Testimony of Mr. Duane D. Highley

President and CEO of the Arkansas Electric Cooperative Corporation (AECC)

to the Committee on Energy and Natural Resources

Subcommittee on Energy

U.S. Senate

July 12, 2016

Introduction

Chairman Risch, Ranking Member Manchin, and all members of the Committee, thank you for inviting me to testify before your committee on this very important topic, it is an honor. I am here today to testify about security in one of the 16 critical infrastructures within the United States, the electric portion of the energy sector, on behalf of the Arkansas Electric Cooperatives Corporation (AECC) and the National Rural Electric Cooperative Association (NRECA). After I give you a little back ground about myself and those I am representing today I will discuss our current practices which help guard against and recover from energy disruptions including private-public partnerships, processes, and regulations.

As an engineer with 34 years' experience in a sector that many call the most critical of the critical, I continuously strive along with other owners and operators in the sector to ensure reliable, resilient and affordable power so that our communities and neighbors can depend on the light switch in their homes and businesses.

I serve as President and CEO of AECC, a not-for-profit power supply system serving 17 distribution systems, who in turn serve about 1 million Arkansans. I report to a democratically-elected board representing the customers we serve. Arkansas Electric Cooperative Corporation (AECC) was created in 1949 and provides power for more than 500,000 farms, homes and businesses served by our 17 electric distribution cooperative owners. AECC relies on a diverse generation mix to serve its members, including hydropower, natural gas, coal, biomass, wind and solar.

In addition, I also serve as President and CEO of Arkansas Electric Cooperatives Inc. (AECI), which provides construction, right-of-way, and electrical products to utilities across the U.S. A new AECI subsidiary, Today's Power Inc. (TPI) develops utility scale community solar projects and other products to enable household distributed generation.

The electric cooperatives of Arkansas are members of the National Rural Electric Cooperative Association (NRECA), a service organization for over 900 not-for-profit consumer-owned electric utilities serving over 42 million people in 47 states. Electric cooperative service territory makes up 75 percent of the nation's land mass and includes over 19 million businesses, homes, schools, churches, farms, irrigation systems, and other establishments in 2,500 of 3,141 counties in the U.S. NRECA's membership includes 65 generation and transmission (G&T) cooperatives, which provide wholesale power to distribution co-ops through their own generation or by purchasing power on behalf of the distribution members. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent.

As member owned not-for-profit utilities, distribution cooperatives and G&Ts reflect the values of our membership, and are uniquely focused on providing reliable energy at the lowest reasonable cost. We have to answer to our owners and justify every expense to them. There is never any debate as to whether a proposed project will benefit our shareholders or our customers, because they are one and the same.

I also serve as a co-chair of the Electricity Subsector Coordinating Council (ESCC), a public/private partnership outlined in the National Infrastructure Protection Plan (NIPP) for critical infrastructure owners and operators to serve as the sectors' principal entity with the government on policy-level security issues. Though membership of these councils do vary dramatically across the critical infrastructure sectors, in the electric sector the council is composed of 30 utility and trade association CEOs, representing all segments of the electricity industry, and it engages regularly with its government counterparts, including, senior Administration officials from the White House, Department of Energy (DOE), Department of Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the Federal Bureau of Investigation (FBI) and others as needed.

Electric Sector Security

Often news headlines about cyber or physical threats to the electric grid focus on far-fetched scenarios and sensational claims. However, though there are real threats to the grid, the scenarios put forth for public consumption are rarely reflective of the real threat environment but rather disproportionally put forth the highest consequence scenarios that are less likely to occur. Many of these scenarios would constitute acts of war on the United States that would directly impact more than just the electric sector.

Protecting the nation's complex, interconnected network of generating plants, transmission lines, and distribution facilities which make up the electric power grid to ensure a supply of safe, reliable, secure and affordable electricity, is a top priority for the electric power industry.

Defense in Depth

We didn't intentionally design the electric grid to defend against intentional attack and acts of war, but fortunately our normal preparations against severe weather and equipment failure serve us well in limiting the potential impact of intentional actions. This approach to protecting critical assets is known as defense-in-depth. To protect against extreme weather events, vandalism and major equipment failure a high level of redundancy is built into the power supply system. The grid is designed to reliably deliver the highest possible summer or winter peak load demand with the most critical facilities out of service – that is our standard. Because of this we have withstood intentional attacks such as the 2013 California and Arkansas substation attacks with no loss of customer service, despite severe damage to our infrastructure.

The grid is incredibly resilient – imagine the worst ice storm – thousands of poles and wires down – and even in these severe cases service is usually restored in days or at most a couple of weeks – longer outages are extremely unlikely. From drafting plans, to coordinating with our partners, private sector and government alike, to assessing and mitigating risks including building in a multitude of redundancies, we are continuously working to ensure outage times are minimal if and when they do occur.

The electric power industry continuously monitors the bulk electric system and responds to events large and small. Consumers are rarely aware of these events primarily because of the

sector's routinely planning, coordinating, and responding to take care of them. In the cases where an event impacts the consumer, these same activities, in addition to the decades of lessons learned from supplying power, have helped ensure there are hazard recovery plans in place for working within the sector and with government counterparts to get the power back on.

It is critical that one threat doesn't get prioritized over any other simply due to media sensationalism or fear mongering. The concept of an act of war on the United States via a nuclear device detonated above the earth causing an electromagnetic pulse (EMP) wiping out all microprocessors within the impact radius – not just ones utilized by those who own or operate the grid – is a great example. There is often a focus in discussion in the media on only the grid in these scenarios and the concept of a magic bullet that can protect the whole infrastructure from a nuclear attack. The grid relies on other critical infrastructures for fuel, water for generator cooling and telecommunications to support quick recovery from a storm or other event. As those infrastructures would also be impacted by an EMP event, the focus on only one infrastructure could result in a misappropriation of critical resources.

In order for the electric sector to better understand the true potential of the EMP threat and potential mitigation options, a number of electric utilities, including electric cooperatives, are funding research through Electric Power Research Institute (EPRI). It is possible that the shielding built into the current generation of electronic equipment, which allows it to function amidst continual gigahertz interference from cell phones and microwave ovens, may also provide some protection for EMP. We need to work based on facts, not speculation.

Again, defense in depth and system redundancies are helping electric utilities to keep the grid reliable and secure. This will continue to be our first and best defense to any event.

Value in Partnerships & Information Sharing

The industry has decades of experience working together to protect our shared infrastructure and is constantly reevaluating threats and taking steps to protect the system as well as plan for its recovery. Electric cooperatives make protection and security of their consumer-members' assets a high priority. NRECA, their member cooperatives, industry partners and government agencies work closely to develop effective approaches to protecting the electric system. One example is the Cybersecurity Capability Maturity Model (C2M2) a public-private partnership effort that supports the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework by assisting organizations – regardless of size, type or industry – to evaluate, prioritize, and improve their own cybersecurity capabilities. This tool was then customized for electric utilities through the creation of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

To further bolster the efforts of C2M2 for electric cooperatives specifically, NRECA's Business and Technology Strategies (BTS) developed a "Guide to Developing a Cyber Security and Risk Mitigation Plan" which includes tools and processes cooperatives (and other utilities) can use today to strengthen their security posture and chart a path of continuous improvement. All co-ops participating in NRECA's Regional Smart Grid Demonstration are using these tools to develop a smart grid cyber security plan. The continued engagement on development and

improvement to cybersecurity programs and tools – combined with access to actionable relevant information, both classified and unclassified – is vital when it comes to security postures in critical infrastructures.

As mentioned earlier, the ESCC serves a role in these efforts as a place for the sector to work with government to coordinate policy-level efforts to prevent, prepare for, and respond to, national-level incidents affecting critical infrastructure. The major trade associations and industry work together with government to improve cyber security through the ESCC. These efforts include: planning and exercising coordinated responses; ensuring that information about threats is communicated quickly among government and industry stakeholders; and deploying government technologies on utility systems that improve situational awareness of threats. At the most recent meeting of the ESCC, the government and private sector worked on a number of issues including identifying R&D needs, developing a cyber mutual assistance program, and gaining a better understanding of the Fixing America's Surface Transportation (FAST) Act provisions.

We stand ready to continue our work with our government counterparts and begin the transition into the next administration.

In addition to pulling industry leadership together with government leadership throughout the year, the ESCC also serves an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC collects and promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is handled confidentially and distributed through NERC's secure portal directly to industry asset owners and operators.

Mandatory and Enforceable Standards

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives work closely with the rest of the electric industry, the North American Electric Reliability Corporation (NERC), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

Approximately 60 generation and transmission and 60 distribution cooperatives must comply with some portion of NERC's reliability standards based on the criticality of the bulk electric system assets they own and operate. Since 2007, when NERC standards (reliability and cyber security) become mandatory, electric cooperative representatives have participated in numerous NERC standard development activities and those cooperatives with compliance responsibilities have been working to both comply and to demonstrate compliance through scheduled NERC audits. When covered entities are found to have violated cyber security and/or other NERC standards, they can be subjected to fines as high as one million dollars per day per violation. Sizable fines have been levied when entities have been found in violation and as a utility CEO I can tell you that we take compliance with the NERC standards very seriously.

The NERC standards development process begins with input from industry experts. After approval by industry, the NERC Board of Trustees is asked to approve the standards, which, if approved, are then submitted to FERC for their approval. Upon FERC approval, the standards become mandatory and enforceable. The electric utility Industry recently developed standards on physical security and geomagnetic disturbances (GMDs) and continues to revise and develop additional cyber security and GMD standards. NERC also has an "alert system" that provides the electric sector with timely and actionable information when a standard may not be the best method to address a particular event or topic.

How Congress Has Helped

In the first half of the 114th Congress, legislation was passed that will assist efforts in securing the grid – thank you.

As mentioned previously, the Fixing America's Surface Transportation (FAST) Act was enacted last year, P.L. 114-94, with a number of helpful provisions including:

- A plan for the Department of Energy to create a plan for a strategic transformer reserve program which assists in all-hazard recovery planning for large scale events;
- Clarification of roles and authorities when there is an imminent threat to the bulk power system as well as identifying DOE as the official lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector – it was already the SSA for the sector but this was clarified to include cyber;
- FOIA exemptions for "critical electric infrastructure information" (CEII) submitted by industry to the Federal Energy Regulatory Commission (FERC) and other federal agencies.

Also enacted into law in the first half of the 114th Congress was the Consolidated Appropriations Act of 2016, P.L. 114-113, which included long-sought legislation to promote robust, multidirectional voluntary information-sharing about cybersecurity threats between and among federal agencies and critical infrastructures, including the utility industry. The implementation of this new law is still in its infancy, and the first milestones with final guidance on how to share is still in process.

How Congress Can Help

An example of where government can improve information sharing with industry is the December 2015 Ukraine event. While the content of the classified and unclassified information from the government was very helpful, the timeliness of getting specific, actionable information to industry must be improved so that we can respond as quickly as possible.

Critical infrastructure owners and operators are aware the biggest threats tend to be those that are hardest to identify – the insider threat. We urge Congress to consider legislation giving the FBI the statutory authority to assist industry with fingerprint-based, criminal and terrorist database background checks for industry-determined personnel that perform critical functions.

This would assist industry in further mitigating risks in a way we cannot accomplish at the local and state levels.

S. 3018, the Securing Energy Infrastructure Act

When I was invited to testify today I was asked to not only discuss ways the sector already protects and guards against threats to the electric grid but to also specifically speak to S. 3018, the Securing Energy Infrastructure Act. This legislation creates a pilot program to study vulnerabilities and consider new and old solutions for isolating and defending industrial control systems (ICS) which would likely be applicable to many outside of the electric sector. Participation in the study would be voluntary and includes an appropriately diverse working group. These are good goals and intentions – not all that different from those of the owners and operators who regularly consider and look at these issues nor their regulators who are tasked with overseeing a sector which utilizes ICS. However, it is important to avoid a one size fits all strategy. For example, security issues relevant for an entity on the bulk electric system may be very different from another entity due to geography, engineering architecture and redundancies among other differences, just as security issues relevant for the bulk electric system are not necessarily equivalent to issues facing the local distribution system.

Cooperatives believe building and investing in partnerships will be vital as the industry navigates this dynamic environment. We are implementing a coordinated and collaborative effort across the electricity sector to respond to threats and to vigilantly modify our tactics as needed to keep pace with these threats. For instance, NRECA's research arm mentioned earlier in my testimony, the Business and Technology Strategies (BTS) unit, leads a highly regarded $5 million cyber security research program. BTS develops products to improve the cyber security capabilities of our members, including a cutting edge early warning system, called Essence, which detects unusual changes in the behavior of a system resulting from a cyber-attack.

Conclusion

Thank you for holding today's hearing on this very important issue. I am proud of the efforts of our sector and hope that my testimony helps the Committee to better understand a few of the many activities and collaborative efforts of our industry and our federal government partners.

In closing, I thank you again for inviting me to testify today and I look forward to your questions.