Sue Kelly

President & CEO

American Public Power Association

Testimony before the Senate Energy and Natural Resources Committee on:

"Keeping the Lights On – Are We Doing Enough to Ensure the Reliability and Security of The U.S. Electric Grid?"

April 10, 2014

The American Public Power Association (APPA), based in Washington, D.C., is the national service organization for the more than 2,000 not-for-profit, community-owned electric utilities in the U.S.. Collectively, these utilities serve more than 47 million Americans in 49 states (all but Hawaii). APPA appreciates the opportunity to provide the following testimony for the Senate Energy and Natural Resources Committee's hearing regarding "Keeping the Lights on – Are We Doing Enough to Ensure the Reliability and Security of the U.S. Electric Grid?"

APPA was created in 1940 as a nonprofit, non-partisan organization to advance the public policy interests of its members and their customers, and to provide member services to ensure adequate, reliable electricity at a reasonable price with the proper protection of the environment. Most public power utilities are owned by municipalities, with others owned by counties, public utility districts, and states. APPA members also include joint action agencies (state and regional entities formed by public power utilities) and state, regional, and local associations that have purposes similar to APPA.

Introduction

The associations in our industry represent a broad variety of stakeholder interests, including investor-owned, cooperatively owned and publicly owned utilities, independent generators, and Canadian utilities. For very legitimate reasons, we often have different views on the policy issues facing our industry. On the issue of the security of the electric bulk-power system, however, we have come together. APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electric Power Supply Association, the Large Public Power Council, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group (associations) have all supported the mandatory electric reliability regime created by the Energy Policy Act of 2005, that applies to the reliability, cyber-security, and now physical-security of the bulk electric system. In recognition of the changing nature of threats to the security of the grid, particularly cyber-threats given their rapidly evolving nature, we have also worked with the Departments of Energy and Homeland Security to expand and elevate the focus of the Electric Sub-sector Coordinating Council (ESCC), which I will discuss in more detail below. Given our similar positions on these issues, this testimony has been endorsed by these associations.

In this testimony, I will discuss physical-security and its importance to the reliability and overall security of the electric grid. Next, I will focus on the importance of cyber-security and the need for limited liability protection. And finally, I will detail how electric utilities address cyber- and physical-security constantly

and simultaneously. (For the purposes of today's testimony, I use the phrase "grid-security" as representative of both cyber- and physical-security.)

Electricity, the movement of electrons, occurs naturally. But to serve industrial, commercial and residential needs for lighting, heating, cooling, refrigeration, computers, and many other daily needs, large amounts of moving electrons must be generated from some other fuel or energy source. Electricity is created from the conversion of a fuel or other source of energy into electrons. Once electricity is generated, it travels over high-voltage bulk power transmission lines to the lower voltage distribution systems where it will be delivered to homes and businesses and consumed. This all happens instantaneously, at nearly the speed of light, making the reliable operation of the electric grid a "24 hours-a-day, seven-days-a-week" job. Furthermore, once electrons flow from the generating unit to the grid, their path cannot generally be controlled. Therefore, the approximately 1,900 owners, users, and operators of the bulk power grid (comprised of the generating facilities and high-voltage transmission lines where electrons freely flow) must work together constantly to ensure security and reliability.

PHYSICAL-SECURITY

While cyber attacks, meteorological events, and terrorist acts have driven much of the public discussion on grid security in recent years, APPA's members and the entire sector have for decades planned for threats to physical security. Unlike cybersecurity threats, which are constantly evolving, many of the threats to physical infrastructure have been identified for years, if not decades, and are more readily understood than potential cyber threats. Electric utilities, including public power utilities, take these threats seriously, and deploy measures to mitigate such threats. At the same time, the sheer size and in some cases, remoteness, of the infrastructure requires that utilities prioritize facilities that, if damaged, would have the most severe impacts on the ability of utilities to "keep the lights on." This risk-based approach enables the industry to prioritize the most important assets, and also allows it to change that prioritization over time. The bulk electric system continually evolves because assets that impact the system change over time. For example, the retirement of a large coal plant might lead to greater reliance on a mix of natural gas based generation, distributed generation, and large wind and renewable projects, which would make very different use of the existing network and require substantial new transmission to reliably serve customers (also known as "load"). This new mix of generation and transmission will present different security risks as well, which the industry analyzes and accounts for in the planning process.

The nation's electric distribution systems have always been, and are today, regulated by state and local governments. Congress "hard-wired" this deliberate separation of jurisdiction into the Federal Power Act (FPA). APPA believes this division of jurisdictional responsibility is appropriate, given the retail nature of distribution systems and the vast differences in the configuration, size, and ownership of the approximately 3,000 distribution utilities in the U.S., approximately 1,900 of which impact the bulk electric grid. Each individual utility's role in the security of its distribution facilities is unique, due to these substantial differences.

Electric utilities intimately understand the importance of physical security and have longstanding programs and protocols designed to protect their utility systems. As the nature of physical threats has changed over the years (in response to the rising number of incidents of copper theft, for example), electric utilities have planned, prepared, and responded accordingly. Today, due to the increased threat of security breaches such as malicious vandalism and potential terrorist attacks that can cause damage to this infrastructure, utilities must develop the best available mitigation practices to address such attacks.

Simple risk mitigation techniques like cameras and locks help utilities deal with routine problems. The key to electric utility physical-security, however, is its "defense-in-depth" approach that incorporates resiliency, redundancy, and the ability to recover, should an extraordinary event occur. While our systems are built to withstand attacks, successful attacks may still occur even with such planning. We use modeling to assess criticality and to build redundancies into the system to support our most critical assets. By modeling, we can determine how a specific event would require power to be re-routed, which equipment would need to be taken off- or brought on-line, and in extreme conditions, the amount and location of customer load (demand) that must be shed to keep the interstate grid as a whole online and prevent any potential damage to utility equipment that might lead to extended outages.

With these plans in place, we can also determine the criticality of individual assets on our systems. While determining what is critical is complicated, numerous models that incorporate both government and industry priorities help to narrow the focus to a manageable group of assets that need to be treated as priorities. Since there are over 45,000 substations in the United States, this focused planning is very important. Once identified, utilities make the necessary investments to secure these assets and put in place the necessary redundancies to ensure a quick recovery, should they go down. As our adversaries evolve, so do the risks we face. Certainly, there is no single solution that can make the grid completely safe and secure. But by focusing on a series of strategies to mitigate risks (and by understanding that risk elimination is practically impossible), utilities take every reasonable step to avoid operational consequences related to physical damage to their equipment.

In recent months, a few high profile attacks on physical infrastructure have drawn increased scrutiny. One high profile incident took place at the Metcalf substation on Pacific Gas and Electric's (PG&E) system in California. Though I am told that the FBI believes one person is likely responsible for the damage at Metcalf, this incident demonstrated a level of sophistication not previously seen by the communications and energy sectors. As a result, the entire electric sector has responded to this attack to assess its impacts and to share lessons learned. The Department of Energy (DOE) and Department of Homeland Security (DHS), in coordination with the Federal Bureau of Investigation, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) and industry experts, conducted a series of briefings across the country for utility owners and operators and local law enforcement regarding security of electric substations. These briefings offered an opportunity to grid operators to learn more about the Metcalf attack, was a response to it and other recent acts against the energy sector.

APPA and our electric sector trade association brethren take this incident very seriously. Shooting at substations is, unfortunately, not an uncommon occurrence. But the sophistication of the Metcalf attack and the fact that the perpetrator has still not been apprehended is quite troubling. However, the notion that the *Wall Street Journal* and other recent media stories have suddenly spurred our industry to action, or have somehow enhanced grid security, is inaccurate. The briefings mentioned above were initiated prior to these recent stories. As discussed previously, the threat of physical attack has been part of our planning for decades. The power stayed on in spite of the Metcalf attack – due to cooperation and coordination with other electric utilities in the region, and redundancy in the system that was planned in advance.

As stated previously, the electric power industry (including nuclear power facilities) is the only critical infrastructure sector with mandatory reliability standards. However, given the evolving nature of threats to both physical and cyber assets, we recognize that standards can only go so far in protecting the actual facilities owned and operated by governmental entities, cooperatives, and private utilities. APPA, therefore, supports physical security initiatives at both the bulk power system and distribution levels and has urged all public power utilities to enact security plans that address both physical- and cyber-security. In light of increasing interest in and attention to physical security by the federal government and Congress, APPA believes this issue should be viewed more comprehensively. On March 7, 2014, under its authority granted in FPA Section 215, the Federal Energy Regulatory Commission (FERC) directed

the North American Electric Reliability Corporation (NERC) to submit proposed reliability standards within 90 days that will require utilities with critical assets to take steps, or to demonstrate that they have taken steps, to address physical security risks and vulnerabilities related to the reliable operation of the bulk power system. Again, as contemplated under Section 215, APPA and our members, along with EEI, NRECA, and their members, are offering our expertise to NERC in drafting this important standard.

APPA is grateful for Acting FERC Chairman Cheryl LaFleur's appearance before this Committee today. She and her colleagues at the FERC have a difficult task before them and we applaud their commitment to making the electric grid safer and more reliable. The difficulty in ordering this standard to be crafted was captured by Commissioner John Norris in his concurrence to FERC's March 7, 2014, Order relating to this standard. Noting that measures taken to address physical security need to be reasonable and cost effective, he said:

> As I have said previously, I believe that [the Metcalf] incident is a serious one, and significant efforts should be made to determine who was responsible for the incident, and to identify appropriate next steps to prevent such incidents from happening in the future. But, it has been well understood for decades that our nation's grid has been vulnerable to physical attack. We simply cannot erect enough barriers to protect North America's over 400,000 circuit miles of transmission, and 55,000 transmission substations. While some locations may require additional physical barriers, I continue to urge caution against over-reaction. I remain concerned that the recent momentum will result in the electricity sector potentially spending billions of dollars erecting physical barriers to protect our grid infrastructure. I am particularly troubled because most if not all of those costs will be passed through to ratepayers.

APPA, as a trade association of not-for-profit utilities, shares Commissioner Norris' concerns and hopes that NERC's physical security standards will be appropriately drafted to protect truly critical infrastructure and ensure that expenditures in this area are reasonable and needed.

While this will be NERC's first standard on physical security, NERC's Critical Infrastructure Protection Committee (CIPC), has recently produced industry guidance on physical security. Also, FERC has recently approved NERC reliability standard EOP-004-2 (Event Reporting), which requires reporting of physical attacks at bulk electric system facilities. The industry also relies on the NERC Electricity Sector Information and Analysis Center (ES-ISAC) to provide industry alerts of physical attacks on electric facilities.

CYBER-SECURITY

At the top of APPA's priorities, and our members' priorities, is the safety, security, and reliability of the U.S. electric grid. By protecting the facilities they own and operate and by following increasingly robust cyber- and physical-security protocols, public power utilities play an important role in the safety and reliability of the grid. APPA's commitment to safety and reliability is not unique in the electric sector—cooperatively and investor-owned electric utilities all share this commitment. That is why our industry collaborated on the mandatory reliability regime spelled out in the Energy Policy Act of 2005 (EPAct05), and now incorporated in Section 215 of the Federal Power Act, as mentioned above. The electric sector participates, in partnership with Congress, FERC, and NERC, in an ongoing effort to establish and enforce comprehensive standards to strengthen the grid, including those that enhance cybersecurity. APPA believes the best way to support these ongoing efforts and to enhance security across critical infrastructure sectors is by improving information sharing between the federal government and such sectors, and vice versa.

As the grid evolves, unfortunately, so do threats to its integrity. Thus, APPA recognizes that new -- but narrowly crafted and limited -- authority may be necessary to fully address emergency threats. The threat of cyber attack is relatively new compared to long-known physical threats, but an attack with operational consequences could occur and cause disruptions in the flow of power if malicious actors are able to hack into the data and control systems used to operate our electric generation and transmission infrastructure. While APPA believes that the industry itself, with NERC, has made great strides in addressing cyber-security threats, vulnerabilities, and potential emergencies, we recognize that any true national emergency will warrant involvement from many federal entities.

To date, the electric utility sector's FPA Section 215 processes coupled with our actions beyond this Section 215 regime have prevented a successful cyber attack causing operational consequences on the bulk electric system. However, the years since full implementation of Section 215 began in 2007 have been marked by jurisdictional debates within the Executive Branch agencies and between the Executive Branch and Congress regarding the appropriate response to the cyber threat regime faced by all critical infrastructure sectors, with some questioning the NERC/FERC standards and calling for more regulation and others focused on enhanced information sharing.

This regulatory partnership between the federal government and the electric sector has proven to be one marked by continuous ongoing improvements in communication, technology, and preparedness as the standards have evolved since 2007. APPA and its members, as well as other utilities, also continue to work on the NERC Critical Infrastructure Protection (CIP) standards on cyber-security. As cyber attacks are ever-changing, so must be the nature of our defenses. As such, CIP Version 3 is in effect and enforceable. Version 5 has been approved by FERC, and is proposed to be enforceable by April 1, 2016. We will continue to enhance these mandatory standards and the independent actions we take to protect our critical cyber assets.

A Note on Liability Protection

There has been discussion in this and other committees relating to providing limited liability protection as an incentive for participation in national cyber-security frameworks. Utilities certainly need no incentive to secure their systems and protect their customers. However, a federal limit on potential legal repercussions to utilities when they are assisting their government partners with national security or for following federal requirements are certainly worth further discussion. Regulatory and legislative proposals from the Obama Administration and Congress focus largely on the steps electric utilities can take to protect and secure their facilities, ensure reliability, and maintain security of customer data. At the same time, it is important to establish guidelines to ensure that unwarranted and counterproductive lawsuits are avoided when utilities are actively engaged in cyber-security and compliance with federal guidelines or regulations. APPA is concerned that electric utilities may not be sufficiently protected from negligence claims alleging they failed to protect against such attacks even when they have taken reasonable precautions.

Some states are considering legislation to address liability related to cyber attacks, but no state or federal statutes currently exist to specifically protect electric utilities, including public power entities, from lawsuits in response to a cyber incident. This leaves APPA's members, which are units of state and local government operating on a not-for-profit basis, vulnerable to time-consuming and expensive litigation even when they are undertaking activities to protect their systems.

Utilities already treat their customers' safety and security as priorities. As the owners and operators of the nation's electric grid, however, we have a unique responsibility to come together in support of national security. Combining and sharing threat information among ourselves and with the federal government

will make the nation safer. Utilities should be able share and receive any relevant threat information without fear of retribution in the courts or regulatory proceedings. Limited liability protection would allow utilities facing cyber attacks to share threat information with relevant state and federal law enforcement agencies and, possibly, with other utilities and would result in increased grid security. Failure to provide these protections to our sector could have a chilling effect on information sharing.

Though the White House considers liability protection to be a priority, the Executive Order on Cybersecurity, issued by President Obama in February 2013, and the corresponding Cybersecurity Framework issued by the National Institute of Standards and Technology (NIST) in February 2014, do not include liability protections for cyber attacks. This and previous Congresses have considered legislation focusing on cyber-security proposals which have included provisions that would grant liability protections to critical infrastructure owners and operators affected by cyber incidents, but no such protections have been enacted into law. Therefore, APPA and the associations support legislation that would protect utilities from liability for cyber incidents, when the utilities have taken appropriate, reasonable steps to shield against such attacks.

THE GRID SECURITY PARTNERSHIP

Partnership, coordination, and sharing of relevant threat information are crucial to grid security. At the national level, as mentioned above, the ESCC, a public/private partnership between the utility sector and the federal government, plays an essential role in coordination and information sharing. Each of the 16 critical infrastructure sections identified in Homeland Security Presidential Directive 7, which outlines national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks, has its own sector coordinating council. Electric utilities are one of only two sectors regulated by a mandatory compliance framework (see above). In October, 2010, the White House's National Infrastructure Advisory Council (NIAC) recommended an "executive-level dialogue with electric and nuclear sector CEOs on the respective roles and responsibilities of the private sector in addressing high-impact infrastructure risks and potential threats… ." This recommendation led to the creation by the electric utility sector of the Joint Electric Executive Committee, which then transitioned into its current role as a revised and expanded ESCC.

The ESCC includes representatives from electric trade associations, including APPA, EEI, NRECA, the Canadian Electricity Association, the Electric Power Supply Association, the Nuclear Energy Institute, the RTO/ISO Council, NERC, and the NIAC, as well as CEOs of public power utilities, investor-owned utilities, rural electric cooperatives, the Tennessee Valley Authority, and the federal Power Marketing Administrations. As part of the "executive level dialogue" initiated by the 2010 NIAC recommendation, ESCC members engage in regular coordination and discussion with federal officials from the White House, relevant cabinet-level agencies, federal law enforcement, and national security organizations. This dialogue is currently focused on three areas: Tools & Technology (deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid); Information Flow (making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner); and Incident Response (planning and exercise coordinated responses to an attack).

To support the ESCC's mission, a Senior Executive Working Group (SEWG) of utility Chief Operating Officers and Chief Information Officers, utility trade association executives, and other senior executives who have relevant experience in the electric power sector has been established. The SEWG meets by phone on a monthly basis and creates ad hoc "sub-teams" to accomplish goals identified by the CEOs and Cabinet Deputy Secretaries participating in the ESCC. In parallel to this effort, the government has organized around these same goals with a commitment to align government and industry efforts. The

ESCC has also helped to enhance industry-government partnerships between electric utilities and law enforcement agencies at the federal, state, and local levels.

Protecting critical infrastructure is a shared responsibility between industry and government. While the government has a law enforcement responsibility and a national security mandate, utility owners and operators own the assets, pay for (via their customers) protection of the assets, and have the operational expertise to keep the lights on. Our industry continuously invests in security measures that protect the grid against evolving threats and to make it more resilient and robust, based, in part, on regular ESCC and ES-ISAC updates on evolving national security threats. We look at all hazards and threats, be they cyber, physical, or natural disasters when protecting our systems. Most recently, a two-day exercise (GridEx II) was held to help drill and prepare for extraordinary scenarios. More than 200 industry and government organizations participated in the grid-wide, international event. There was also an executive tabletop exercise that brought together senior Administration officials and senior utility executives to address the roles and responsibilities of both government and industry in the event of a major power disruption due to national security threats.

In conclusion, APPA, on behalf of the entire electric utility industry, would like to reaffirm the industry's ongoing commitment to protect critical electric utility infrastructure from both cyber and physical threats. To do this, we need to work in partnership with all levels of government, from local law enforcement to Cabinet level executive departments. Information sharing with the assurance of confidentiality, provision of tools and technologies to assist electric utilities in better protecting their assets, and liability protection for utilities that take reasonable measures to protect their systems are all important elements of such a partnership. Thank you for the opportunity to appear before you today to address these issues.