STATEMENT OF WILLIAM H. SPENCE
CHAIRMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER
PPL CORPORATION

BEFORE THE HOUSE COMMITTEE ON TRANSPORTATION & INFRASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS
AND EMERGENCY MANAGEMENT

"PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER AND PHYSICAL THREATS"

APRIL 14, 2016

Introduction

Good morning Chairman Barletta, Ranking Member Carson and Members of the Subcommittee. My name is Bill Spence, and I am the Chairman, President and Chief Executive Officer of PPL Corporation.

Headquartered in Allentown, Pennsylvania, PPL Corporation is one of the largest companies in the U.S. utility sector. Our seven utility subsidiaries serve 10 million customers in the U.S. and the United Kingdom. We deliver electricity to customers in the U.K., Pennsylvania, Kentucky, Virginia and Tennessee. We deliver natural gas in Kentucky. In addition, we own and operate about 8,000 megawatts of generation capacity in Kentucky.

In addition to overseeing PPL's domestic and international operations, I am a member of the Executive Committee of the Edison Electric Institute (EEI) and co-chairman of EEI's CEO Policy Committee on Reliability and Business Continuity. I am also a member of the Electricity Sub-Sector Coordinating Council (ESCC), which serves as the principal liaison between the federal government and the electric power sector to address national security threats to the nation's power grid.

Thank you for providing PPL Corporation with an opportunity to testify on the important topic of the reliability and resiliency of the power grid in the face of continuing cyber, physical and natural threats.

As I hope to convey in my testimony, PPL and the broader electric power industry are committed to protecting the nation's power grid from threats of all types. This commitment did not arise in the face of new, modern threats; it is a shared commitment that is deeply rooted in the fabric of the industry. We have made, and continue to make, significant investments in tools, technology and people to strengthen our defensive capabilities and ensure grid reliability and resiliency.

In particular, we recognize that cyber threats are persistent and evolving. Even as we enhance our responses to meet the rising threats, there is no way to fully guarantee a breach will not occur. As such, we plan and drill regularly to ensure we can respond and recover quickly and effectively should an emergency arise.

Overview of Industry Efforts

Protecting the nation's electric power grid and ensuring a reliable and affordable supply of energy are top priorities for the electric power industry.

As owners and operators of critical infrastructure, the electric power industry's top priority is to ensure the reliability and resiliency of the North American electric grid. With cyber and physical security a key focus of our reliability assurance strategy, the industry has a strong record of working together and with government partners to identify, assess, and respond to all threats.

The electric sector takes a "defense-in-depth" approach to protecting grid assets. This includes: rigorous, mandatory, enforceable and regularly audited reliability standards; close coordination among industry and with government partners at all levels; and efforts to prepare, respond and recover should power grid operations be affected in any way.

Security standards and regulations are an important part of the industry's security posture.

The electric power and nuclear sectors are subject to North American Electric Reliability Corporation (NERC) mandatory, enforceable and monitored Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties of up to $1 million per violation per day. In fact, our industry is the only one subject to mandatory, federally enforceable cyber and physical standards.

These mandatory standards continue to evolve with input from subject matter experts across the industry and government. Currently, the electric power sector must comply with Version 3 of the cybersecurity standards, while Versions 5 and 6 become enforceable on July 1, 2016. These new versions are more rigorous than the past versions and not only increase the scope of the standards, but also add several new cybersecurity requirements that mirror cybersecurity best practices.

In addition to implementing Versions 5 and 6 of the cybersecurity requirements, the industry is implementing requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry is also using voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as the Department of Energy's Cybersecurity Capability Maturity Model (C2M2).

PPL and others throughout the industry are assessing their cybersecurity capabilities against this framework and capability maturity model and, based on results, prioritizing their investments to strengthen cybersecurity.

While regulations and standards provide a solid foundation for strengthening the industry's security posture, they alone are not sufficient. As the threat environment evolves, so must the industry's security efforts.

In addition to regulations and standards, close coordination and the sharing of threat information between government and industry help to protect the power grid.

Protecting the grid is a responsibility shared by both industry and government. The industry owns and operates most of the grid, while the government has law enforcement and intelligence gathering capabilities and is responsible for national security. That's why industry and government must work together to protect infrastructure critical to the life, health and safety of Americans.

According to the National Infrastructure Advisory Council, the electric power sector is viewed as a model for how critical infrastructure sectors can more effectively partner with the government. Our intent is to keep it that way.

The Electricity Sub-Sector Coordinating Council (ESCC), which I referenced earlier in my remarks, brings senior electric power industry executives like myself together with senior Administration officials from the White House; Departments of Energy, Homeland Security, and Defense; the Federal Energy Regulatory Commission; and the Federal Bureau of Investigation, to improve sector-wide resilience against all hazards and potential threats.

The ESCC is focused on several key areas, including planning and exercising coordinated responses to attacks or major disruptions to the power grid; making sure that information about threats is communicated quickly among government and industry stakeholders; deploying government-held technologies on electric power systems that improve situational awareness of threats to the power grid; and cross-sector coordination with the interdependent critical infrastructure sectors.

The ESCC has developed a playbook that provides a framework for senior industry and government executives to coordinate in support of response and recovery efforts. This playbook already has been used during exercises, including NERC's GridEx III exercise this past November, which I will address later in my testimony.

In addition, the ESCC recently established several industry-government working groups on key initiatives. These initiatives include:

- Developing a cyber mutual assistance framework to coordinate responses to significant cyber incidents;

- Partnering with the Electric Power Research Institute to address threats posed by electromagnetic pulses;
- Reviewing threats to the supply chain;
- Accessing enhanced background checks for critical employees;
- Instituting a Member Executive Committee, which I chair, that is providing strategic guidance to the Electricity Information Sharing and Analysis Center (E-ISAC).

The Member Executive Committee is working directly with the E-ISAC to ensure the electric power sector has the very best information-sharing and analysis capabilities and an organization that responds to the needs of industry operators. This endeavor is an extraordinary example of the partnership that can lead to improved outcomes for security of the industry and, by extension, the nation.

The federal government plays a crucial role in strengthening the security of the power grid through information sharing.

In the fight against cyber and physical threats, industry-government information sharing, as well as close coordination among grid operators and government partners, is critical. The E-ISAC gathers industry information on security-related events for sharing with its government partners and shares government information on threats with industry.

The sharing of threat information and data analysis is taking place between the E-ISAC and the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). The coordination between the E-ISAC and NCCIC is improving the security posture, situational awareness, and preparedness and response capabilities of federal, state and local governments; intelligence and law enforcement communities; and the private sector when it comes to cyber and physical events that might impact the electric power sector.

One example of the industry-government information-sharing efforts worth highlighting is the implementation of the Cyber Risk Information Sharing Program (CRISP), which is bolstering the sector's and the government's situational awareness. CRISP is a public-private partnership that enables sharing of cyber threat data among the government, the National Labs, the E-ISAC, and industry stakeholders. Cyber threat information shared through CRISP is helping to inform important security decisions not just among participating electric power companies, but all

sector participants through the E-ISAC. When one company experiences a cyber event, that information is immediately shared with all companies that deploy CRISP. This sharing of information allows industry members to deploy the best resources to identify and deflect incoming threats. By the end of 2015, more than 100 million households, or about 75 percent of U.S. electricity customers, were covered by companies, including PPL, that had deployed CRISP.

However, more actionable threat information sharing is needed, which is why the industry and PPL fully supported Congress passing cybersecurity information-sharing legislation, including liability protections for businesses, to provide a framework for more voluntary information sharing. The industry looks forward to working with the government to fully implement the Cybersecurity Information Sharing Act of 2015, commonly referred to as CISA.

Congress also has passed legislation that granted the Secretary of Energy limited-duration authority to address declared grid security emergencies, and directed DOE to submit a plan to Congress evaluating the feasibility of establishing a Strategic Transformer Reserve.

We appreciate the efforts of Congress to work with our industry to further protect our nation's power grid. And, because cyber threats are always evolving, we hope Congress will support more investment in research and development focused on strengthening existing efforts and developing new technologies, including those that will improve the speed, integration and analysis of threat information while protecting sensitive information.

The electric power sector is focusing even more on incident response and recovery efforts.

The third major element of the industry's "defense-in-depth" strategy is incident response. Power grid operators manage risk, but do not eliminate it, which is why a sound approach to security must include contingency planning.

Electric power companies, including PPL, continuously plan and exercise for a range of potential threats to the power grid, as well as the possibility of a widespread incident.

Electric power companies are constantly managing risk by understanding that something could go wrong and planning for the worst-case scenario. If you look at the power grid, it is one big, interconnected machine with thousands of owners and operators; everyone has to work together.

Through storm preparation and mutual assistance networks, the electric power sector has decades of experience working together in response to major incidents. For example, the electric power sector's response to Superstorm Sandy had companies from as far away as California, Texas and Canada sending equipment and crews into the affected regions to restore power. More than 80 companies and tens of thousands of mutual assistance crews responded. Following Hurricanes Katrina and Rita, PPL sent crews as far as the Gulf Coast states to support recovery efforts. In short, mutual assistance is not just a program, it is in our DNA.

Just as electric power companies share crews as part of the industry's voluntary mutual assistance programs to restore power, they also regularly share transformers and other equipment. The electric power sector is expanding equipment-sharing programs – like the Spare Transformer Equipment Program (STEP), *SpareConnect*, and the newly announced Grid Assurance program – to improve grid resilience no matter the threat.

The electric power sector's success regarding these transformer sharing programs depends upon the industry's ability to move large spare equipment, such as transformers, quickly over our rails, roadways and waterways. That is why the industry is working with other critical infrastructure sectors and the government to improve the coordination and preparation involved in moving large transformers during an emergency. For example, electric power companies, Class I railroads, and the heavy hauler and rigging industries developed a new Transformer Transportation Emergency Support Guide to expedite the deployment of equipment and services that would be needed to move these critical assets rapidly in an emergency.

With respect to exercises, this past November, NERC conducted the third industry-wide grid security and incident response exercise, known as GridEx III. GridEx III brought together more than 364 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to participate. PPL's U.S. distribution and transmission subsidiaries participated fully in the exercise, which was a rigorous and comprehensive two-day drill that simulated coordinated cyber and physical attacks on the power grid.

GridEx III also included an executive tabletop exercise that brought together 32 electric power sector executives and senior U.S. government officials to work through incident response protocols to address widespread outages. GridEx III was a continuation of industry-government efforts to participate in exercises that strengthen the security and resiliency of the power grid.

On March 31, NERC released its GridEx III After-Action Report to the public. Overall, NERC found that since GridEx II, industry and government responses to a significant cyber / physical attack continue to improve. The After-Action Report identified a number of recommendations for industry and government to continue to strengthen their coordination, preparation and response capabilities. As was the case with GridEx I and II, these recommendations will provide a road map for how the ESCC, with input from NERC, and the government will address security issues over the next two years.

Following GridEx III, the ESCC and our government partners agreed that more work is needed to help coordinate sector-wide response and recovery efforts, especially at the state and local level. Also, the ESCC established the Cyber Mutual Assistance Task Force to convene industry experts in an effort to inform and establish a cyber mutual assistance framework to aid electric power companies in rebuilding and recovering necessary computer systems in the event of a regional or national cyber incident. This program will build on the electric power sector's culture and tradition of mutual assistance to develop resource-sharing relationships that provide "surge capacity" should a cyber incident exceed the capacity for an individual company to respond.

PPL's Commitment to Protecting Critical Infrastructure

PPL is actively engaged in the industry efforts I have highlighted and takes an aggressive, defense in-depth approach to protect the power grid.

We strive at all times to comply with the industry's rigorous, mandatory and enforceable cyber and physical security standards.

We coordinate closely with industry partners and federal government agencies to share best practices and to prepare for and respond to potential threats. As I highlighted earlier, I am a member of the ESCC. PPL was an early participant in E-ISAC. We also participate in the CRISP

program. Through that program, we have received threat notifications and taken proactive security measures.

In addition, we continue to work to maintain and strengthen our ties to state agencies, state and local law enforcement, and state Fusion Centers that receive, analyze, gather and share threat-information.

As part of our broader efforts to modernize and reinforce the power grid — efforts that included infrastructure investments of more than $3.5 billion in 2015 and will include additional investment of more than $16 billion over the next five years — PPL is taking steps to better protect critical infrastructure. This includes improved system designs and redundancy that make the power grid more resilient and secure.

We conduct education and training for employees to improve threat awareness and prevent attacks. Further, we exercise and prepare regularly for grid emergencies, be they the result of an attack or severe weather. We have robust crisis management plans in place to guide our efforts in responding to threats and restoring power quickly if issues arise. As we have demonstrated in recent years during major storms, we are also committed to keeping federal, state and local officials, along with the general public, well informed of our efforts when service to customers is affected. This includes holding conference calls for elected officials and community leaders. It also includes keeping the public aware of the status of our restoration efforts via the Web, social media, news releases and direct communication to customers through text, email and other means.

Conclusion

In conclusion, PPL and the electric power industry are united in our commitment to protecting the nation's critical energy infrastructure.

Providing safe, reliable and affordable electricity is our top priority. Our industry invested more than $103 billion in energy infrastructure in 2015 alone — investments that included modernizing and better securing the nation's power grid. In addition, the industry made significant investments in preparedness, including training and exercises, to ensure we can respond quickly and effectively should a physical or cyber attack affect grid operations.

These sustained investments are making the grid more resilient and more secure every day.

Thank you again for the opportunity to present testimony on this important issue. I look forward to answering any questions you may have.