Testimony of Mr. Duane D. Highley

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

to the Committee on Energy and Natural Resources

U.S. Senate

April 4, 2017

Introduction

Chairwoman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify before you on this very important topic, it is an honor. I am here today to testify on behalf of the Arkansas Electric Cooperatives Corporation (AECC) and the National Rural Electric Cooperative Association (NRECA) about efforts to protect U.S. energy delivery systems from cyber security threats. First, a little background about myself and those I am representing today prior to getting into how we guard against and recover from energy disruptions utilizing private-public partnerships, processes, and regulations.

As an engineer with 34 years of 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, which in turn serves over 1 million Arkansans. I report to a democratically-elected board consisting of the customers we serve. 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. AECI's subsidiary ERMCO is one of the largest manufacturers of distribution transformers for utilities nationwide. AECI's newest subsidiary Today's Power Inc. (TPI) develops utility-scale, community solar projects and produces do-it-yourself solar kits 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 42 million people in 47 states. Electric cooperative service territory covers 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 on the market.

As member-owned, not-for-profit utilities, distribution cooperatives and G&Ts reflect the values of our membership, and they 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 one of the three co-chairs who jointly lead the Electricity Subsector Coordinating Council (ESCC), a public/private partnership of the type 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 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.

Cyber Security in 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 electric co-ops and other segments of the electric power industry.

Often news headlines about cyber or physical threats to the electric grid focus on far-fetched scenarios or sensationalized claims. However, though there are real and legitimate threats to the grid, the scenarios most often put forth for public consumption are rarely reflective of the real threat environment but rather disproportionally emphasize the highest consequence scenarios that are the least likely to occur. Many of the more dramatic scenarios would constitute acts of war on the United States that would directly impact more than just the electric sector. In addition, these news headlines don't take into account our expert operator actions and plans that each and every day work to ensure reliable and resilient electricity.

Defense in Depth

We didn't originally design the electric grid to defend against intentional physical or cyber attacks nor 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 even when our most critical facilities are out of service – that is our standard. Because of this we have withstood intentional attacks such as the 2013 California substation and Arkansas transmission line 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.

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

As mentioned earlier, the ESCC serves a vital role in 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 by industry CEOs from all segments of the electricity sector and their government counterparts 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: transition planning; identifying R&D needs; fostering a better understanding and protection of our mutual dependencies through cross sector engagement including joint exercises and sharing information; a cyber mutual assistance program, and gaining a better understanding of the Fixing America's Surface Transportation (FAST) Act's provisions and implementation.

In addition to pulling industry leadership together with government leadership throughout the year and all of the hard work they do, 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 North American Electric Reliability Corporation's (NERC) secure portal directly to industry asset owners and operators.

The E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership co-funded by the Department of Energy (DOE) and industry that seeks to facilitate timely bidirectional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry with near real-time exchange of machine to machine information. This is a great example of efforts to bridge the divides between classified space and sharing actionable, relevant information with private industry.

We appreciate efforts of the new administration in meeting with ESCC leadership recently to work on the transition and ensure our existing partnership and associated initiatives continue to advance without any loss of momentum. We stand ready and intend to continue our work with our government counterparts, across sectors and with each on ensuring a secure, reliable and resilient grid from all-hazards.

It Takes a Toolbox: Additional Tools and Resources

When it comes to cyber security a toolbox with many different tools, resources and options allowing flexibility is necessary – there are no "silver bullets". For the electric sector this includes, but is not limited to: cyber assessments; guidance; tools and resources for small and medium entities; Cyber Mutual Assistance programs; as well as a national industry playbook.

Examples of Cyber Assessments: 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 cyber security capabilities. This tool was customized for electric utilities through the creation of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Example of Guidance: To further bolster the efforts of ES-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 used these tools to develop a smart grid cyber security plan. The continued engagement on development and improvement to cyber security 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.

Tools and resources for small and medium entities: The DOE's Office of Electricity Delivery and Energy Reliability provided funding to NRECA and the American Public Power Association to implement programs that will help utilities improve their cyber and physical security capabilities. In June 2016, NRECA used this funding to create the Rural Cooperative Cyber Security Capabilities Program (RC3). The RC3 Program is designed to assist cooperatives in developing cyber resiliency and security programs. RC3 funding is primarily focused on assisting small- and mid-sized cooperatives with smaller information technology staff, but all of the products and materials developed in RC3 will be available to help all cooperatives. In addition to developing tools and resources RC3 will provide training and guidance to assist cooperatives in assessing their cyber security risks, enhancing their cyber

security capabilities to prevent and mitigate cyber incidents, and implementing cyber security best practices.

Cyber Mutual Assistance programs: The electric sector, including cooperatives, have a unique and effective approach to emergency management and disaster recovery as they have a lot of experience. Following a disaster, cooperatives will rapidly deploy support staff and equipment to emergency and recovery zones to assist sister cooperatives. To help with this process there are Mutual Assistance Agreements, signed by the vast majority of NRECA member electric cooperatives, which formalize the arrangements that have historically been made informally among cooperatives to help each other when disaster strikes. Cooperatives help each other and other electric utilities as needed. Co-ops often work through their statewide organizations, which helps lead coordination efforts to identify in-state and cross-state needs and resources. This culture of mutual assistance can be found across the industry and is being applied to the implementation of the ESCC's recommendation for the formation of a Cyber Mutual Assistance (CMA) Program, a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies. The CMA program is still young but already has 93 members, including 18 cooperatives, participating. What this means is that in the U.S. there are approximately 118 million electricity customers, approximately 80% of all U.S. electricity customers, who are currently served by utilities that participate in CMA.

ESCC Playbook: Most events impacting electric power supply tend to impact a community or a region – not the bulk power system as a whole. However, planning for response and recovery at a national level for widespread events is necessary in a world where terrorists and nation states have an eye toward harming our critical infrastructure. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry is greatly enhancing our nation's ability to defend, protect against and recover from threats to our systems. The ESCC Playbook provides a framework for senior industry and government executives to coordinate response and recovery efforts and communicating to the American public when such a situation arises. The Playbook has been tested and will be an evergreen document that can be updated by industries when lessons are learned from an exercise or real world experiences.

However, it is important to note, that with a national level event, while our society depends on electricity to function, our electricity systems are reliant on other systems including transportation systems for our fuel, water systems for cooling, and telecommunications for operations. When dealing with national events coordination across all these systems is imperative.

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 NERC, the DHS, the DOE, and the 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 last Congress, legislation was passed that assists 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 cyber security for the energy sector – it was already the SSA for the sector but this was appropriately clarified to include cyber;
- FOIA exemptions for "critical electric infrastructure information" (CEII) submitted by industry to the 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 cyber security threats between and among federal agencies and critical infrastructures, including the utility industry.

As the implementation of these new laws is ongoing, it is difficult to demonstrate their importance when it comes to grid security. However, from an industry perspective these were

necessary and important steps forward in clarifying roles, protecting information and planning for all-hazard recovery scenarios – all vital to the reliability of electricity.

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 understand that 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.

Additionally, though we are the only critical infrastructure with mandatory and enforceable standards - developed by NERC, approved by FERC and applicable Canadian governmental authorities - the issue of liability after a cyber event creates serious concerns for the sector. In particular, we are deeply concerned that no matter what steps are taken, our members could face costly and unnecessary litigation in state or federal courts after a cyber event that would serve no purpose. Though the language of the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (the "SAFETY Act") statute, as well as its Final Rule, have always made clear that the protections offered by the law apply to cyber events, in practice there has been some hesitancy on the part of industry to utilize the SAFETY Act to protect against federal claims arising out of cyber attacks due to the requirement that the attack be deemed an "act of terrorism" by the Secretary of Homeland Security before liability protections become available. A legislative clarification that explicitly allows the Secretary of Homeland Security to declare that a "qualifying cyber incident" triggers the liability protections of the SAFETY Act, thereby removing the need to link a cyber attack to an "act of terrorism", would likely go a long way. While state liability actions would remain a concern, the industry and vendors of cyber security technologies and services will be much more likely to use the SAFETY Act program with these clarifications. This would fulfill the law's original intent of promoting the widespread deployment of products and services that can deter, defend against, respond to, mitigate, defeat, or otherwise mitigate a variety of malicious events, including those related to cyber security.

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. As such, funding streams from the Office of Electricity Delivery and Energy Reliability for programs like NRECA's RC3 to help small and medium cooperatives should be protected.

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. We share your goal of protecting the nation's critical infrastructure from cyber threats and appreciate your efforts to address this important national security issue.

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.

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