately 2 million customers in Delaware, the District of Columbia, Maryland and New Jersey. My remarks speak to whether additional definitions and security controls are necessary to protect Bulk Electric System (BES) communication networks including secure remote access to control and monitoring devices. These remarks commend the industry for making significant advances in the area of cyber security fostered by the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Reliability Standards. NERC CIP Reliability Standards require information protection and adequate security practices to protect the reliability of the BES. Utilities outside of North America are choosing to voluntarily comply with these standards. The NERC CIP Version 5 Reliability Standards continue to drive proven security practices to support the reliability of the BES. In this pursuit, utilities are addressing technical challenges and dedicating resources to advance the security and reliability of the BES. The industry is actively identifying the facilities and assets to be covered and classified under NERC CIP Version 5. A stable set of standards is the best environment to enable business to drive mature processes.

BES communications networks are usually complex private networks with large capital investments connecting numerous field sites with control centers. They have been designed with redundancy and high availability requirements. BES networks and systems that depend on field asset data often have integrated monitoring to further support reliable operations. Adding compliance layers to these high availability networks would serve mostly to increase cost and network complexity.

Ensuring effective definitions are in place is essential. The latest version of the NERC glossary of terms is missing some key cybersecurity and communications definitions. Terms like end-to-end encryption, authentication, authorization and identity services are important to robust cyber security and communications programs. It is important that cybersecurity terms are defined so that a common understanding of the terms can be established. Many cybersecurity terms are already defined in the National Institute of Standards and Technology Interagency Report (NISTIR) 7298 and this document may be referenced as an approved definition source in future NERC guidance documents. Terms that are specific to NERC CIP should be defined in the document and definitions should not be duplicated that are already defined in NIST IR 7298. The Cyber Asset definition references the term programmable

electronic device which is very broad and may actually distract from the identification of key digital assets that secure the BES. The revised definition of the physical security perimeter (PSP) correctly shifts the focus away from the six-walled boundary concept to controlled access areas. It also removes references to computer and telecommunications rooms which may lead to missed communications system protections. Entities are perceptive to maintain a supplemental glossary of terms specific to their compliance program.

Protecting access to critical non-routable assets within a cyber program is challenging. Entities are prudent to document all connections to essential cyber assets, including dial-up and non-routable devices. These connections are then described on the Electronic Security Perimeter (ESP) drawing. NERC CIP Version 5 requires strong authentication of dial-up connectivity. Mature cybersecurity programs secure non-routable links especially that extend to multiple network segments.

Critical cabling within an ESP already receives the protections of a PSP. To further manage risks, entities must consider protection methodologies for key local communication control systems and related cabling. As mentioned, PHI internal communication networks offer high performance, high availability communications networks such as Multiple Protocol Label Switching and Synchronous Optical Networks. Given the reliability of these communications technologies and redundancy designed into these systems the core cabling should remain outside the scope of the NERC CIP standards. End points of these communication links are already in scope as they become access points into ESPs, which have effective security requirements.

Under NERC CIP Version 5 secure remote access to cyber assets requires authentication, authorization, and access privileges. NERC CIP Version 5 requires a dedicated asset outside of the ESP known as the "jump box" to provide the trusted platform to connect to the cyber assets within the ESP. This model ultimately provides flexibility and strong security.

NERC CIP Version 5 is mostly silent on securing data in motion across the network. Access is strictly controlled at the Electronic Access Point (EAP) and using identity services. In addition to access controls, utilities may further reduce risks by using standards based encryption and active monitoring services like Intrusion Detection Systems, Network Access Control systems and anomaly detection to address unusual network traffic.

Encryption provides another layer of protection for securing the data. However, as encryption methods are selected many items need to be taken into account. Encryption adds latency to the transmission of the data. Many of the end devices do not yet support internal encryption. While encryption obfuscates the message from intruders, it also introduces complexities into device-to-device connections and most monitoring systems.

Docket No. RM13-5-000

PHI will continue to work with utility asset vendors to enhance their products to support security protections. Targeted system replacements and upgrades will support security and compliance initiatives. PHI will continue to seek to improve its services which automate identity, access, encryption, monitoring and alerting systems. The NERC CIP Version 5 Reliability Standards together with PHI's security architecture will continue to drive strong security practices into the BES.