Testimony of The Honorable Jim Matheson

Chief Executive Officer

National Rural Electric Cooperative Association

to the Committee on Energy and Natural Resources

U.S. Senate

March 1, 2018

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. I am Jim Matheson, the chief executive officer at the National Rural Electric Cooperative Association (NRECA) and I am testifying today on behalf of more than 900 electric cooperatives that are working together to protect U.S. energy delivery systems from cybersecurity threats.

I have served in that capacity since 2016 after serving in the U.S. House of Representatives for 14 years, including serving on the Energy and Commerce, and the Transportation and Infrastructure Committees. I also was a principal at Squire Patton Boggs in Washington, D.C., and worked in the energy industry for several years before my years of government service.

NRECA is the national service organization for America's electric cooperatives. Member-owned, not-for-profit electric co-ops constitute a unique sector of the electric utility industry and provide electricity to more than 42 million people in 47 states. Electric cooperatives are driven by their purpose to power communities and empower their members to improve their quality of life. Affordable electricity is the lifeblood of the American economy, and electric co-ops have provided energy and other services that grow their communities. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve.

America's electric cooperatives serve 56 percent of the nation's landmass, 88 percent of all counties, and 12 percent of the nation's electric customers, while accounting for approximately 13 percent of all electricity sold in the United States. NRECA's member cooperatives include 63 generation and transmission (G&T) cooperatives and 834 distribution cooperatives. The G&Ts are owned by the distribution cooperatives they serve. The G&Ts generate and transmit power to nearly 80 percent of the distribution cooperatives, and those distribution cooperatives provide power directly to the end-of-the-line member-owners. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. NRECA members account for about five percent of national generation and, on net, generate approximately 50 percent of the electric energy they sell. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

In my leadership role at NRECA, I represent electric cooperatives on the Steering Committee of the Electric Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between leadership in the federal government and in the electric power sector, with the mission of coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. Protecting the electric grid from threats that could impact national security and public safety is a responsibility shared by both the government and the electric power sector. The ESCC supports policy- and public affairs-related activities and initiatives designed to enhance the reliability and resilience of the electric grid. The ESCC coordinates with 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.

Addressing Cybersecurity in the Electric Sector

Protecting the nation's complex, interconnected network of generators, transmission lines, and distribution facilities that make up the electric power system, while ensuring a supply of reliable, secure and affordable electricity is a top priority for electric co-ops and other segments of the electric power industry.

The U.S. electric system was originally designed with a focus on safety, reliability and affordability. Today, there are new considerations for the electric system, including intentional physical- or cyber-attacks. Fortunately, our normal preparations to prevent damage from severe weather and equipment failure serve us well in limiting the potential impact of intentional actions. To protect against extreme weather events, vandalism and major equipment failure, a high level of redundancy is built into the power supply system. This includes multiple layers of protection to safeguard assets from cyber threats. The grid is designed to reliably meet the highest possible summer or winter load demand even when our most critical facilities are out of service. That is our industry standard. Because of this, our industry has 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. This approach to protecting critical assets is known as defense-in-depth.

The electric power industry continuously monitors the electric grid and responds to events large and small. Consumers are rarely aware of these events because of system resilience supported by effective planning, coordination and response/recovery efforts. In rare cases where an event does impact electric service, industry resilience and preparedness ensures service is promptly restored in most cases.

The possibility of a cybersecurity attack impacting grid operations is something for which the power sector has been preparing for years. These preparations include:

- Implementing security standards and technologies to protect systems,
- Forging close partnerships to identify threats and solutions, and to respond to incidents,
- Engaging in active information sharing about threats and vulnerabilities,
- Participating in industry and cross-sector disaster planning exercises such as DOE's Clear Path and the North American Electric Reliability Corporation's (NERC) GridEx biannual exercise, and
- Partnering with the DOE, the National Laboratories and other federal agencies on cybersecurity research to improve the tools and resources needed by industry to address cyber threats.

As threats and threat actors continue to evolve, so must the industry's capability to defend against them. Maintaining the resilience and security of the electric grid requires a flexible approach that draws on a variety of tools, resources and options.

Much of the public discourse around cyber- or physical- threats to the electric grid often focuses on far-fetched scenarios, sensationalized claims or misunderstandings of the bulk electric system (BES) function. Facilities that are part of the BES are considered to be the ones that could potentially impact the reliability of the nationwide flow of electricity. The scenarios most publicized are rarely reflective of the real threat environment, and disproportionately 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 and would directly impact more than just the electric sector. In addition, these scenarios do not always take into account our expertise and planning to ensure reliable and resilient electricity delivery.

That is not to say there are not legitimate threats to the grid. They exist. Rather than being reactive or fearful, the electric sector considers the entire threat landscape to ensure grid operations meet high reliability standards. 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 planning and coordinated response to manage these threats. 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 partners to get the power back on.

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

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), DHS, DOE and FERC on matters of critical infrastructure protection, including sharing needed information about potential threats and vulnerabilities related to the bulk electric system. FERC delegated authority from the Energy Policy Act of 2005 to NERC, a private not-for-profit entity, to develop and enforce reliability and cybersecurity standards that protect the BES. The Electric sector today is the only one with mandatory and enforceable standards when it comes to cybersecurity.

Approximately 60 generation and transmission cooperatives and an equal number of distribution cooperatives must comply with some portion of NERC's reliability standards, based on the critical bulk electric system assets they own and operate. Since NERC reliability and cybersecurity standards became mandatory, electric cooperative representatives have participated in NERC standard development activities. Those cooperatives with compliance responsibilities have been working both to comply and demonstrate compliance through scheduled NERC audits. If covered entities are found to have violated cybersecurity and/or other NERC standards, they can be subjected to fines as high as $1 million per day per violation. As the CEO for the association that represents America's electric cooperatives, I can tell you that compliance with the NERC standards is taken 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 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 cybersecurity and GMD standards. Geomagnetic disturbances are initiated by events on the surface of the sun where masses of electrically charged particles of varying levels are hurled toward the Earth, creating the potential for ground-based disturbances due to their interaction with the Earth's magnetic field. When the particles interact with the Earth's magnetic field, especially in certain geographic regions, they can cause ground-induced currents (GIC) and other potentially disruptive phenomena.

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.

Cybersecurity for Electric Cooperatives

Electric cooperatives with NERC compliance responsibilities are subject to scheduled NERC audits. Entities that can impact the BES, our national supply and transmission of electricity tend to have larger IT departments and therefore more resources at their disposal. Those who own or operate components of the BES like electric generation resources, transmission lines or interconnections with neighboring systems must to be concerned about the operations technology (OT) used to support these assets. However, those who are not part of the BES still take cybersecurity very seriously, though often with more of an emphasis on the business or information technology (IT) platforms, which encompass employees, consumers, architecture, and sensitive data. Most states have laws enforcing data security that require compliance from all entities. NRECA is playing a leading role in nurturing a culture of cybersecurity with electric co-ops to help prepare for and respond to cybersecurity challenges – operations and business systems alike. Assessments, awareness, and training are key for helping these entities engage and protect their assets. NRECA's cybersecurity programs provide cybersecurity support and resources to our members at all levels – technical, regulatory, legislative, and legal. In fact, during our Annual Meeting and TechAdvantage event this week we had an opportunity to discuss cybersecurity with our membership and highlighted a number of efforts and resources available for electric cooperatives.

NRECA thanks DOE Secretary Perry and Assistant Secretary Walker for the partnership between the Office of Electricity Delivery and Energy Reliability and electric co-ops to protect our system against cyber threats. DOE provided funding to NRECA and the American Public Power Association to implement programs that will specifically help small- and mid-sized utilities improve their cyber and physical security capabilities. NRECA used this funding to create the Rural Cooperative Cybersecurity Capabilities Program (RC3), which assists cooperatives in advancing their cybersecurity posture. RC3 provides cybersecurity training, services and tools to help our members build stronger cybersecurity programs.

A major priority of the RC3 Program is developing a self-assessment maturity model to enable small- and mid-sized utilities to assess and benchmark their cybersecurity capabilities, and to build a culture of security within their organization. This effort builds on existing work using the DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), a Risk Mitigation Guide NRECA developed with funding from the Office of Electricity in 2011, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. For the past year, NRECA has been field testing this maturity model in a Self-Assessment Research Program.

Cybersecurity is not just the responsibility of IT staff. All employees have the ability—and responsibility—to impact their organization's cybersecurity posture. The Self-Assessment Research Program works with the executive team of a cooperative and helps each member of that team take a hard look at where their cybersecurity efforts are strong and where they can be improved. Through this program, NRECA provides intensive two-day cybersecurity training and has used it to evaluate programs at 36 small- and mid-sized cooperatives in 13 states.

As NRECA continues our work with cooperatives, we are already seeing measureable progress. For example, we are documenting improvements in securing network access, strengthening physical security, and integrating cybersecurity awareness into negotiations with third-party vendors. With continued DOE support, NRECA is working to expand this program to more of our members.

In addition, the RC3 Program held six Cybersecurity Summits in 2017 that provided staff representing 151 cooperatives cybersecurity training. "Every presentation provided something I could take home to benefit our company," said one attendee. The most valuable aspect of the summits was the opportunity for co-ops to come together and discuss cybersecurity challenges and solutions. With continued support from DOE, NRECA will hold another round of Cybersecurity Summits this year.

It Takes a Toolbox: Resources for Rural Electric Cooperatives

When it comes to cybersecurity, a flexible toolbox with many different resources and options is necessary. There are no "silver bullets." For the electric sector, this includes, but is not limited to: standards, cyber assessment, guidance, tools and resources for small and medium entities, cyber mutual assistance programs, and a national industry playbook. Below is a summation of some of the cybersecurity resources available for rural electric cooperatives, either directly from government or through NRECA. Many of these have been alluded to earlier in the testimony.

Tools and resources for small and medium entities: In addition to the Self-Assessment Research Program and the Cybersecurity Summit Series, the RC3 Program is developing:

- cybersecurity training and guidance resources to assist co-op employees to understand their roles and their ability to help protect their cooperative;
- increased awareness of existing information sharing resources and opportunities; and

- new technologies to identify, prevent and/or mitigate cyber incidents.

Though the RC3 Program is specifically focused on developing resources for those utilities with limited resources, all of the resources developed through the RC3 Program will be available to all NRECA members.

Examples of Cyber Assessments for Industry Broadly: 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. One example is the ES-C2M2, developed by the Office of Electricity through a public-private partnership that supports the adoption of the NIST Cybersecurity Framework by assisting organizations to improve their cybersecurity capabilities. The Office of Electricity is in the process of updating the ES-C2M2, and NRECA will be involved in ensuring that this tool continues to meet the needs of electric cooperatives. The continued development of cybersecurity programs and tools, like the ES-C2M2–combined with access to actionable relevant information, both classified and unclassified–is vital to strengthening security postures in critical infrastructures.

NRECA Guidance for Electric Cooperatives: To further bolster the efforts of ES-C2M2 specifically for electric cooperatives, NRECA developed a "Guide to Developing a Cybersecurity 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 Project used these tools to develop a smart grid cybersecurity plan. The most recent version of the guide was published in 2014. This resource, developed by NRECA with funding from the Office of Electricity, is available to all utilities and is posted on DOE's website

Cyber Mutual Assistance programs: Given the extensive experience they have responding to storms and natural disasters, electric cooperatives have an effective approach to emergency management and disaster recovery. Following a disaster, cooperatives rapidly deploy crews and equipment to impacted areas to assist other cooperatives with the restoration of power. The foundation of this program is a standard Mutual Assistance Agreement, signed by the vast majority of NRECA member electric cooperatives. Cooperatives help each other and other electric utilities as needed. Individual co-ops typically coordinate mutual assistance efforts through their statewide organizations, which lead efforts to identify in-state and cross-state needs and resources. This culture of mutual assistance can be found across the electric sector 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 has 141 members, including 35 cooperatives, participating—covering more than 80% of all U.S. electricity customers.

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 may target elements of 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 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 public when such a situation arises. The playbook is an evergreen document that can be updated by industry when lessons are learned from an exercise or real-world experiences.

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.

Importance of Partnerships & Information Sharing

As mentioned earlier, the ESCC serves a vital role by providing the venue 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 cybersecurity through the ESCC.

These efforts by industry CEOs from all segments of the electric 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.

In addition to industry and government collaboration throughout the year, the ESCC serves in 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 managed confidentially and distributed through the NERC secure internet portal directly to electric industry asset owners and operators.

The E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership co-funded by DOE and industry that facilitates the 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 an excellent example of efforts to bridge the divides between the classified realm and sharing actionable, relevant information with private industry.

We appreciate the continued efforts of the administration in coordinating with the ESCC and we stand ready to continue our work with government counterparts to ensure a secure, reliable and resilient grid.

Additionally, NRECA and our members look forward to working with the leadership and staff that will be assigned to the recently announced DOE Office of Cybersecurity, Energy Security and Emergency Response.

How Congress Can Continue to Help

In the previous Congress, several pieces of legislation were passed that assist efforts in securing the grid. Congress passed 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 electric utility industry. This legislation provided additional confidence in sharing information safely through existing channels, such as the E-ISAC, between the federal government and private sector. Congress also enacted into law the Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), which included these provisions:

- 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. DOE was already the SSA for the sector, but this was appropriately clarified to include cyber issues; and
- Freedom of Information Act exemptions for "critical electric infrastructure information" submitted by industry to FERC and other federal agencies.

Congress should recognize that the electric utility industry is the only one with mandatory and enforceable cybersecurity standards. As such, we ask that lawmakers keep this in mind when considering broad cybersecurity proposals to ensure that they do not conflict with existing standards within our industry. With that being said, here are some areas for how Congress can and should help:

1. **Information Sharing**: One of the best examples of how government can improve its information sharing with industry is the December 2015 Ukraine cyber breach. While the content of the classified and unclassified information from our government was helpful, the timeliness of getting specific, actionable information to industry after an event must be improved so that electric utilities can respond as quickly as possible. In addition, assurances that sensitive information shared from industry to government is properly protected and free of liability concerns when shared in good faith would improve the information-sharing environment.

2. **Insider Threats**: The owners and operators of critical infrastructure understand that the most significant threats tend to be those that are hardest to identify – including the insider threat. We urge Congress to consider legislation giving the FBI the statutory authority to assist industry on a voluntary basis in performing enhanced background checks for terrorist activity 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.

3. **Continue Assistance for Small and Medium Utilities**: A one-size-fits-all cybersecurity strategy simply does not work in the electric sector. For example, security issues relevant for an entity on the BES may be very different from another BES entity due to geography, engineering architecture and redundancies. Similarly, security issues relevant for the BES are not necessarily the same as issues facing the local distribution system. As such, Congress should protect funding for DOE's "Improving the Cyber and Physical Security Posture of the Electric Sector" initiative, which supports NRECA's RC3 Program and is funded by the Office of Electricity Delivery and Energy Reliability's Cybersecurity for Energy Delivery Systems program (CEDS). This is the only program where DOE and NRECA are specifically focused on addressing the unique cybersecurity needs of small- and mid-sized distribution utilities. The RC3 Program emphasizes collaboration and personalized training and is helping distribution cooperatives build stronger cybersecurity programs.

4. **Supply Chain:** The language of the SAFETY Act of 2002 and the accompanying rule always have made clear that protections under the law apply to cyber events and would apply regardless of whether a terrorist group conducted such an attack. In practice, there has been some hesitancy on the part of industry to utilize the SAFETY Act to protect against federal claims arising from 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. Senator Daines' legislation—S. 2392, the Cyber Support for Anti-Terrorism by Fostering Effective Technologies Act of 2018 (Cyber SAFETY Act)—would explicitly allow for the liability protections of the SAFETY Act to become available when the Secretary deems that an act of terrorism or a "qualifying cyber incident" has occurred. Without the need to link a cyberattack to an "act of terrorism," more companies would take advantage of the SAFETY Act program, thereby fulfilling the law's original intent of promoting the widespread deployment of products and services that mitigate malicious events, including those related to cybersecurity.

5. **Continued Support for Cybersecurity Research and Development**: Fundamental research is needed within the electricity sector to develop the tools and technology necessary to strengthen our cybersecurity posture and ensure the ability to rapidly recover from a cyber incident. NRECA works collaboratively with the DOE's Office of Electricity on many research projects, electric cooperatives partner with the DOE's National Laboratories to advance research efforts, and NRECA and our members provide industry input into the department's research priorities. NRECA is an active member supporting the Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS) research consortium, an initiative located at the University of Arkansas and supported by the Office of Electricity. Without a strong research and development program, many industry vendors will not be able to keep pace in developing solutions to address the rapidly changing cybersecurity threats that our industry faces.

Conclusion

Thank you for holding today's hearing on this very important issue. I am proud of the efforts electric cooperatives and the broader electric sector make to continually improve our

cybersecurity posture. Even though our sector is comprised of various business models, we work together to secure our nation's reliable electricity supply. I hope that my testimony provides the Committee insight regarding a few of the many activities and collaborative efforts among electric cooperatives and the broader industry and our federal government partners. We share your goal of protecting this nation's critical infrastructure from cyber threats and appreciate your efforts to address this important national security issue.

Electric cooperatives believe building and investing in partnerships is 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 security tactics as needed to keep pace with these threats.