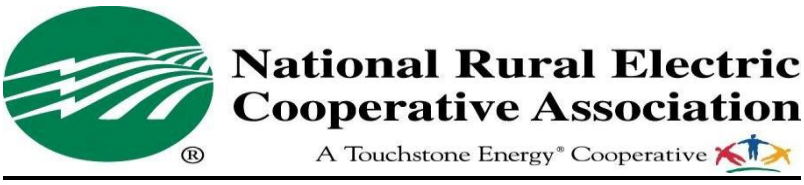

Testimony of Mr. Duane D. Highley

President and CEO of the Electric Cooperatives of Arkansas

to the Committee on Energy and Commerce

U.S. House of Representatives

May 21, 2013

Introduction

Mr. Chairman, Mr. Ranking Member, and all members of the Committee, thank you for inviting me to testify today on the electric power sector's involvement with the ongoing implementation of the Administration's Cybersecurity Executive Order.

The National Rural Electric Cooperative Association (NRECA) is the national service organization dedicated to representing the national interests of cooperative electric utilities and the consumers they serve. NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Electric cooperative service territory makes up 75 percent of the nation's land mass. 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.

NRECA members are not-for profit, consumer-owned distribution cooperatives. NRECA's members also include 67 generation and transmission ("G&T") cooperatives, which generate and transmit power to 668 of the 838 distribution cooperatives across the nation. The G&Ts are owned by the distribution cooperatives they serve. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost.

Because we are owned by the members we serve, 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 bit of our expenses 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.

Arkansas Electric Cooperative Corporation (AECC) was created in 1949 and provides power for the more than 500,000 farms, homes and businesses served by our 17 distribution electric cooperative owners. AECC relies on a diverse generation mix, including hydropower, natural gas, coal, and renewables, to serve its members.

Electric cooperatives are dedicated to protecting and securing our electric system assets. We are guided by our obligation to serve and the fact that our consumers are our owners. The Rural Utilities Service (RUS) has long required each electric cooperative borrower to adhere to rigorous construction standards. Beginning in October 2004, RUS Electric System Emergency Restoration Plan (ERP) regulations in 7 CFR Part 1730 required each borrower to perform a vulnerability and risk assessment and to develop emergency recovery plans for physical and cyber incidents. In addition, borrowers are also required to annually exercise their ERP.

Electric cooperatives take cybersecurity risks very seriously and work diligently to understand, mitigate and respond to cyber events. NRECA supports them by working with policymakers and stakeholders to strengthen the public-private partnerships that are an essential component of grid protection. NRECA's Cooperative Research Network (CRN) has been extremely proactive in developing cybersecurity tools targeting distribution utilities (but

applicable to utilities of all sizes) which typically are not subject to NERC standards compliance because their operations do not impact the Bulk Electric System (BES). Since electric cooperatives are at the forefront of smart grid deployment, our members are very much aware of the need to comprehensively address the security of any new telecommunications-enabled devices. As part of its fulfillment of a $68 million smart grid demonstration program under the American Reinvestment and Recovery Act, CRN developed cybersecurity plans for the 23 participating electric cooperatives. That effort led to the development of a tool that compiles thousands of pages of industry and government guidance on cybersecurity into a digestible, deployable plan. It is publicly available at http://www.nreca.coop/bestbets/cybersecurity and anecdotal evidence tells us it is in use at many utilities, including some outside the cooperative network. CRN now leads training open to all segments of the industry on the plan and cybersecurity best practices.

NERC Cybersecurity Mandatory Standards

Electric power sector representatives have participated in each stage of the evolution of the North American Electric Reliability Corporation (NERC), including helping develop Energy Policy Act of 2005 (EPAct '05) amendments to the Federal Power Act which enabled NERC to receive FERC's approval as the Electric Reliability Organization (ERO) in 2006. We appreciate the support and leadership of many members of the Energy and Commerce Committee who contributed to EPAct's reliability provisions. Nearly eight years later, the legislation is working, and should provide a model for other Critical Infrastructure sectors as they work through Executive Order implementation. NERC collaborates with the electric power sector to develop mandatory, enforceable reliability standards that apply to users, owners and operators of the BES.

The NERC reliability standards, 116 in all, include nine devoted to cybersecurity, known as the Critical Infrastructure Protection, or CIP, standards. Electric power sector entities which own or operate BES assets are required to adhere to one or more of the NERC CIP standards. In order to comply, utilities have made significant investments in strategic plans, consultants, hardware, software, training, and teams of full-time employees to ensure compliance and create a culture of security.

The CIP standards and the Nuclear Regulatory Commission (NRC) cybersecurity standards are the only mandatory and enforceable cybersecurity standards in place across the vast array of US critical infrastructures. When covered entities are found to have violated the CIP 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.

Today, hundreds of electric power sector technical experts are routinely deployed in NERC teams working on the continual process of writing and improving the already-extensive body of NERC reliability standards, including cyber security standards. On January 31, 2013, NERC filed its CIP Version 5 standards with FERC for approval. NERC and the industry are continuing to address FERC directives, National Institute of Standards and Technology (NIST) standards, and other best practices to make sure that the standards evolve with improvements in technology and the ever-changing risks. CIP Version 5 is a comprehensive approach; it addresses all of FERC's directives and implements key elements of NIST cybersecurity

guidelines. On April 18, 2013, FERC issued a Notice of Proposed Rulemaking in which it proposed to approve CIP Version 5.

Given the constantly evolving landscape of cyber risks, the industry recognizes that not every threat or vulnerability can or should be addressed in a standard. To keep up with emerging threats, the industry participates in the Electric Sector-Information Sharing and Analysis Center (ES-ISAC), which is operated by NERC. The ES-ISAC 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, distributed through NERC's secure portal directly to asset owners and operators.

Perspectives on Executive Order Implementation

Overview of Framework and Potential Intersection with NERC Standards

The electric power sector appreciates the Administration's engagement on cybersecurity as a national security imperative and agrees with the Executive Order's directive that the Cybersecurity Framework "shall provide a prioritized, flexible, repeatable, and performance-based and cost- effective approach." Sec. 7(b). To that end, we believe that the framework must:

(1) Be high-level and flexible, to ensure that the Cybersecurity Framework can be adapted to each of the Nation's diverse critical infrastructure sectors, without unintended consequences;

(2) Build upon each sector's existing processes, standards and guidance, including the sector-specific regulatory standards which already exist in the electric and nuclear industries;[1]

(3) Avoid time-consuming and unnecessary duplication of efforts;[2]

(4) Preserve and build upon existing public-private partnerships;[3] and

(5) Be risk-based and cost-effective.

Among the existing government-industry partnerships we believe NIST should be aware of as it seeks to craft a Framework is the innovative and cooperative approach the electric power sector and the federal government are now pursuing. With both sides committing their expertise and leadership to keep the electric grid as secure and resilient as possible, the sector is working to improve coordination with the government at the most senior levels.

Specifically, a group of CEOs from the investor-owned, public power and cooperative segments of the electric power sector have engaged in what we hope will become an ongoing partnership with senior officials throughout the government, including the White House National

[1] This is consistent with Section 7 of the Executive Order, which directs that the Cybersecurity Framework incorporate existing consensus-based standards and industry best practices to the fullest extent possible.
[2] This is consistent with Sec. 10(c) of the Executive Order which requires agencies to report on duplicative, conflicting or excessively burdensome cybersecurity requirements.
[3] See generally Section 8 of the Executive Order.

Security Staff, Department of Energy (DOE), and Department of Homeland Security (DHS) leadership. This collaboration has resulted in classified briefings to inform senior industry executives of some threats facing the electric grid, as well as a commitment from government representatives to improve the flow of information between the government and industry. Other initiatives for this government-industry partnership include addressing legal, technical, and procedural hurdles associated with the deployment of proprietary government technology on utility networks to improve real-time situational awareness, and a directive to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

I would like to emphasize that neither the Executive Order process nor its resulting Framework should be considered a substitute for, or a competitor with, the mandatory standards approved by independent regulatory agencies such as FERC and the NRC. Moreover, any framework must not undermine the existing NERC standards development process, which develops standards that can operate across the North American grid and helps to assure cybersecurity on an international basis. These mandatory standards address public policy objectives that are unique to the electric and nuclear sectors. The Framework should be focused on a much broader task, leveraging the federal government's capabilities and expertise with that of the nation's private sector critical infrastructure owners and operators, to ensure cybersecurity protection and resiliency through rapid sharing and adoption of voluntary standards, guidelines and best practices and close cooperation with our federal government partners.

The Critical Need for Information Sharing and Security Clearances

Information sharing must be a critical component of the Executive Order conversations and eventual Framework. The electric power sector appreciates the support of many members of the Energy and Commerce Committee for H.R. 624, the Cybersecurity Intelligence Sharing and Protection Act. The risks and potential impacts are very different for public-facing elements of a utility's Internet-connected business systems, versus their industrial control systems, which typically are not Internet-connected, or if they are, they are protected with more aggressive security schemes. Given that millions of attempted cyber-attacks occur daily on our public facing sites, utilities will need to rely upon assistance from governmental authorities, particularly in the form of helping to identify threats as well as threat trends.

Much of the information needed to fully understand the nature of the cyber threats faced by our industry is classified at a level that is unavailable to our organizations. The DHS Private Sector Clearance Program (PSCP) has helped key electric utility staff obtain security clearances, which allow them access to basic information about such threats. However, a recent shutdown of the PSCP created a substantial backlog in the processing of clearance applications, and hampered the industry's access to important information. Processing of these applications has now resumed and our hope is that we can continue to expand our ability to access needed information.

In addition to expanding the number of utility personnel with clearances, it is critical that government agencies regularly share clear, actionable information with industry personnel in cleared briefings. Our industry is staffed by dedicated, qualified employees who can be counted on to take the steps necessary to protect our systems – if they understand the nature of the threat against them. There is also a need for a limited number of electric industry personnel to obtain

higher-level clearances than provided by the PSCP, which would allow these individuals to help the government analyze threat information and provide context for the intelligence community.

Effective information sharing should take the form of a timely and efficient mechanism to pass along threat data, warnings, and trend information. Examples of the kinds of information that would be useful to share include: signatures of known viruses and malware; points of origination for known threat actors; known behavioral techniques of anonymous threats such as "Advanced Persistent Threats" (APT); information regarding potential vectors for introduction of cyber threats, such as counterfeit parts and software; and the sharing of best practices or policies to combat or defeat emerging threats and vulnerabilities.

Many federal stakeholders refer to the existing Defense Industrial Base information sharing pilot program as a potential model for the Framework. That program has certainly enjoyed some successes, but there are lessons to be learned there and a careful review of its effectiveness will be critical to ensuring that taxpayer funds are not spent on unnecessarily duplicative or marginally-effective programs.

Liability Protections

Liability protections will also need to be woven into the Framework. Even if current authority does not allow the Administration to extend liability protections, a full discussion of the need for liability protections must be a central part of the Framework discussion so that Congress can fully examine this complex but uniquely important aspect of cybersecurity policy.

Utilities already do their utmost to protect personally identifiable information (PII), but at the same time realize there could be a compelling need to share information that could accidentally include PII. The potential civil liability for the sharing of such information is a significant deterrent, and so we encourage the development of mechanisms that would protect Critical Infrastructure entities from such claims. We also encourage the use of liability protection in the form of shields that protect an entity from claims that it should have acted upon information received. Even with the filtering that is likely to be performed by the government to help narrow the types of information shared to only the most useful, it is still likely to be a monumental task for electric utility employees to determine what information is relevant and actionable. Utility employees should not have to be concerned that despite their best efforts to filter through the shared information, certain actions may or may not be taken that could lead to a cyber-event. Only a liability shield can resolve those concerns.

One mechanism for attaching affirmative legal defenses to the Framework is already in place and in use. DHS administers the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or the "SAFETY Act". The SAFETY Act, which was passed into law as part of the Homeland Security Act of 2002 (the law authorizing the creation of DHS), is intended to offer affirmative legal defenses to companies that sell or otherwise deploy security technologies (which includes products, services, policies, and procedures) designed to deter, defeat, respond to, mitigate, or otherwise combat security threats. The SAFETY Act offers two types of liability protection. The first type of protection is known as "Designation", which sets a specific cap on damages that may be awarded in litigation following an attack, along with a

prohibition on punitive damages and pre-judgment interest, as well as a requirement that SAFETY Act-related claims may only be brought in Federal courts. Under Designation, the cap on damages is equal to an amount of insurance that the "seller" of the SAFETY Act-approved technology or service must carry as a condition of the award.

The second layer of protection under the SAFETY Act is referred to as "Certification". A Certification award provides the same protections as a Designation, as well as a presumption of immunity from claims arising out of or related to the use of the SAFETY Act-approved technology or service. The protections of the SAFETY Act can be negated with a demonstration that the applicant committed fraud or willful misconduct in the submission of the SAFETY Act application to DHS.

Conclusion

In closing, I thank you again for inviting me to testify. I hope that our extensive experience in responding to and recovering from unexpected events can serve as a model that informs the Framework for all critical infrastructure sectors.