Statement of
Kenneth W. DeFontes, Jr.
President and Chief Executive Officer, Baltimore Gas & Electric
On Behalf of Exelon Corporation, the Edison Electric Institute, and the Electric Power Supply Association

Before the
House Permanent Select Committee on Intelligence
United States House of Representatives

February 14, 2013

Mr. Chairman and Members of the Committee:

My name is Ken DeFontes, and I am the President and Chief Executive Officer of Baltimore Gas & Electric (BG&E), an Exelon company. I also serve on the Edison Electric Institute's (EEI) CEO Business Continuity Task Force, and Exelon is the Chair of the Electric Power Supply Association's (EPSA) Board of Directors for 2013. I have also served as a charter member and Vice Chair of the Board of Directors of ReliabilityFirst. ReliabilityFirst is one of the eight approved Regional Entities in North America charged with ensuring compliance with mandatory reliability standards by utilities in the Midwest through the Mid-Atlantic. I am appearing today on behalf of Exelon, EEI and EPSA.

Exelon is a holding company headquartered in Chicago. Our retail utilities, ComEd in Chicago, PECO in Philadelphia, and BG&E, serve 6.6 million customers in central Maryland, northern Illinois, and southeastern Pennsylvania, making Exelon one of the largest electric and natural gas utility companies. Our generation subsidiary, Exelon Generation, is one of the top competitive power generators in the country and owns or controls approximately 35,000 MW of generating facilities, including fossil, hydro, nuclear, and renewable energy facilities. Exelon is the largest owner and operator of nuclear power plants in the nation and the third largest in the world. Our nuclear fleet consists of 17 reactors, as well as an ownership interest in an additional five reactors. Exelon serves numerous federal and military facilities including the National Security Agency (NSA) headquarters in Maryland.

EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members worldwide. EEI's U.S. members serve more than 98% of the ultimate customers in the shareholder-owned segment of the industry and represent about 70% of the U.S. electric power industry.

EPSA is the national trade association representing competitive power suppliers, including generators and marketers. Competitive suppliers, which collectively account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities. EPSA seeks to bring the benefits of competition to all power customers.

Both EEI and EPSA also are part of a broader coalition of electric power stakeholders that is focused on cybersecurity issues. While I am not testifying on its behalf, this coalition includes several major trade associations representing the full range of electric generation, transmission and distribution companies in the United States, as well as regulators, Canadian interests and large industrial consumers. While these groups do not always find consensus on public policy issues, in the case of securing the electric grid, there is near unanimous support for a regime that leverages the strength of both public and private sectors to improve cybersecurity.

I appreciate your invitation to appear today to discuss securing the North American electric grid against cyber threats, and the opportunity to testify about the Cyber Intelligence Sharing and Protection Act (CISPA). I also would like to thank Chairman Rogers and Ranking Member Ruppersberger for your leadership and thoughtful approach to improving government-industry coordination in defense of critical infrastructure.

My testimony focuses on the value of information sharing, as well as close coordination, among grid operators and our government partners, and provides examples of initiatives already underway that are improving this public-private partnership. I also will share our industry's observations about the best ways to promote cybersecurity and express our appreciation for CIPSA's adherence to principles that the industry believes are integral to successful cybersecurity policy.

As owners, operators, and users of the bulk power system, electric utilities take cybersecurity very seriously. We are actively engaged in addressing cybersecurity threats as they arise and in employing specific strategies that make every reasonable effort to protect our cyber infrastructure and mitigate the risks of cyber threats. As the industry relies increasingly on electronic and computerized devices and connections, and the nature of cyber threats continually evolves and becomes more complex, cybersecurity will remain a constant challenge. But we believe we are up to the task, building on our industry's historical and deep-rooted commitment to maintaining system reliability. One example of this commitment is reflected in the EEI Threat Scenario Project. This effort, run in conjunction with the Chertoff Group (led by former DHS chief Michael Chertoff), works to identify major cyber threats and to lower risks. By helping organizations identify risks, the Chertoff Group assists in building a framework and developing effective policies to prevent and respond to cybersecurity incidents.

Development and Implementation of Cybersecurity Standards under Existing Law Is Well Underway.

The electric utility industry is well on its way to implementing cybersecurity standards to safeguard our critical infrastructure. Our industry is already subject to cybersecurity standards. The Energy Policy Act of 2005 made the electric power sector subject to cybersecurity standards under the jurisdiction of the Federal Energy Regulatory Commission (FERC). The standards drafting relies heavily on the technical expertise of industry experts convened by the North American Electric Reliability Corporation (NERC) working in conjunction with federal regulators to ensure that cybersecurity standards are technically and operationally sound and do not result in unintended consequences. In addition, a memorandum of understanding, and policy

statements by the Nuclear Regulatory Commission (NRC), ensure that there is good coordination between NERC and the NRC so that no gaps in protection exist for nuclear generators.

This unique regulatory regime is a source of pride for the sector as it helps to ensure reliable operation of the electric grid under a common set of standards that have been drafted with input from grid engineers, information technology experts, and federal regulators. And, with respect to cybersecurity, the electric power sector is the only industry with mandatory, enforceable cybersecurity standards (known as Critical Infrastructure Protection, or CIP, standards) and the NRC requirements embodied in 10 CFR 73.54.

Owners and operators of nuclear energy facilities like Exelon are subject to extensive regulation by the Nuclear Regulatory Commission (NRC) to ensure cybersecurity protection. The nuclear energy industry implemented a cybersecurity program in 2002 to protect critical digital assets. In 2009, the NRC built upon this program by establishing cybersecurity regulations for U.S. nuclear reactors and today critical systems used to control these facilities are not connected to the Internet. The requirements in 10 CFR 73.54 provide high assurance that digital computer and communication systems and networks in nuclear power plants are adequately protected against cyber attacks. This level of protection ensures that cyber attacks of nuclear plants do not impact the reliability of the bulk power system. The requirements adopted to implement 10 CFR 73.54 include assessing vulnerabilities and threats on an ongoing basis. The NRC currently inspects nuclear plant implementation of these regulatory requirements. Through these efforts, the electric sector that includes nuclear energy facilities has been and continues to be a leader in private sector efforts to secure critical infrastructure from cybersecurity threats and vulnerabilities.

However, one of the key lessons Exelon and the industry has learned as we have worked to advance our own readiness is that threats and our nation's adversaries evolve rapidly. While standards encourage good business practices and enforce a baseline level of security, standards alone are not sufficient to address cyber threats. Standards may take a long time to develop and can provide a road map for our adversaries to evade security controls. Cyber threats are constantly evolving in real time. They require quick action and flexibility that can come only from constant vigilance and close collaboration with the government and emergency response protocols that are planned and practiced before a disaster strikes.

Since the cybersecurity threat environment is constantly changing, ongoing dissemination of vulnerability and threat information and analysis must play an important role in informing protective actions. There are existing venues for this sort of information sharing, including the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) and the NERC Electricity Sector-Information Sharing and Analysis Center (ES-ISAC), both of which inform the industry on recommended preventative actions.

Having mechanisms for the government and industry to share information with each other to alert electric power companies to potential threats, and providing guidance on mitigation of those threats, illustrates a defense tactic that does not require a formal standard. In fact, these Alerts and Notifications are a valuable tool to rapidly provide more detailed and tactical information to all components, assets and functions of the bulk power system.

Taken together, the standards development process, Alerts and Notifications, and other security services provided by NERC have helped improve grid resilience and the industry's security posture. In addition to developing mandatory cybersecurity standards, NERC's role in informing, convening, and auditing the industry, along with comparable efforts by the NRC, have proven invaluable to grid reliability.

Further Progress on Cybersecurity Protection Requires Information Sharing Legislation and Enhanced Public Private Partnership with Federal and State Governments.

Both the federal government and electric companies have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attacks. The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and electric companies in ensuring the cybersecurity of the nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for ongoing consultation and sharing of information between government agencies and the electric power sector.

However, the private sector can sometimes be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of inherent limitations on its access to intelligence information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric companies are not privy. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operate. Owners, users, and operators of the electric grid are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation.

To this end, the electric sector has long championed cybersecurity legislation that would facilitate greater cooperation, coordination and intelligence sharing between government and the private sector. Thus, the industry appreciates that such a mechanism is built into the legislation that we are discussing today.

CISPA would help address the needs of our companies by providing timely and actionable information from government partners that can help protect electric companies' computer networks. It would address legal and logistical barriers that have limited the sharing of cyber threat information between and among elements of the public and private sectors. In addition, we expect that the information-sharing efforts envisioned in this bill would serve to supplement, rather than replace, the public-private partnerships fostered under the National Infrastructure Protection Plan framework, which continues to mature.

I would add that creating mechanisms for information sharing is only part of the solution. As I know from my role at BG&E serving the NSA, our national defense and intelligence gathering operations require a reliable supply of electricity. Given this reality, it is important that we continue to develop an "operational relationship" at the highest levels of both government and

industry, and then drill on a regular basis to ensure that, in times of crisis, those with relevant information and operational expertise can operate and communicate seamlessly and quickly.

We are pleased that both the government and industry are embarking on an innovative and cooperative approach to senior-level coordination, with both sides committing their expertise and leadership to keep the bulk electric grid as secure and resilient as possible. Following recommendations in an October 2010 report to the President by the National Infrastructure Advisory Council (NIAC), the electric power industry proactively contacted the Obama Administration and has begun working to improve coordination with the government at the most senior levels.

Under the auspices of the NIAC report, several electric utility CEOs have recently initiated what we hope will be an ongoing collaboration with key White House staff and other senior officials throughout the government. This recent collaboration has already resulted in multiple classified briefings to make senior industry executives aware of the full scope of the threats facing the electric grid, as well as a commitment from government representatives to improve the flow of information between the government and industry. Other goals for this government-industry partnership include addressing legal, technical, and procedural hurdles associated with the deployment of proprietary government technology on utility networks to improve real-time situational awareness, and a directive to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

Technology, in particular, is a key focus of this engagement. The recent defense industrial base pilot project is a key model for demonstrating how government cyber threat intelligence can be shared with the private sector in an operationally usable manner. Our industry has also worked closely with national security agencies in deploying new technologies to assess and combat cybersecurity challenges in connection with recent events like the G-8, G-20, and NATO summits. Employing new technology in collaboration with national security agencies is critical to addressing cybersecurity.

Interdependence of critical infrastructure requires cross-sector and intergovernmental coordination.

Finally, I would like to extend thanks for the Chairman and Ranking Member's recognition that a multi-sector approach is needed to address cybersecurity. While EEI, EPSA, and Exelon's interest lies with protecting the electric grid, the interconnected nature of critical infrastructure requires a comprehensive approach to cybersecurity. Electric companies, for example, rely on telecommunications systems to operate the grid, pipelines to help fuel our generation, water to cool our systems and create steam, and wholesale markets to sell our product. Should any of these critical sectors be compromised, the electric grid could be impacted as well. Likewise, each of these sectors relies on the electric grid for the power they need to operate.

The approach CISPA takes recognizes this truth; I would urge the Congress to follow your leadership and approach this issue in a holistic manner. Your legislation also recognizes that over-classification of sensitive information can actually be detrimental to security. While electric companies understand the value of controlling access to national security information,

stovepipes are not the answer. When it comes to cybersecurity, it is impossible to know in advance what piece of information may be integral to a company's—or the nation's—own defense. If an electric company observes an anomaly and has no mechanism for sharing that with the government or with another sector, we all lose. We need a reasonable process to share potentially important information with the government and each other. As an adviser to President Obama said just last week: "The government needs to accept more risk in sharing information."

As the CEO of an electric and gas utility, I take very seriously our responsibility to ensure that our customers' personal information and data are protected. While I am aware that some have raised concerns regarding the potential impact of CISPA on privacy rights, we believe that the voluntary exchange of information between the public and private sector that CISPA would facilitate is not inconsistent with the safeguarding of our customers' data and personal information.

Finally, much of this testimony has discussed information sharing across critical infrastructure sectors and between the federal government and industry. I would like to mention another issue relevant to the electric sector. As you know, portions of our infrastructure are regulated by both the Federal Energy Regulatory Commission (FERC) and state utility commissions. While the focus of this Committee is national security, federal, state, and local governments need to be heard when it comes to issues that impact their jurisdiction. This, again, is largely a function of information sharing. I am not aware that FERC or any state commission would deny cost recovery for utility expenditures made in the name of national security. However, all commissioners need to be informed of the prudence of these costs. This is of particular significance to competitive wholesale power suppliers that may have no ability to recover such costs through rate base. As you consider the various audiences that need to be engaged in an information-sharing regime, please recognize the role public utility commissions play.

Conclusion

Critical infrastructure is deemed as such because it is critical to national security. On behalf of owners and operators of electric critical infrastructure, Exelon, EEI, and EPSA appreciate the Committee's urgency and desire to get information into the hands of industry so we can be active in our own defense and the defense of the nation.

Promoting clearly defined roles and responsibilities, as well as effective processes for ongoing consultation and sharing of information between government and the private sector, is the best approach to improving cybersecurity. Each cybersecurity situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the electric grid.

Our industry remains fully committed to working with the government and industry partners to increase cybersecurity, and we appreciate your efforts to advance legislation that would create such a framework.

Thank you again for the opportunity to appear today, and I would be happy to answer any questions.