Statement for the Record

Joseph Rigby

Chairman, President and CEO

Pepco Holdings, Inc.

"Enhancing Resilience in Energy Infrastructure and Addressing Vulnerabilities"

Before the Quadrennial Energy Review Task Force

April 11, 2014

Thank you Secretary Moniz, Dr. Holdren and the distinguished members of the Quadrennial Energy Review Task Force for the opportunity to address this very important forum created by President Obama. My name is Joseph Rigby and I am theChairman, President and CEO for Pepco Holdings, Inc. (PHI), an electric utility delivering power to about 2 million customers in the Mid-Atlantic region, including Washington, D.C. It is a pleasure to appear before you today to discuss an issue of fundamental significance to our nation – the vulnerabilities of the grid, strategies to address these vulnerabilities and opportunities for public-private partnership to advance grid resilience.

The electric grid generates, transmits, and distributes electric power to millions of Americans in homes, schools and businesses across the country. Construction of the grid began more than one hundred years ago. From the end of World War II into the 1970's, the grid grew at an amazing rate, using technology and equipment that often lasts for decades. And, though the grid continues to evolve to incorporate new technologies and ever improving standards and best practices to meet the challenges posed by cyber, physical and climactic threats -- the advanced age of many grid components is now contributing to grid vulnerability. This vulnerability coupled with our increased economic and lifestyle dependence on electricity make grid modernization and resiliency investment imperative.

Severe Weather Impacts

Severe weather remains the leading cause of power outages to large numbers of people in the United States. Weather-related power outages shut down businesses, close schools and impede emergency services, resulting in considerable costs to our economy and disruption in the lives of our citizens. And, these severe storms and other events seem to be coming with increasing frequency and intensity. For instance, in just the past few years PHI's Mid-Atlantic service territory has experienced the

'Snowmageddon', an earthquake, Hurricane Irene, the Derecho followed by a heat wave, Superstorm Sandy and a polar vortex. Some of these events directly damage grid infrastructure while others strain it through energy demand volatility, but all test a utility's capacity to meet its obligation to serve customers reliably and at a reasonable cost.

Though much of the grid may be decades old, the continuous advent of new technologies, improvements in the manufacture of key components, and better design methods for traditional equipment, have allowed the utility industry to continuously build resiliency into the grid. Nonetheless, the increasing number and severity of weather events is compelling utilities and regulatory commissions to look for additional grid strengthening strategies. The utility industry understands what measures need to be put in place but the cost impact of many of these strategies will be significant and it will take time to physically execute. The most immediately beneficial and also cost-effective of these measures include:

- Hardening transmission and distribution substations and lines to make equipment less susceptible to storm damage;
- Raising or moving vulnerable or outage-susceptible substations and other infrastructure to less damage prone areas and building additional new substations and infrastructure to create or increase redundancy;
- Selectively undergrounding infrastructure to mitigate the impact a weather-related event has on the overhead system and reducing the associated recovery time where an overhead outage is experienced;
- Enhancing vegetation management programs to lessen the impacts of falling trees and branches on overhead lines; and,
- Deploying technologies that enhance system information, intelligence, and control and, in so doing:
    - Empower grid operators with real-time information to avert outages;
    - Establish intelligent systems that can adjust to conditions automatically; and
    - Provide for greater remote control over critical devices for faster restoration of power.

While not as immediately impactful, these new control and information technologies are also making possible further sectionalizing and networking of the grid into microgrids that may allow operation independently of the main grid during times of system emergency. Though some believe this form of decentralization is the correct path for security, consumer independence, and proliferation of clean energy resources, moving toward decentralization via microgrids will increase costs. Furthermore, moving to a decentralized system without payment from those that use the grid could result in unreasonable cost shifts

or insufficient recovery of grid costs, which could discourage needed transmission and distribution investment. Policy Makers must consider:

- How the grid will be safely, fairly, and efficiently operated;
- Who will be responsible for reliability and safety;
- How reliability and safety standards will be enforced;
- How costs of the grid and access to back-up power will be allocated; and,
- How to minimize unreasonable cost-shifting among customers.

Man-Made Threats

We know our adversaries are pursuing capabilities to attack, manipulate, or disable grid assets through cyber means. Similarly, as evidenced by the physical attack on a California substation in 2013, the threat of a violent and deliberate attack on utility infrastructure is very real. In the face of these evolving security threats, 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 assistance 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.

On the cyber front, PHI and the other owners and operators of Bulk Power System assets are already subject to mandatory Critical Infrastructure Protection Standards enforceable by the Federal Energy Regulatory Commission (FERC). The electric utility industry is also actively engaged in a number of on-going efforts to advance cyber protections and response capabilities such as the voluntary cybersecurity framework developed in response to the President's Executive Order. Other industry-wide cybersecurity advancement and coordination initiatives include the National Cybersecurity and Communications Integration Center, the Electricity Subsector Coordinating Council, and ICS-CERT. Individual utilities, like PHI, have also benefitted greatly from opportunities to apply federally-developed cyber threat detection technologies to their operations.

In the physical arena, utilities are actively expanding their view of physical security from merely protection from intrusion and theft to one that expands the perimeter and realm of possible threats to

include attacks such as gunfire from a remote location, intrusion via explosive device, and vehicle-born explosive devices. In addition, last month FERC issued an order requesting the North American Electric Reliability Commission (NERC) develop standards that require utilities to demonstrate that they have taken steps to address physical security risks and vulnerabilities. The utility sector supports this initiative in that it recognizes that each utility -- based on its location (urban, suburban, rural), geography, redundancy, system design, and need to harmonize with local communities -- could have different challenges regarding how to address the physical threats to their infrastructure. The best way to determine the right measures for a given utility involves:

- Sharing intelligence with national and local law enforcement to determine the risk/threats;
- Putting appropriate substation measures (fencing, motion detection cameras, line of sight barriers etc.) in place to deter, detect, and delay intrusion;
- Coordinating physical attack response and recovery through individual and joint planning, exercises, and spare equipment logistics;
- Grid operator-level planning that is more stringent and recognizes that it is conceivable and realistic to build enough redundancy into the system to mitigate the impact the loss of a critical or series of critical facilities, even during peak periods.

Whether in addressing cyber or physical threats to the grid, public-private partnership is key. Though much has already been achieved through existing public-private partnerships, open issues do exist. For instance, though the federally-administered cyber technology programs offer some threat information sharing capacity, in the absence of federal legislation much is left undefined with regard to data privacy and the liability associated with bi-directional threat information sharing. Similarly, forums exist for physical and cyber event response coordination, but without explicit authorization these forums may not resolve all jurisdictional issues. And, very importantly, we must have clear protocols for industry-government event response before an event occurs. Finally, some assurance of prompt and reasonable recovery of security-enhancing investments will be imperative. Today, our regulators seem willing to acknowledge the value of our investments in security. However, as the threat continues to become more sophisticated, our investments will grow signiciantly, and some systemized form of prompt cost recovery would facilitate our capacity to grow our expertise and security.

Economic Factors

Clearly, the security and resiliency of our energy infrastructure impacts our nation's economic competitiveness and expansion capacity. The relationship between the economy and grid resilience is, however, bi-directional in that the ability of private grid owners and operators to address grid

vulnerabilities and expand grid resilience is dependent on various economic and regulatory factors. In the past, the need for new grid investments has been matched by growing electricity demand. The recent flattening of electricity demand, however, makes more challenging the financing of the significant investments necessary to address emerging, evolving or intensifying severe weather, cyber, and physical threats. In addition, regulatory concerns regarding the rate impacts resulting from utility security and resiliency investments may cause untenable lags in utility cost recovery. This regulatory impact may be exacerbated by approaches to the integration of distributed generation that do not properly recognize the continued grid-dependence of the beneficiaries of these distributed generation assets.

In fact, while the wide scope of new electric power supply resources, including Demand Response, combined heat and power, distributed generation (DG), Solar Photovoltaic (PV), Customer Backup Generation and microgrids, have an important role in our Nation's evolving energy mix, it is essential that these resources be properly integrated into the grid to provide safe, reliable, affordable, and environmentally responsible electricity to consumers. Proper integration includes technical compatibility, a diverse resource portfolio, and the mission of overall grid reliability. A lack of integration into the power grid either during the planning or operation of these new distributed energy resources could lead to unforeseen consequences impacting the safety, reliability, and resiliency of the grid.

Opportunities to Partner with Government

As the cybersecurity experience has taught us, there are great benefits to be gained from public-private partnerships to advance grid security. At PHI, we have also had the opportunity to see this illustrated at the local level in the area of grid resilience. In the aftermath of the Derecho in June 2012, the Mayor of D.C. asked me to co-chair a committee with the city administrator to investigate and propose an initiative to place vulnerable overhead electric distribution equipment underground. Months of diligent work by customers, the District's Public Service Commission, Office of People's Counsel, District government and PHI resulted in legislation that would place much of PHI's local utility affiliate Potomac Electric Power Company's (Pepco) feeders underground. The legislation provides that Pepco will fund 50% of the investment, while the District will fund the remainder through a combination of securitization bonds and other public money.

This public-private partnership will increase system resiliency and reliability in a cost effective manner designed to limit the financial impact on customers. Residents, businesses, government, non-profits and visitors will all benefit from the increased reliability, and make the District of Columbia a better, more resilient place in which to live, work and play. This is a great example of a public-private partnership delivering real value at a reasonable cost.

In summary, the grid has tremendous value as a key enabler of economic growth, of our advanced standard of living, and of an "all of the above" energy strategy. But, the grid is also vulnerable to emerging climatic, physical and cyber threats. These threats are best addressed through public-private partnerships and policies that draw on the different strengths and capacities of our public institutions and the private entities that have developed expertise as the owners and operators of the majority of grid assets. Existing partnerships should be expanded to allow for better information flow, role clarity and for expanded event planning and response coordination. New partnerships between the electric utility industry and all levels of government should be developed to establish new financing mechanisms for security and resiliency investment. And, government policies should be shaped to attract capital, provide regulatory certainty, and mitigate risks so that grid operators can continue to meet the very real need for a dynamic and resilient modern grid.

Thank you again for allowing me to provide input to this very important topic.