Scott R. Bowers

Vice President of Government Relations

Indiana Electric Cooperatives

Testimony before the Senate Appropriations Homeland Security Subcommittee on:

"Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future"

May 7, 2014

Indiana Electric Cooperatives (IEC), the nation's first electric cooperative service organization, represents 39 electric distribution cooperatives that serve over 1.3 million Hoosiers in 89 of the state's 92 counties. Collectively, our members employ more than 1,500 individuals and represent the second-largest electric power provider in Indiana. We serve a diverse expanse of Indiana communities, from rural and farming areas, industrial parks and employment zones to burgeoning suburbs. IEC appreciates the opportunity to provide the following testimony before the Senate Appropriations Homeland Security Subcommittee regarding "Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future."

Indiana's electric cooperatives played a foundational role in delivering electricity to communities across Indiana 80 years ago. Today, we fuel progress by delivering more than electricity to the communities we serve. We contribute to economic development, community development and youth and education programs across Indiana. We continue to deliver safe, secure, reliable and affordable electric power across the state, including hard-to-reach rural areas. These same electric cooperatives are at the forefront in the promotion of renewable energy sources, energy efficiency programs and technology, ensuring electric power sources for future generations.

Introduction

IEC recognizes your concerns related to the issue of cybersecurity. We have taken steps, sometimes independent of government regulation, to provide the security and reliability required and necessary for our consumers. Due to our construct and the areas we generally serve, most people do not recognize the leadership role electric cooperatives have assumed - specifically in the areas of renewable energy sources, energy efficiency and cybersecurity.

IEC has two generation and transmission cooperative (G&Ts) members, Hoosier Energy Rural Electric Cooperative (Hoosier Energy) and Wabash Valley Power Association (Wabash Valley), who provide Indiana distribution cooperatives with wholesale electric power from coal, natural gas and renewable energy sources. Both G&Ts are fully integrated and registered on the North American Electric Reliability Corporation (NERC) Compliance Registry by applicable function. As such, each of Indiana's G&T cooperatives are required to comply with approved Reliability Standards related to cybersecurity, operations and system reliability.

Our 39 distribution cooperatives generally do not own Bulk Electric System (BES) assets. Therefore, they focus largely on the reliability and security of their distribution systems, which brings electricity to homes and businesses, protecting member data and their business systems where the data is processed and stored.

This afternoon, I would like to specifically recognize the cybersecurity efforts of our two G&Ts. I will start by discussing Hoosier Energy's efforts to address the cybersecurity threat.

Hoosier Energy

Hoosier Energy maintains a thorough cybersecurity program that protects facilities that are critical to the reliability of the BES against a myriad of cyber vulnerabilities. Most notably, Hoosier Energy developed an in-house scanning utility called the Windows Configuration Management Utility (WinCMU) which gives Hoosier Energy complete visibility into its systems and reports any unexpected changes to its security team. Knowing what is on a system is the most important step in maintaining a secure environment. During a recent audit by NERC, auditors acknowledged this and praised WinCMU and Hoosier Energy for going above and beyond the requirements in NERC's cybersecurity standards. Compliance with these standards is enforced by NERC and the Federal Energy Regulatory Commission (FERC).

In addition to complying with such standards, Hoosier Energy's cybersecurity program mitigates and protects against a wide range of vulnerabilities including:

- Ignorance, Indifference and Lack of Knowledge of Cyber Threat Protection;
- Information Exfiltration;
- Network Based Cyber Attacks;
- Unmanaged Changes to Cyber Assets and Protective Systems;
- Direct Attack on Cyber Assets; and
- Physical Attack on Cyber Assets.

(See Appendix A for description of these vulnerabilities)

IEC's other G&T, Wabash Valley, also has a cybersecurity program which includes some similar elements to Hoosier Energy's program. Next, I would like to highlight Wabash Valley's efforts to address the issue of cybersecurity.

Wabash Valley

The protection of people and assets are top priorities for Wabash Valley. As technology continues to evolve, cybersecurity threats become more advanced and increasingly difficult to detect and prevent. Wabash Valley firmly believes it takes every employee being vigilant to ensure their personal safety and the safety of Wabash Valley's assets (both physical safety and cybersecurity).

Relative to cybersecurity standards, Wabash Valley, along with other small entities, awaits the implementation of NERC's Critical Infrastructure Protection (CIP) standards, Version 5 (cybersecurity standards). Although not required by previous versions of the CIP standards, Wabash Valley has already developed a cybersecurity plan. In addition, an external consultant was hired by Wabash Valley to perform an assessment on its CIP program and systems. The consultant determined its CIP program was thorough for a small entity and that no changes to systems were required at that point in time.

Under NERC's event reporting standards, applicable entities were required to establish a reporting relationship with the Federal Bureau of Investigation (FBI). Wabash Valley established reporting relationships with FBI offices in all states and cities where it has member cooperatives or plant facilities (Indiana, Ohio, Illinois and Missouri). Although direct reporting of events to the FBI is no longer required by the NERC standard, Wabash Valley feels it is important to continue to keep the FBI or the Joint Terrorism Task Force (JTTF) in the reporting chain for cybersecurity (and other) events. Wabash Valley is part of the FBI's Strategic Partnership with businesses. As such, Wabash Valley receives regular bulletins and communications from the FBI to keep them informed about various situations/threats that could affect the safety and security of company assets and/or personnel.

Through the NERC Alert System and the Electric Sector Information Sharing and Analysis Center (ES-ISAC) housed within NERC, communications and alerts related to various potential threats are provided to our industry. It is part of Wabash Valley's established procedures for these communications to be reviewed by compliance and technical services personnel to assess a potential threat to the G&T. If the threat has potential applicability to Wabash Valley, then systems are reviewed and, as appropriate, preventive actions implemented. If the threat, such as HEARTBLEED, has potential impact for company employees on their computer systems at home, information is communicated to Wabash Valley employees. On a regular basis, the Wabash Valley security officer emails pertinent security topics to staff.

Wabash Valley welcomes the finalization of the cyber and physical security standards in the near future. In the meantime, they will continue to seek proactive measures to ensure the security of all G&T personnel and assets.

So where do we go from here? Beyond just the updating of the CIP standards, there are other actions that can assist us, the owners and operators, in assuring access to power. In talking with both our G&Ts, they shared concerns regarding some areas where they see opportunity for improvement.

Information Sharing

While we recognize and appreciate that improvement has been made by the federal government in the flow and sharing of cyber and physical security related information over time, the need for continued improvement still exists. Our ability to receive timely and actionable information remains a work in progress. The media remains our primary source of threat-related information. By the time information is shared with us from the federal agencies, it can be too late for us to address the threat. Under our current situation, the damage is already done and we have moved into mitigation mode if we were impacted by the threat. Improving the timeliness of the threat communication would also better position us to take preventive actions on the front end in hopes to fend off or, if penetrated, minimize the impact to our system.

Additionally, expanding the number of "secret" clearances permitted for cooperative staff and allowing for "top secret" clearance for select senior-level executive staff would also be beneficial. This adjustment in security clearance procedures, along with liability protections for information sharing with the government, would allow for more real-time and actionable information to be shared.

Flexibility

IEC would strongly encourage Congress and the federal agencies to avoid enacting "one size fits all" solutions for cyber and physical security. Our member cooperatives share a common mission, core principles and similarities in structure, but they are each independent and unique in the tactics, processes and protocols they utilize to serve their members. By affording Indiana's electric cooperatives that flexibility, each of our member cooperatives would be positioned to deploy the measures, technologies and systems that best fit their operations, assets and efforts to combat cyber and physical threats. In addition, each cooperative would be able to account for implementation costs, which helps maintain affordability, without compromising the security measures.

Partnerships

Partnerships have been one of the most beneficial and productive tools used by Indiana's electric cooperatives in addressing the cybersecurity issue. The partnerships that have been most successful for us have generally been cooperative to cooperative based. Indiana's electric cooperatives have also benefitted

from their relationships with other private organizations, i.e. ACES, through their interactions with their Regional Transmission Organizations (RTO) as well as our national association, the National Rural Electric Cooperative Association (NRECA). While electric cooperatives were born with the assistance of the federal government in the 1930s, our approach has generally been to work within the cooperative community or the private sector to find cost effective solutions to the issues facing our industry. These types of partnerships, along with finding additional opportunities to enhance the working relationship between the responsible federal agencies and our member cooperatives through our members and through the NRECA, should be encouraged as well. The Electricity Sector Coordinating Council (ESCC) is a great example of one of these partnerships. With the ESCC you see individual cooperative G&Ts, as well as participants from the Investor Owned Utilities and Municipal Electric Utilities, and the associated trade associations at a table with the Department of Energy (DOE), FERC, NERC and the Department of Homeland Security (DHS) working together to identify and find solutions.

Consistency

Due to the multiple levels of government oversight concerning cybersecurity (e.g. FERC, NERC and NERC's regional entities), finding consistency in the compliance process has had its challenges. The vague nature of some of the cybersecurity standards coupled with inconsistencies in the interpretation and auditing of those standards have created challenges with cybersecurity compliance for our member cooperatives. Refining this process to increase consistency and by providing more clarity with the respective standards would help streamline the process, enhance our effectiveness and provide greater certainty to our cybersecurity initiatives.

Physical Security

While the focus of this hearing was specific to the issue of cybersecurity, IEC would like to briefly address the issue of physical security. There has been increased discussion surrounding this issue due to recent events and IEC acknowledges the importance of protecting our physical assets as well. The current initiative by FERC and NERC to develop physical security standards for critical assets is viewed as a positive step by Indiana's electric cooperatives. There is more to be accomplished with this effort and we welcome the opportunity to engage and provide our perspective throughout the process.

Conclusion

My comments today outlining areas of opportunity should not be viewed negatively on the interactions Indiana's electric cooperatives have had to date with the federal agencies engaged in the cybersecurity arena. Our member cooperatives who work most closely with FERC, NERC, DHS and DOE, to name a few, would agree significant improvements and advancements have been made in all of these areas since the effort began. Our primary message for you today is that we are on a good path, but opportunities to improve still exist. Each of us, not just the respective federal agencies, must assume our individual responsibility to work constructively, effectively and, most importantly, in partnership to address both current and future cyber-related threats to the reliability and security of our nation's electric grid.

Appendix A: Descriptions of Referenced Cyber Security Mitigated Vulnerabilities

Ignorance, Indifference and Lack of Knowledge of Cyber Threat Protection

Hoosier Energy's cybersecurity program ensures all levels of the organization are appropriately engaged. Responsibilities are clearly delineated among leadership and those responsible for direct cybersecurity activities.

Training and awareness programs are required for all who have access to cyber assets critical to the reliability of the BES. Training covers why Hoosier Energy's program is important, how it protects us and the relevant responsibilities. In addition, Hoosier performs awareness exercises exemplified by a Spearphishing exercise in 2013 that reduced click-thru rates from 30 percent to 2 percent.

Information Exfiltration

Hoosier Energy maintains an information protection program that identifies and classifies critical information, how it can be shared and with whom it can be shared.

Network-Based Cyber Attacks

Hoosier Energy maintains a separate, isolated network through the use of an electronic security perimeter (ESP) that isolates its critical cyber assets from less secure corporate network and neighboring utility connections. All communication is denied by default. Allowed communications are limited to specific protocols and approved sources from outside the ESP.

Direct Attack on Cyber Assets

Like in the ESP, communication is denied by default at each individual cyber asset.

In addition:

- All relevant security patches are applied judiciously
- Malicious software prevention is installed and kept current
- Strong passwords are required and changed periodically
- Unnecessary physical ports are blocked or disabled

Unauthorized Access and Changes to Cyber Assets and Protective Systems

All access is provisioned on the principle of need-to-know. No access is granted without first successfully completing a background check.

ESP communications are monitored and logged around the clock. Any change in configuration or any attempts at unauthorized access automatically creates an alert.

The WinCMU creates a baseline for each protected cyber asset. The WinCMU performs a daily comparison of the actual configuration and the baseline to systematically identify and alert on unexpected changes.

Physical Attack on Cyber Assets

All critical cyber assets are protected within a physical security perimeter (PSP) with access controlled using key cards, monitoring and logging.