Statement for the Record

David Velazquez
Executive Vice President, Power Delivery
Pepco Holdings, Inc.

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"

Before the Committee on Homeland Security and Governmental Affairs
United States Senate
March 26, 2014

Thank you, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. My name is David Velazquez and I have the privilege of serving as Executive Vice President of Power Delivery for Pepco Holdings, Inc. (PHI), an electric utility delivering power to about 2 million customers in the Mid-Atlantic, including Washington, D.C. It is a pleasure to appear before you today to discuss an issue of fundamental significance to the electric utility sector— public-private partnerships to advance the security of the grid.

We know our adversaries are pursuing capabilities to attack, manipulate, or disable assets across the critical infrastructure sectors through cyber means. Complicating the defense of critical infrastructure is the fact that so many of these potential targets are owned and operated by the private sector. That's why it is imperative that government and industry work closely and leverage each other's expertise for the benefit of utility customers and the general public. The government has intelligence-gathering capability and military forces; the utility sector needs the government to help identify threats and provide technological support to assist in the defense of our systems. Similarly, the utility sector has experience operating an electric utility system; the government must depend on this private sector engineering and operational expertise that keeps the grid running reliably in the face of all hazards.

As the utility powering the nation's capital, PHI has been actively engaged in cybersecurity protection and planning and in the advancement of national cybersecurity regulations and legislation for a number of years. In addition to the sensitivity of our service territory, we are a relatively small utility yet we serve customers in four jurisdictions. The thought that in the absence of federal action, each of these jurisdictions could potentially develop its own cybersecurity framework and protocols is daunting. We believe legislation is necessary and commend the work this Committee and others in the House and Senate have done to try to advance legislation. Recognizing, however, the challenge passing cybersecurity legislation entails, PHI has participated in the development and rollout of the cybersecurity Framework released last month pursuant to the President's Executive Order issued last year.

To this end, PHI was very actively involved in the many public information gathering sessions led by the National Institute of Standards and Technology (NIST). We found this NIST-led process to be extremely collaborative, evolutionary, and respectful of the work that the electric utility sector and our regulators had already done in the cyber space. At the February release of the Framework, PHI pledged to be among the first utilities to work with the Department of Homeland Security and Department of Energy to apply the self-assessment process to our operations. Today, that process is ongoing. We believe the Framework allows us another valuable perspective of the cyber problem and is a tool to help us prioritize our activities and allocate our resources in a rigorous and repeatable manner. The voluntary assessment process the Framework sets forth will give our regulators an important means to effectively communicate cybersecurity efforts within the electric sector and other key critical infrastructure sectors. However, for this process to be truly resonant with our regulators, PHI believes it would benefit from some form of standardized third-party verification.

Though the development of the Framework has significantly advanced electric sector interface with the government on cybersecurity, it is not the first example of this public-private partnership. I'd like to take a few moments to share with you some summary comments on some of these additional tools and partnerships.

Critical Infrastructure Protection Standards (CIP)

CIP standards are both mandatory for all owners and operators of Bulk Power System assets, and enforceable by the Federal Energy Regulatory Commission (FERC) with fines of up to $1

million per day. CIP standards are essential for ensuring basic network hygiene and baseline levels of security for the thousands of entities operating the electric grid. However, they alone cannot account for the very dynamic nature of cyber risks. Instead, the electric power sector has seen the value both of implementing CIP standards *and* of developing close working relationships with federal and state governments. These strategic partnerships help to identify vulnerabilities that could be exploited, implement defenses quickly based on the ever-changing threat environment, and respond in a coordinated way to any successful attacks.

National Cybersecurity & Communications Integration Center (NCCIC)

NCCIC serves as a centralized location where operational elements involved in cybersecurity are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. As a critical infrastructure operator, PHI is in the process of obtaining the clearances needed to maintain a seat on the NCCIC floor and thus participate in NCCIC efforts to provide actionable and comprehensive information in real time to advance a whole-of-nation approach to prevention, response, mitigation, and recovery efforts.

Electricity Subsector Coordinating Council (ESCC)

The ESCC is made up of utility CEOs (including PHI's CEO, Joe Rigby) and trade association leaders representing all segments of the industry, actively partnering with government executives to prepare for, and respond to, national-level disasters or threats to the electric grid. In meetings with senior government leaders over the last year, the ESCC has focused its efforts on three areas of industry-government collaboration:

Incident Response: planning and exercising to coordinate responses to an attack

Information Flow: making sure actionable intelligence and threat indicators are communicated to the right people at the right time

Tools & Technology: deploying the proprietary government technologies that enable machine-to-machine information sharing

The establishment of the ESCC has been invaluable, providing a primary liaison for government entities and other sectors to partner at the senior-executive level with the electric utility industry.

Application of Federally Developed Threat Detection Technologies

Though I am not at liberty to discuss the details of the threat detection programs in which we are partnering with various federal agencies, I can say that PHI has been afforded the opportunity to participate in federal security technology applications that allow for both temporary and permanent real-time, machine-to-machine threat detection. These programs allow us, sometimes at a considerable investment of time and money, to avail ourselves of some of the federal government's far superior capacity to monitor cyber systems for bad actors.

Grid-Ex II

Last November, the North American Electric Reliability Corporation (NERC) conducted a large-scale grid security and incident response exercise in which PHI was one of the many voluntary utility participants. The two-day exercise simulated a coordinated physical and cyber attack damaging the bulk power system and causing widespread outages followed by partial restoration and rotating outages. More than 165 organizations across industry and the government participated. One key learning from the exercise was the need for clearer protocols to coordinate governmental roles in the physical defense of privately held critical infrastructure. For instance, though law enforcement authority traditionally escalates from local to state to national as the scope of an incident becomes clear, in the case of a wide-spread or dispersed physical attack on the grid, all levels of government will need to immediately coordinate their efforts to lessen the potential for cascading impacts.

ICS-CERT

PHI is an active participant in ICS-CERT, a program that provides vulnerability information regarding industry control systems. Other assessment programs under ICS-CERT have helped bring awareness to design principles related to cybersecurity and reliability.

Open Issues

The potential roles for government in cybersecurity can be broken down into four areas:

- Standards and voluntary best practices sharing and assessment
- Information sharing

- Event response protocols
- Coordination of jurisdictional issues

The CIP Standards detailed above and the Framework released last month focus largely on the first of these areas. The CIP Standards set some threshold security mandates for bulk power operators, and the Framework is a voluntary tool to assess the application of existing standards and to determine and share best practices. Though these two programs significantly advance cybersecurity preparedness for grid operators, more can and should be done in the other three areas. For instance, though the federally administered technology programs in which a number of electric utilities participate offer some threat information sharing capacity, in the absence of legislation, much is left undefined with regard to data privacy and the liability associated with bi-directional threat information sharing. Similarly, though the NCCIC and ESCC create forums for event response coordination, they do not resolve all jurisdictional issues. Jurisdictional clarity is particularly important for a cyber-event because, unlike natural disasters, a cyber-event could be a crime, a national security incident, or even an act of war. As such, the primary objectives of different state and federal entities could vary greatly. In fact, governmental objectives might even be in conflict with one agency focused on restoring power and another focused on maintaining evidence needed to catch and prosecute attackers. We must have clear protocols for industry-government event response so that when an attack is identified, we can work quickly to contain the damage, begin restoration but so we can do so without destroying the government's capacity to investigate and prosecute the offense.

Finally, while the value of our investment in cybersecurity and response readiness is hard to measure, some assurance of prompt and reasonable recovery of those investments will be imperative. We know that the potential economic impact of a significant attack on the grid is enormous, and— regardless of how much you invest—you can't absolutely eliminate all threat. This is an issue with which the regulators who approve our rates are grappling. Today, our regulators seem willing to acknowledge the value of our investments in cybersecurity. However, as the threat continues to become more sophisticated, our investments will likely rise rapidly, and some systemized form of prompt cost recovery would facilitate our capacity to grow our expertise to align with this rapidly evolving threat.

In summary, PHI has been very active in and benefitted greatly from the growing array of opportunities to partner with federal, state and local authorities to advance our capacity to address threats to the grid. Public-private partnerships have improved cyber threat detection and cyber and physical event preparation and response coordination. However, more can be done. In particular, issues still needing attention include real-time and actionable threat information sharing, liability protection, event response protocols and systemized cost recovery. We look forward to continuing to work with the Administration, this Committee, and your colleagues in the Senate and House to advance legislation to address these open issues and to continue to improve our capacity to protect the grid from these ever-evolving threats.